Prof. Dr. Antje von Ungern-Sternberg

# Reader zur Vorlesung „Recht der Daten“

Universität Trier, Schwerpunktbereich 8

Universität Trier

# Inhaltsverzeichnis

**A. NORMEN ..... 4**

**I) EU-DATENSCHUTZGRUNDVERORDNUNG ..... 4**

ERWÄGUNGSGRÜNDE ..... 4
KAPITEL I: ALLGEMEINE BESTIMMUNGEN (ART. 1-4) ..... 36
KAPITEL II: GRUNDSÄTZE (ART. 5-11) ..... 39
KAPITEL III: RECHTE DER BETROFFENEN PERSON (ART. 12-23) ..... 43
KAPITEL IV: VERANTWORTLICHER UND AUFTRAGSVERARBEITER (ART. 24-43) ..... 50
KAPITEL V: ÜBERMITTLUNGEN PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN (ART. 44-50) ..... 61
KAPITEL VI: UNABHÄNGIGE AUFSICHTSBEHÖRDEN (ART. 51-59) ..... 66
KAPITEL VII: ZUSAMMENARBEIT UND KOHÄRENZ (ART. 60-76) ..... 71
KAPITEL VIII: RECHTSBEHELFE, HAFTUNG UND SANKTIONEN (ART. 77-84) ..... 79
KAPITEL IX: VORSCHRIFTEN FÜR BESONDERE VERARBEITUNGSSITUATIONEN (ART. 85-91) ..... 82
KAPITEL X: DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE (ART. 92-93) ..... 83
KAPITEL XI: SCHLUSSBESTIMMUNGEN (ART. 94-99) ..... 84

**II) BUNDESDATENSCHUTZGESETZ ..... 86**

TEIL 1 GEMEINSAME BESTIMMUNGEN (§§ 1-21) ..... 86
*Kapitel 1: Anwendungsbereich und Begriffsbestimmungen ..... 86*
*Kapitel 2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten ..... 87*
*Kapitel 3 Datenschutzbeauftragte öffentlicher Stellen ..... 88*
*Kapitel 4 Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ..... 89*
*Kapitel 5 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union ..... 94*
*Kapitel 6 Rechtsbehelfe ..... 95*
TEIL 2 DURCHFÜHRUNGSBESTIMMUNGEN FÜR VERARBEITUNGEN ZU ZWECKEN GEMÄß ARTIKEL 2 DER VERORDNUNG (EU) 2016/679 (§§ 22-44) ..... 96
*Kapitel 1 Rechtsgrundlagen der Verarbeitung personenbezogener Daten ..... 96*
*Kapitel 2 Rechte der betroffenen Person ..... 102*
*Kapitel 3 Pflichten der Verantwortlichen und Auftragsverarbeiter ..... 104*
*Kapitel 4 Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen ..... 105*
*Kapitel 5 Sanktionen ..... 106*
*Kapitel 6 Rechtsbehelfe ..... 107*
TEIL 3 BESTIMMUNGEN FÜR VERARBEITUNGEN ZU ZWECKEN GEMÄß ARTIKEL 1 ABSATZ 1 DER RICHTLINIE (EU) 2016/680 (§§45-85) ..... 107
*Kapitel 1 Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten ..... 107*
*Kapitel 2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten ..... 109*
*Kapitel 3 Rechte der betroffenen Person ..... 111*
*Kapitel 4 Pflichten der Verantwortlichen und Auftragsverarbeiter ..... 114*
*Kapitel 5 Datenübermittlungen an Drittstaaten und an internationale Organisationen ..... 121*
*Kapitel 6 Zusammenarbeit der Aufsichtsbehörden ..... 123*
*Kapitel 7 Haftung und Sanktionen ..... 124*

TEIL 4 BESONDERE BESTIMMUNGEN FÜR VERARBEITUNGEN IM RAHMEN VON NICHT IN DIE ANWENDUNGSBEREICHE DER VERORDNUNG (EU) 2016/679 UND DER RICHTLINIE (EU) 2016/680 FALLENDEN TÄTIGKEITEN (§ 85) ... 124

**B. URTEILE ... 126**

**I) BVERFGE ... 126**

1) BVERFGE 65, 1 – VOLKSZÄHLUNG ... 126
*a) Sachverhalt ... 126*
*b) Leitsätze ... 126*
*c) Begründung ... 126*

2) BVERFGE 109, 279 – GROßER LAUSCHANGRIFF ... 137
*a) Sachverhalt ... 137*
*b) Leitsätze ... 137*
*c) Begründung ... 138*

3) BVERFGE 120, 274 – SCHUTZ DER VERTRAULICHKEIT UND INTEGRITÄT INFORMATIONSTECHNISCHER SYSTEME ... 155
*a) Sachverhalt ... 155*
*b) Leitsätze ... 156*
*c) Begründung ... 156*

4) BVERFGE 115, 320 – RASTERFAHNDUNG II ... 176
*a) Sachverhalt ... 176*
*b) Leitsätze ... 178*
*c) Begründung ... 178*

5) BVERFGE 129, 208 – TKÜ-NEUREGELUNG ... 190
*a) Sachverhalt ... 190*
*b) Leitsätze ... 191*
*c) Begründung ... 192*

**II) EUGH ... 199**

1) EUGH C-465/00, C-138, C-139/01 – RECHNUNGSHOF ... 199
*a) Sachverhalt ... 199*
*b) Leitsätze ... 201*
*c) Begründung ... 201*

2) EUGH C-92, C-93/09 - VOLKER UND MARKUS SCHECKE GBR, HARTMUT EIFERT ... 207
*a) Sachverhalt ... 207*
*b) Leitsätze ... 208*
*c) Begründung ... 209*

3) EUGH C-293, C-594/12 - DIGITAL RIGHTS IRELAND LTD ... 216
*a) Sachverhalt ... 216*
*b) Leitsätze ... 216*
*c) Begründung ... 217*

4) EUGH C-131/12 - GOOGLE SPAIN SL, GOOGLE INC. ... 222
*a) Sachverhalt ... 222*
*b) Leitsätze ... 225*
*c) Begründung ... 225*

5) EUGH C-363/14 - EUROPÄISCHES PARLAMENT ... 233

*a) Sachverhalt* ... *233*

*b) Begründung* ... *233*

6) EuGH C-518/07 - Europäische Kommission ... 241
*a) Sachverhalt* ... *241*

*b) Leitsatz* ... *241*

*c) Begründung* ... *242*

7) EuGH C-203/15, C-689/15 - Home Department ... 246
*a) Sachverhalt* ... *246*

*b) Leitsätze* ... *247*

*c) Begründung* ... *247*

8) EuGH Gutachten 1/15 ... 256
*I. Gutachtenantrag* ... *256*

*II. Rechtlicher Rahmen* ... *257*

*III. Vorgeschichte des geplanten Abkommens* ... *258*

*IV. Entwurf eines Beschlusses des Rates über den Abschluss des geplanten Abkommens* ... *260*

*V. Das geplante Abkommen* ... *260*

*VI. Ausführungen des Parlaments in seinem Gutachtenantrag* ... *268*

*VII. Zusammenfassung der beim Gerichtshof eingereichten Stellungnahmen* ... *270*

*VIII. Stellungnahme des Gerichtshofs* ... *273*

*IX. Antwort auf den Gutachtenantrag* ... *289*

## A. Normen

### I) EU-Datenschutzgrundverordnung

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 27. April 2016
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
(Text von Bedeutung für den EWR)
DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,
auf Vorschlag der Europäischen Kommission,
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,
nach Stellungnahme des Ausschusses der Regionen,
gemäß dem ordentlichen Gesetzgebungsverfahren,
in Erwägung nachstehender Gründe:

**Erwägungsgründe**

(1)Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2)Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3)Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

(4)Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

(5)Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt. Der unionsweite Austausch personenbezogener Daten zwischen öffentlichen und privaten Akteuren einschließlich natürlichen Personen, Vereinigungen und Unternehmen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten, zusammenzuarbeiten und personenbezogene Daten auszutauschen, damit sie ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen können.

(6)Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirt-

schaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.

(7) Diese Entwicklungen erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, da es von großer Wichtigkeit ist, eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen. Natürliche Personen, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.

(8) Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.

(9) Die Ziele und Grundsätze der Richtlinie 95/46/EG besitzen nach wie vor Gültigkeit, doch hat die Richtlinie nicht verhindern können, dass der Datenschutz in der Union unterschiedlich gehandhabt wird, Rechtsunsicherheit besteht oder in der Öffentlichkeit die Meinung weit verbreitet ist, dass erhebliche Risiken für den Schutz natürlicher Personen bestehen, insbesondere im Zusammenhang mit der Benutzung des Internets. Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, können den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.

(10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern. Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „sensible Daten“). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

(11) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie — in den Mitgliedstaaten — gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.

(12) Artikel 16 Absatz 2 AEUV ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen.

(13) Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle

der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Das reibungslose Funktionieren des Binnenmarkts erfordert, dass der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten wird. Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinstunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission maßgebend sein.

(14) Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.

(15) Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.

(16) Diese Verordnung gilt nicht für Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Verkehrs personenbezogener Daten im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten. Diese Verordnung gilt nicht für die von den Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchgeführte Verarbeitung personenbezogener Daten.

(17) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst und im Lichte der vorliegenden Verordnung angewandt werden. Um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu gewährleisten, sollten die erforderlichen Anpassungen der Verordnung (EG) Nr. 45/2001 im Anschluss an den Erlass der vorliegenden Verordnung vorgenommen werden, damit sie gleichzeitig mit der vorliegenden Verordnung angewandt werden können.

(18) Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

(19) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016/680 mit Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den An-

wendungsbereich dieser Verordnung fällt,
als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung.

(20) Diese Verordnung gilt zwar unter anderem für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten.

(21) Die vorliegende Verordnung berührt nicht die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates und insbesondere die der Vorschriften der Artikel 12 bis 15 jener Richtlinie zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste. Die genannte Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt.

(22) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend.

(23) Damit einer natürlichen Person der gemäß dieser Verordnung gewährleistete Schutz nicht vorenthalten wird, sollte die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen betroffenen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten. Um festzustellen, ob dieser Verantwortliche oder Auftragsverarbeiter betroffenen Personen, die sich in der Union befinden, Waren oder Dienstleistungen anbietet, sollte festgestellt werden, ob der Verantwortliche oder Auftragsverarbeiter offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten. Während die bloße Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt ist, können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich in der Union befinden, darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen in der Union Waren oder Dienstleistungen anzubieten.

(24) Die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens

von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.

(25) Ist nach Völkerrecht das Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, so sollte die Verordnung auch auf einen nicht in der Union niedergelassenen Verantwortlichen Anwendung finden.

(26) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

(27) Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

(28) Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der „Pseudonymisierung“ in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.

(29) Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um — für die jeweilige Verarbeitung — die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche, sollte die befugten Personen bei diesem Verantwortlichen angeben.

(30) Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.

(31) Behörden, gegenüber denen personenbezogene Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags offengelegt werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, sollten nicht als Empfänger gelten, wenn sie personenbezogene Daten erhalten, die für die Durchführung — gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten — eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Offenlegung, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte den für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.

(32) Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den

konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.

(33) Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.

(34) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.

(35) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

(36) Die Hauptniederlassung des Verantwortlichen in der Union sollte der Ort seiner Hauptverwaltung in der Union sein, es sei denn, dass Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung des Verantwortlichen in der Union getroffen werden; in diesem Fall sollte die letztgenannte als Hauptniederlassung gelten. Zur Bestimmung der Hauptniederlassung eines Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werden. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird. Das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten oder Verarbeitungstätigkeiten begründen an sich noch keine Hauptniederlassung und sind daher kein ausschlaggebender Faktor für das Bestehen einer Hauptniederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, oder — wenn er keine Hauptverwaltung in der Union hat — der Ort, an dem die wesentlichen Verarbeitungstätigkeiten in der Union stattfinden. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter betroffen, so sollte die Aufsichtsbehörde des Mitgliedstaats, in dem der Verantwortliche seine Hauptniederlassung hat, die zuständige federführende Aufsichtsbehörde bleiben, doch sollte die Aufsichtsbehörde des Auftragsverarbeiters als betroffene Aufsichtsbehörde betrachtet werden und diese Aufsichtsbehörde sollte sich an dem in dieser Verordnung vorgesehenen Verfahren der Zusammenarbeit beteiligen. Auf jeden Fall sollten die Aufsichtsbehörden des Mitgliedstaats oder der Mitgliedstaaten, in dem bzw. denen der Auftragsverarbeiter eine oder mehrere Niederlassungen hat, nicht als

betroffene Aufsichtsbehörden betrachtet werden, wenn sich der Beschlussentwurf nur auf den Verantwortlichen bezieht. Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.

(37) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.

(38) Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

(39) Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

(40) Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder — wann immer in dieser Verordnung darauf Bezug genommen wird — aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

(41) Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof“) und des Europäischen Gerichtshofs für Menschenrechte vor-

hersehbar sein.

(42)Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

(43)Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

(44)Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.

(45)Erfolgt die Verarbeitung durch den Verantwortlichen aufgrund einer ihm obliegenden rechtlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen. Mit dieser Verordnung wird nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt. Ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge kann ausreichend sein, wenn die Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt oder wenn die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnten in diesem Recht die allgemeinen Bedingungen dieser Verordnung zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten präzisiert und es könnte darin festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, ob es sich bei dem Verantwortlichen, der eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder, sofern dies durch das öffentliche Interesse einschließlich gesundheitlicher Zwecke, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, gerechtfertigt ist, eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln sollte.

(46)Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.

(47)Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht

überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

(48) Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.

(49) Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams — CERT, beziehungsweise Computer Security Incident Response Teams — CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

(50) Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.
Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem

Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

(51) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs „rassische Herkunft“ in dieser Verordnung nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist. Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.

(52) Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien von personenbezogenen Daten sollten auch erlaubt sein, wenn sie im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen sind, und — vorbehaltlich angemessener Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte — wenn dies durch das öffentliche Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Eine solche Ausnahme kann zu gesundheitlichen Zwecken gemacht werden, wie der Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll, oder wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient. Die Verarbeitung solcher personenbezogener Daten sollte zudem ausnahmsweise erlaubt sein, wenn sie erforderlich ist, um rechtliche Ansprüche, sei es in einem Gerichtsverfahren oder in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, geltend zu machen, auszuüben oder zu verteidigen.

(53) Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und

Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse harmonisieren, insbesondere wenn die Verarbeitung dieser Daten für gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und angemessene Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden. Den Mitgliedstaaten sollte gestattet werden, weitere Bedingungen — einschließlich Beschränkungen — in Bezug auf die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten beizubehalten oder einzuführen. Dies sollte jedoch den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten.

(54) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.

(55) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.

(56) Wenn es in einem Mitgliedstaat das Funktionieren des demokratischen Systems erfordert, dass die politischen Parteien im Zusammenhang mit Wahlen personenbezogene Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern geeignete Garantien vorgesehen werden.

(57) Kann der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren. Allerdings sollte er sich nicht weigern, zusätzliche Informationen entgegenzunehmen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen. Die Identifizierung sollte die digitale Identifizierung einer betroffenen Person — beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden — einschließen.

(58) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

(59) Es sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung der Rechte, die ihr nach dieser Verordnung zustehen, erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantra-

gen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, insbesondere wenn die personenbezogenen Daten elektronisch verarbeitet werden. Der Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person unverzüglich, spätestens aber innerhalb eines Monats zu beantworten und gegebenenfalls zu begründen, warum er den Antrag ablehnt.

(60) Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Darüber hinaus sollte er die betroffene Person darauf hinweisen, dass Profiling stattfindet und welche Folgen dies hat. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Die betreffenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, so sollten sie maschinenlesbar sein.

(61) Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung mitgeteilt werden oder, falls die Daten nicht von ihr, sondern aus einer anderen Quelle erlangt werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die personenbezogenen Daten rechtmäßig einem anderen Empfänger offengelegt werden dürfen, sollte die betroffene Person bei der erstmaligen Offenlegung der personenbezogenen Daten für diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck zu verarbeiten als den, für den die Daten erhoben wurden, so sollte er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und andere erforderliche Informationen zur Verfügung stellen. Konnte der betroffenen Person nicht mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.

(62) Die Pflicht, Informationen zur Verfügung zu stellen, erübrigt sich jedoch, wenn die betroffene Person die Information bereits hat, wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist. Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein. Als Anhaltspunkte sollten dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien in Betracht gezogen werden.

(63) Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

(64) Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-

Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.

(65) Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein „Recht auf Vergessenwerden“, wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten — insbesondere die im Internet gespeicherten — später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist. Die weitere Speicherung der personenbezogenen Daten sollte jedoch rechtmäßig sein, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

(66) Um dem „Recht auf Vergessenwerden“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen — auch technischer Art — treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.

(67) Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentliche Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden.

(68) Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als ihrer Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist. Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen. Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfül-

lung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden.

(69) Dürfen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt — die dem Verantwortlichen übertragen wurde, — oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sich aus ihrer besonderen Situation ergebenden personenbezogenen Daten einzulegen. Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.

(70) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so sollte die betroffene Person jederzeit unentgeltlich insoweit Widerspruch gegen eine solche — ursprüngliche oder spätere — Verarbeitung einschließlich des Profilings einlegen können, als sie mit dieser Direktwerbung zusammenhängt. Die betroffene Person sollte ausdrücklich auf dieses Recht hingewiesen werden; dieser Hinweis sollte in einer verständlichen und von anderen Informationen getrennten Form erfolgen.

(71) Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling“, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich des Profilings, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der Institutionen der Union oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung. Diese Maßnahme sollte kein Kind betreffen.

Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben. Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.

(72) Das Profiling unterliegt den Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten, wie etwa die Rechtsgrundlage für die Verarbeitung oder die Datenschutzgrundsätze. Der durch diese Verordnung eingerichtete Europäische Datenschutzausschuss (im Folgenden „Ausschuss“) sollte, diesbezüglich Leitlinien herausgeben können.

(73)Im Recht der Union oder der Mitgliedstaaten können Beschränkungen hinsichtlich bestimmter Grundsätze und hinsichtlich des Rechts auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, des Rechts auf Datenübertragbarkeit und Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person und bestimmten damit zusammenhängenden Pflichten der Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, die Verhütung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung — was auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt — oder die Verhütung, Aufdeckung und Verfolgung von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen, das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses sowie die Weiterverarbeitung von archivierten personenbezogenen Daten zur Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen gehört, und zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen soziale Sicherheit, öffentliche Gesundheit und humanitäre Hilfe, zu schützen. Diese Beschränkungen sollten mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

(74)Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

(75)Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

(76)Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

(77)Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Ausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Ausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.

(78)Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten

natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

(79) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es — auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden — einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.

(80) Jeder Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf betroffene Personen beziehen, die sich in der Union aufhalten, und dazu dienen, diesen Personen in der Union Waren oder Dienstleistungen anzubieten — unabhängig davon, ob von der betroffenen Person eine Zahlung verlangt wird — oder deren Verhalten, soweit dieses innerhalb der Union erfolgt, zu beobachten, sollte einen Vertreter benennen müssen, es sei denn, die Verarbeitung erfolgt gelegentlich, schließt nicht die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ein und bringt unter Berücksichtigung ihrer Art, ihrer Umstände, ihres Umfangs und ihrer Zwecke wahrscheinlich kein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich oder bei dem Verantwortlichen handelt es sich um eine Behörde oder öffentliche Stelle. Der Vertreter sollte im Namen des Verantwortlichen oder des Auftragsverarbeiters tätig werden und den Aufsichtsbehörden als Anlaufstelle dienen. Der Verantwortliche oder der Auftragsverarbeiter sollte den Vertreter ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln. Die Benennung eines solchen Vertreters berührt nicht die Verantwortung oder Haftung des Verantwortlichen oder des Auftragsverarbeiters nach Maßgabe dieser Verordnung. Ein solcher Vertreter sollte seine Aufgaben entsprechend dem Mandat des Verantwortlichen oder Auftragsverarbeiters ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des Verantwortlichen oder Auftragsverarbeiters sollte der bestellte Vertreter Durchsetzungsverfahren unterworfen werden.

(81) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die — insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen — hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen — auch für die Sicherheit der Verarbeitung — getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen

oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(82) Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

(83) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau — auch hinsichtlich der Vertraulichkeit — gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

(84) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

(85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(86) Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt

sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

(87)Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.

(88)Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde.

(89)Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen gehören insbesondere solche, bei denen neue Technologien eingesetzt werden oder die neuartig sind und bei denen der Verantwortliche noch keine Datenschutz-Folgenabschätzung durchgeführt hat bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine Datenschutz-Folgenabschätzung notwendig geworden ist.

(90)In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

(91)Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

(92)Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig

sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.

(93) Anlässlich des Erlasses des Gesetzes des Mitgliedstaats, auf dessen Grundlage die Behörde oder öffentliche Stelle ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt, können die Mitgliedstaaten es für erforderlich erachten, solche Folgeabschätzungen vor den Verarbeitungsvorgängen durchzuführen.

(94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.

(95) Der Auftragsverarbeiter sollte erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.

(96) Eine Konsultation der Aufsichtsbehörde sollte auch während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften, in denen eine Verarbeitung personenbezogener Daten vorgesehen ist, erfolgen, um die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.

(97) In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

(98) Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Insbesondere könnten in diesen Verhaltensregeln — unter Berücksichtigung des mit der Verarbeitung wahrscheinlich einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen — die Pflichten der Verantwortlichen und der Auftragsverarbeiter bestimmt werden.

(99) Bei der Ausarbeitung oder bei der Änderung oder Erweiterung solcher Verhaltensregeln sollten Verbände

und oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, die maßgeblichen Interessenträger, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.

(100)Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

(101)Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

(102)Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt. Die Mitgliedstaaten können völkerrechtliche Übereinkünfte schließen, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen beinhalten, sofern sich diese Übereinkünfte weder auf diese Verordnung noch auf andere Bestimmungen des Unionsrechts auswirken und ein angemessenes Schutzniveau für die Grundrechte der betroffenen Personen umfassen.

(103)Die Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, und auf diese Weise in Bezug auf das Drittland oder die internationale Organisation, das bzw. die für fähig gehalten wird, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Die Kommission kann, nach Abgabe einer ausführlichen Erklärung, in der dem Drittland oder der internationalen Organisation eine Begründung gegeben wird, auch entscheiden, eine solche Feststellung zu widerrufen.

(104)In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlands oder eines Gebiets oder eines bestimmten Sektors eines Drittlands berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, der Rechtsweg gewährleistet ist und die internationalen Menschenrechtsnormen und -standards eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor eines Drittlands sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmter Verarbeitungsvorgänge und des Anwendungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen personenbezogene Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden.

(105)Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, die Verpflichtungen, die sich aus der Teilnahme des Drittlands oder der in-

ternationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des Drittlands zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Ausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.

(106) Die Kommission sollte die Wirkungsweise von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem bestimmten Sektor eines Drittlands oder einer internationalen Organisation überwachen; sie sollte auch die Wirkungsweise der Feststellungen, die auf der Grundlage des Artikels 25 Absatz 6 oder des Artikels 26 Absatz 4 der Richtlinie 95/46/EG erlassen werden, überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung von deren Wirkungsweise vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen. Für die Zwecke der Überwachung und der Durchführung der regelmäßigen Überprüfungen sollte die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments und des Rates sowie der anderen einschlägigen Stellen und Quellen berücksichtigen. Die Kommission sollte innerhalb einer angemessenen Frist die Wirkungsweise der letztgenannten Beschlüsse bewerten und dem durch diese Verordnung eingesetzten Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates (12) sowie dem Europäischen Parlament und dem Rat über alle maßgeblichen Feststellungen Bericht erstatten.

(107) Die Kommission kann feststellen, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Verordnung in Bezug auf die Datenübermittlung vorbehaltlich geeigneter Garantien, einschließlich verbindlicher interner Datenschutzvorschriften und auf Ausnahmen für bestimmte Fälle werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

(108) Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen. Datenübermittlungen dürfen auch von Behörden oder öffentlichen Stellen an Behörden oder öffentliche Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen — wie beispielsweise einer gemeinsamen Absichtserklärung –, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden, aufzunehmen sind. Die Genehmigung der zuständigen Aufsichtsbehörde sollte erlangt werden, wenn die Garantien in nicht rechtsverbindlichen Verwaltungsvereinbarungen vorgesehen sind.

(109) Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.

(110)Jede Unternehmensgruppe oder jede Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sollte für ihre internationalen Datenübermittlungen aus der Union an Organisationen derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, genehmigte verbindliche interne Datenschutzvorschriften anwenden dürfen, sofern diese sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.

(111)Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat, wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Verfahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist. Die Übermittlung sollte zudem möglich sein, wenn sie zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaats festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn sie aus einem durch Rechtsvorschriften vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In letzterem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.

(112)Diese Ausnahmen sollten insbesondere für Datenübermittlungen gelten, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. Die Übermittlung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein Interesse, das für die lebenswichtigen Interessen — einschließlich der körperlichen Unversehrtheit oder des Lebens — der betroffenen Person oder einer anderen Person wesentlich ist, zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben. Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten sollten solche Bestimmungen der Kommission mitteilen. Jede Übermittlung personenbezogener Daten einer betroffenen Person, die aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen, an eine internationale humanitäre Organisation, die erfolgt, um eine nach den Genfer Konventionen obliegende Aufgabe auszuführen oder um dem in bewaffneten Konflikten anwendbaren humanitären Völkerrecht nachzukommen, könnte als aus einem wichtigen Grund im öffentlichen Interesse notwendig oder als im lebenswichtigen Interesse der betroffenen Person liegend erachtet werden.

(113)Übermittlungen, die als nicht wiederholt erfolgend gelten können und nur eine begrenzte Zahl von betroffenen Personen betreffen, könnten auch zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der Verantwortliche sämtliche Umstände der Datenübermittlung geprüft hat. Der Verantwortliche sollte insbesondere die Art der personenbezogenen Daten, den Zweck und die Dauer der vorgesehenen Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland berücksichtigen und angemessene Garantien zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogener Daten vorsehen. Diese Übermittlungen sollten nur in den verbleibenden Fällen möglich sein, in denen keiner der anderen Gründe für die Übermittlung anwendbar ist. Bei wissenschaftlichen oder historischen Forschungszwecken oder bei statistischen Zwecken sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Der Verantwortliche sollte die Aufsichtsbehörde und die betroffene Person von der Übermittlung in Kenntnis setzen.

(114)In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Datenschutzniveaus vorliegt, sollte der Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten in der Union nach der Übermittlung dieser Daten eingeräumt werden, damit sie weiterhin die Grundrechte und Garantien genießen können.

(115)Manche Drittländer erlassen Gesetze, Vorschriften und sonstige Rechtsakte, die vorgeben, die Verarbei-

tungstätigkeiten natürlicher und juristischer Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar zu regeln. Dies kann Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden in Drittländern umfassen, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird und die nicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets der betreffenden Drittländer kann gegen internationales Recht verstoßen und dem durch diese Verordnung in der Union gewährleisteten Schutz natürlicher Personen zuwiderlaufen. Datenübermittlungen sollten daher nur zulässig sein, wenn die Bedingungen dieser Verordnung für Datenübermittlungen an Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Offenlegung aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt ist.

(116) Wenn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, besteht eine erhöhte Gefahr, dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können und sich insbesondere gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, widersprüchliche Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. Um Mechanismen der internationalen Zusammenarbeit zu entwickeln, die die internationale Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtern und sicherstellen, sollten die Kommission und die Aufsichtsbehörden Informationen austauschen und bei Tätigkeiten, die mit der Ausübung ihrer Befugnisse in Zusammenhang stehen, mit den zuständigen Behörden der Drittländer nach dem Grundsatz der Gegenseitigkeit und gemäß dieser Verordnung zusammenarbeiten.

(117) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die befugt sind, ihre Aufgaben und Befugnisse völlig unabhängig wahrzunehmen, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde errichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.

(118) Die Tatsache, dass die Aufsichtsbehörden unabhängig sind, sollte nicht bedeuten, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden bzw. sie keiner gerichtlichen Überprüfung unterzogen werden können.

(119) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er mittels Rechtsvorschriften sicherstellen, dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Ausschuss und der Kommission gewährleistet.

(120) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, einschließlich derer im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über einen eigenen, öffentlichen, jährlichen Haushaltsplan verfügen, der Teil des gesamten Staatshaushalts oder nationalen Haushalts sein kann.

(121) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Rechtsvorschriften von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder im Wege eines transparenten Verfahrens entweder — auf Vorschlag der Regierung, eines Mitglieds der Regierung, des Parlaments oder einer Parlamentskammer — vom Parlament, der Regierung oder dem Staatsoberhaupt des Mitgliedstaats oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder ihr Amt integer ausüben, von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben. Die Aufsichtsbehörde sollte über eigenes Personal verfügen, das sie selbst oder eine nach dem Recht des Mitgliedstaats eingerichtete unabhängige Stelle auswählt und das ausschließlich der Leitung des Mitglieds oder der Mitglieder der Aufsichtsbehörde

unterstehen sollte.

(122)Jede Aufsichtsbehörde sollte dafür zuständig sein, im Hoheitsgebiet ihres Mitgliedstaats die Befugnisse auszuüben und die Aufgaben zu erfüllen, die ihr mit dieser Verordnung übertragen wurden. Dies sollte insbesondere für Folgendes gelten: die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen oder Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats, die Verarbeitung personenbezogener Daten durch Behörden oder private Stellen, die im öffentlichen Interesse handeln, Verarbeitungstätigkeiten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben, oder Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Union, sofern sie auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet sind. Dies sollte auch die Bearbeitung von Beschwerden einer betroffenen Person, die Durchführung von Untersuchungen über die Anwendung dieser Verordnung sowie die Förderung der Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließen.

(123)Die Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen im Hinblick auf die Verarbeitung ihrer Daten zu schützen und den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern. Zu diesem Zweck sollten die Aufsichtsbehörden untereinander und mit der Kommission zusammenarbeiten, ohne dass eine Vereinbarung zwischen den Mitgliedstaaten über die Leistung von Amtshilfe oder über eine derartige Zusammenarbeit erforderlich wäre.

(124)Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte — im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung — insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.

(125)Die federführende Behörde sollte berechtigt sein, verbindliche Beschlüsse über Maßnahmen zu erlassen, mit denen die ihr gemäß dieser Verordnung übertragenen Befugnisse ausgeübt werden. In ihrer Eigenschaft als federführende Behörde sollte diese Aufsichtsbehörde für die enge Einbindung und Koordinierung der betroffenen Aufsichtsbehörden im Entscheidungsprozess sorgen. Wird beschlossen, die Beschwerde der betroffenen Person vollständig oder teilweise abzuweisen, so sollte dieser Beschluss von der Aufsichtsbehörde angenommen werden, bei der die Beschwerde eingelegt wurde.

(126)Der Beschluss sollte von der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden gemeinsam vereinbart werden und an die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters gerichtet sein und für den Verantwortlichen und den Auftragsverarbeiter verbindlich sein. Der Verantwortliche oder Auftragsverarbeiter sollte die erforderlichen Maßnahmen treffen, um die Einhaltung dieser Verordnung und die Umsetzung des Beschlusses zu gewährleisten, der der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters im Hinblick auf die Verarbeitungstätigkeiten in der Union von der federführenden Aufsichtsbehörde mitgeteilt wurde.

(127)Jede Aufsichtsbehörde, die nicht als federführende Aufsichtsbehörde fungiert, sollte in örtlichen Fällen zuständig sein, wenn der Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, der Gegenstand der spezifischen Verarbeitung aber nur die Verarbeitungstätigkeiten in einem einzigen Mitgliedstaat und nur betroffene Personen in diesem einen Mitgliedstaat betrifft, beispielsweise wenn es um die Verarbeitung von personenbezogenen Daten von Arbeitnehmern im spezifischen Beschäftigungskontext eines Mitgliedstaats geht. In solchen Fällen sollte die Aufsichtsbehörde unverzüg-

lich die federführende Aufsichtsbehörde über diese Angelegenheit unterrichten. Nach ihrer Unterrichtung sollte die federführende Aufsichtsbehörde entscheiden, ob sie den Fall nach den Bestimmungen zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden gemäß der Vorschrift zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden (im Folgenden „Verfahren der Zusammenarbeit und Kohärenz“) regelt oder ob die Aufsichtsbehörde, die sie unterrichtet hat, den Fall auf örtlicher Ebene regeln sollte. Dabei sollte die federführende Aufsichtsbehörde berücksichtigen, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat, damit Beschlüsse gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter wirksam durchgesetzt werden. Entscheidet die federführende Aufsichtsbehörde, den Fall selbst zu regeln, sollte die Aufsichtsbehörde, die sie unterrichtet hat, die Möglichkeit haben, einen Beschlussentwurf vorzulegen, dem die federführende Aufsichtsbehörde bei der Ausarbeitung ihres Beschlussentwurfs im Rahmen dieses Verfahrens der Zusammenarbeit und Kohärenz weitestgehend Rechnung tragen sollte.

(128) Die Vorschriften über die federführende Behörde und das Verfahren der Zusammenarbeit und Kohärenz sollten keine Anwendung finden, wenn die Verarbeitung durch Behörden oder private Stellen im öffentlichen Interesse erfolgt. In diesen Fällen sollte die Aufsichtsbehörde des Mitgliedstaats, in dem die Behörde oder private Einrichtung ihren Sitz hat, die einzige Aufsichtsbehörde sein, die dafür zuständig ist, die Befugnisse auszuüben, die ihr mit dieser Verordnung übertragen wurden.

(129) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter, insbesondere im Fall von Beschwerden natürlicher Personen, Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse und Genehmigungsbefugnisse und beratende Befugnisse, sowie — unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten — die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Gerichtsverfahren anzustrengen. Dazu sollte auch die Befugnis zählen, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Die Mitgliedstaaten können andere Aufgaben im Zusammenhang mit dem Schutz personenbezogener Daten im Rahmen dieser Verordnung festlegen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Verordnung geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Verfahrensrecht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Jede rechtsverbindliche Maßnahme der Aufsichtsbehörde sollte schriftlich erlassen werden und sie sollte klar und eindeutig sein; die Aufsichtsbehörde, die die Maßnahme erlassen hat, und das Datum, an dem die Maßnahme erlassen wurde, sollten angegeben werden und die Maßnahme sollte vom Leiter oder von einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein und eine Begründung für die Maßnahme sowie einen Hinweis auf das Recht auf einen wirksamen Rechtsbehelf enthalten. Dies sollte zusätzliche Anforderungen nach dem Verfahrensrecht der Mitgliedstaaten nicht ausschließen. Der Erlass eines rechtsverbindlichen Beschlusses setzt voraus, dass er in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, gerichtlich überprüft werden kann.

(130) Ist die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, nicht die federführende Aufsichtsbehörde, so sollte die federführende Aufsichtsbehörde gemäß den Bestimmungen dieser Verordnung über Zusammenarbeit und Kohärenz eng mit der Aufsichtsbehörde zusammenarbeiten, bei der die Beschwerde eingereicht wurde. In solchen Fällen sollte die federführende Aufsichtsbehörde bei Maßnahmen, die rechtliche Wirkungen entfalten sollen, unter anderem bei der Verhängung von Geldbußen, den Standpunkt der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde und die weiterhin befugt sein sollte, in Abstimmung mit der zuständigen Aufsichtsbehörde Untersuchungen im Hoheitsgebiet ihres eigenen Mitgliedstaats durchzuführen, weitestgehend berücksichtigen.

(131) Wenn eine andere Aufsichtsbehörde als federführende Aufsichtsbehörde für die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters fungieren sollte, der konkrete Gegenstand einer Beschwerde oder der mögliche Verstoß jedoch nur die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters in dem Mitgliedstaat betrifft, in dem die Beschwerde eingereicht wurde oder der mögliche Verstoß aufgedeckt wurde, und die Angelegenheit keine erheblichen Auswirkungen auf betroffe-

ne Personen in anderen Mitgliedstaaten hat oder haben dürfte, sollte die Aufsichtsbehörde, bei der eine Beschwerde eingereicht wurde oder die Situationen, die mögliche Verstöße gegen diese Verordnung darstellen, aufgedeckt hat bzw. auf andere Weise darüber informiert wurde, versuchen, eine gütliche Einigung mit dem Verantwortlichen zu erzielen; falls sich dies als nicht erfolgreich erweist, sollte sie die gesamte Bandbreite ihrer Befugnisse wahrnehmen. Dies sollte auch Folgendes umfassen: die spezifische Verarbeitung im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde oder im Hinblick auf betroffene Personen im Hoheitsgebiet dieses Mitgliedstaats; die Verarbeitung im Rahmen eines Angebots von Waren oder Dienstleistungen, das speziell auf betroffene Personen im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde ausgerichtet ist; oder eine Verarbeitung, die unter Berücksichtigung der einschlägigen rechtlichen Verpflichtungen nach dem Recht der Mitgliedstaaten bewertet werden muss.

(132) Auf die Öffentlichkeit ausgerichtete Sensibilisierungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, und an natürliche Personen, insbesondere im Bildungsbereich, richten.

(133) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist. Eine Aufsichtsbehörde, die um Amtshilfe ersucht hat, kann eine einstweilige Maßnahme erlassen, wenn sie nicht binnen eines Monats nach Eingang des Amtshilfeersuchens bei der ersuchten Aufsichtsbehörde eine Antwort von dieser erhalten hat.

(134) Jede Aufsichtsbehörde sollte gegebenenfalls an gemeinsamen Maßnahmen von anderen Aufsichtsbehörden teilnehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer bestimmten Frist antworten müssen.

(135) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) für die Zusammenarbeit zwischen den Aufsichtsbehörden eingeführt werden. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme zu erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragt, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Dieses Verfahren sollte andere Maßnahmen, die die Kommission möglicherweise in Ausübung ihrer Befugnisse nach den Verträgen trifft, unberührt lassen.

(136) Bei Anwendung des Kohärenzverfahrens sollte der Ausschuss, falls von der Mehrheit seiner Mitglieder so entschieden wird oder falls eine andere betroffene Aufsichtsbehörde oder die Kommission darum ersuchen, binnen einer festgelegten Frist eine Stellungnahme abgeben. Dem Ausschuss sollte auch die Befugnis übertragen werden, bei Streitigkeiten zwischen Aufsichtsbehörden rechtsverbindliche Beschlüsse zu erlassen. Zu diesem Zweck sollte er in klar bestimmten Fällen, in denen die Aufsichtsbehörden insbesondere im Rahmen des Verfahrens der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden widersprüchliche Standpunkte zu dem Sachverhalt, vor allem in der Frage, ob ein Verstoß gegen diese Verordnung vorliegt, vertreten, grundsätzlich mit einer Mehrheit von zwei Dritteln seiner Mitglieder rechtsverbindliche Beschlüsse erlassen.

(137) Es kann dringender Handlungsbedarf zum Schutz der Rechte und Freiheiten von betroffenen Personen bestehen, insbesondere wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht. Eine Aufsichtsbehörde sollte daher hinreichend begründete einstweilige Maßnahmen in ihrem Hoheitsgebiet mit einer festgelegten Geltungsdauer von höchstens drei Monaten erlassen können.

(138) Die Anwendung dieses Verfahrens sollte in den Fällen, in denen sie verbindlich vorgeschrieben ist, eine Bedingung für die Rechtmäßigkeit einer Maßnahme einer Aufsichtsbehörde sein, die rechtliche Wirkungen entfalten soll. In anderen Fällen von grenzüberschreitender Relevanz sollte das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden zur Anwendung gelangen, und die betroffenen Aufsichtsbehörden können auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen, ohne auf das Kohärenzverfahren zurückzugreifen.

(139) Zur Förderung der einheitlichen Anwendung dieser Verordnung sollte der Ausschuss als unabhängige Einrichtung der Union eingesetzt werden. Damit der Ausschuss seine Ziele erreichen kann, sollte er Rechtspersönlichkeit besitzen. Der Ausschuss sollte von seinem Vorsitz vertreten werden. Er sollte die mit der Richt-

linie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten ersetzen. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder deren jeweiligen Vertretern gebildet werden. An den Beratungen des Ausschusses sollte die Kommission ohne Stimmrecht teilnehmen und der Europäische Datenschutzbeauftragte sollte spezifische Stimmrechte haben. Der Ausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission insbesondere im Hinblick auf das Schutzniveau in Drittländern oder internationalen Organisationen beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Ausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.

(140) Der Ausschusssollte von einem Sekretariat unterstützt werden, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird. Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, sollte diese Aufgaben ausschließlich gemäß den Anweisungen des Vorsitzes des Ausschusses durchführen und diesem Bericht erstatten.

(141) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, sollte die betroffene Person über den Zwischenstand informiert werden. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(142) Betroffene Personen, die sich in ihren Rechten gemäß dieser Verordnung verletzt sehen, sollten das Recht haben, nach dem Recht eines Mitgliedstaats gegründete Einrichtungen, Organisationen oder Verbände ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes personenbezogener Daten tätig sind, zu beauftragen, in ihrem Namen Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder das Recht auf Schadensersatz in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. Die Mitgliedstaaten können vorsehen, dass diese Einrichtungen, Organisationen oder Verbände das Recht haben, unabhängig vom Auftrag einer betroffenen Person in dem betreffenden Mitgliedstaat eine eigene Beschwerde einzulegen, und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf haben sollten, wenn sie Grund zu der Annahme haben, dass die Rechte der betroffenen Person infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung verletzt worden sind. Diesen Einrichtungen, Organisationen oder Verbänden kann unabhängig vom Auftrag einer betroffenen Person nicht gestattet werden, im Namen einer betroffenen Person Schadenersatz zu verlangen.

(143) Jede natürliche oder juristische Person hat das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof eine Klage auf Nichtigerklärung eines Beschlusses des Ausschusses zu erheben. Als Adressaten solcher Beschlüsse müssen die betroffenen Aufsichtsbehörden, die diese Beschlüsse anfechten möchten, binnen zwei Monaten nach deren Übermittlung gemäß Artikel 263 AEUV Klage erheben. Sofern Beschlüsse des Ausschusses einen Verantwortlichen, einen Auftragsverarbeiter oder den Beschwerdeführer unmittelbar und individuell betreffen, so können diese Personen binnen zwei Monaten nach Veröffentlichung der betreffenden Beschlüsse auf der Website des Ausschusses im Einklang mit Artikel 263 AEUV eine Klage auf Nichtigerklärung erheben. Unbeschadet dieses Rechts nach Artikel 263 AEUV sollte jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Das Recht auf einen wirksamen gerichtlichen Rechtsbehelf umfasst jedoch nicht rechtlich nicht bindende Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Verfahrensrecht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den bei ihnen anhängigen Rechts-

streit maßgebliche Sach- und Rechtsfragen zu prüfen, einschließt. Wurde eine Beschwerde von einer Aufsichtsbehörde abgelehnt oder abgewiesen, kann der Beschwerdeführer Klage bei den Gerichten desselben Mitgliedstaats erheben.

Im Zusammenhang mit gerichtlichen Rechtsbehelfen in Bezug auf die Anwendung dieser Verordnung können einzelstaatliche Gerichte, die eine Entscheidung über diese Frage für erforderlich halten, um ihr Urteil erlassen zu können, bzw. müssen einzelstaatliche Gerichte in den Fällen nach Artikel 267 AEUV den Gerichtshof um eine Vorabentscheidung zur Auslegung des Unionsrechts — das auch diese Verordnung einschließt — ersuchen. Wird darüber hinaus der Beschluss einer Aufsichtsbehörde zur Umsetzung eines Beschlusses des Ausschusses vor einem einzelstaatlichen Gericht angefochten und wird die Gültigkeit des Beschlusses des Ausschusses in Frage gestellt, so hat dieses einzelstaatliche Gericht nicht die Befugnis, den Beschluss des Ausschusses für nichtig zu erklären, sondern es muss im Einklang mit Artikel 267 AEUV in der Auslegung des Gerichtshofs den Gerichtshof mit der Frage der Gültigkeit befassen, wenn es den Beschluss für nichtig hält. Allerdings darf ein einzelstaatliches Gericht den Gerichtshof nicht auf Anfrage einer natürlichen oder juristischen Person mit Fragen der Gültigkeit des Beschlusses des Ausschusses befassen, wenn diese Person Gelegenheit hatte, eine Klage auf Nichtigerklärung dieses Beschlusses zu erheben — insbesondere wenn sie unmittelbar und individuell von dem Beschluss betroffen war –, diese Gelegenheit jedoch nicht innerhalb der Frist gemäß Artikel 263 AEUV genutzt hat.

(144) Hat ein mit einem Verfahren gegen die Entscheidung einer Aufsichtsbehörde befasstes Gericht Anlass zu der Vermutung, dass ein dieselbe Verarbeitung betreffendes Verfahren — etwa zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter oder wegen desselben Anspruchs — vor einem zuständigen Gericht in einem anderen Mitgliedstaat anhängig ist, so sollte es mit diesem Gericht Kontakt aufnehmen, um sich zu vergewissern, dass ein solches verwandtes Verfahren existiert. Sind verwandte Verfahren vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene Gericht das Verfahren aussetzen oder sich auf Anfrage einer Partei auch zugunsten des zuerst angerufenen Gerichts für unzuständig erklären, wenn dieses später angerufene Gericht für die betreffenden Verfahren zuständig ist und die Verbindung von solchen verwandten Verfahren nach seinem Recht zulässig ist. Verfahren gelten als miteinander verwandt, wenn zwischen ihnen eine so enge Beziehung gegeben ist, dass eine gemeinsame Verhandlung und Entscheidung geboten erscheint, um zu vermeiden, dass in getrennten Verfahren einander widersprechende Entscheidungen ergehen.

(145) Bei Verfahren gegen Verantwortliche oder Auftragsverarbeiter sollte es dem Kläger überlassen bleiben, ob er die Gerichte des Mitgliedstaats anruft, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder des Mitgliedstaats, in dem die betroffene Person ihren Aufenthaltsort hat; dies gilt nicht, wenn es sich bei dem Verantwortlichen um eine Behörde eines Mitgliedstaats handelt, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

(146) Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.

(147) Soweit in dieser Verordnung spezifische Vorschriften über die Gerichtsbarkeit — insbesondere in Bezug auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter — enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des

Rates enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.

(148)Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(149)Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, festlegen können. Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.

(150)Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.

(151)Nach den Rechtsordnungen Dänemarks und Estlands sind die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig. Die Vorschriften über die Geldbußen können so angewandt werden, dass die Geldbuße in Dänemark durch die zuständigen nationalen Gerichte als Strafe und in Estland durch die Aufsichtsbehörde im Rahmen eines Verfahrens bei Vergehen verhängt wird, sofern eine solche Anwendung der Vorschriften in diesen Mitgliedstaaten die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen hat. Daher sollten die zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen. In jeden Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.

(152)Soweit diese Verordnung verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen diese Verordnung — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht. Es sollte im Recht der Mitgliedstaaten geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.

(153)Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftli-

chen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und Kohärenz und besondere Datenverarbeitungssituationen erlassen. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das Recht des Mitgliedstaats angewendet werden, dem der Verantwortliche unterliegt. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.

(154) Diese Verordnung ermöglicht es, dass bei ihrer Anwendung der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten berücksichtigt wird. Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden. Personenbezogene Daten in Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Stelle befinden, sollten von dieser Behörde oder Stelle öffentlich offengelegt werden können, sofern dies im Unionsrecht oder im Recht der Mitgliedstaaten, denen sie unterliegt, vorgesehen ist. Diese Rechtsvorschriften sollten den Zugang der Öffentlichkeit zu amtlichen Dokumenten und die Weiterverwendung von Informationen des öffentlichen Sektors mit dem Recht auf Schutz personenbezogener Daten in Einklang bringen und können daher die notwendige Übereinstimmung mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung regeln. Die Bezugnahme auf Behörden und öffentliche Stellen sollte in diesem Kontext sämtliche Behörden oder sonstigen Stellen beinhalten, die vom Recht des jeweiligen Mitgliedstaats über den Zugang der Öffentlichkeit zu Dokumenten erfasst werden. Die Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates (14) lässt das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des Rechts der Mitgliedstaaten unberührt und beeinträchtigt diesen in keiner Weise, und sie bewirkt insbesondere keine Änderung der in dieser Verordnung dargelegten Rechte und Pflichten. Insbesondere sollte die genannte Richtlinie nicht für Dokumente gelten, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nicht oder nur eingeschränkt zugänglich sind, oder für Teile von Dokumenten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, bei denen Rechtsvorschriften vorsehen, dass ihre Weiterverwendung nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist.

(155) Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

(156) Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken sollte geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung unterliegen. Mit diesen Garantien sollte sichergestellt werden, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere der Grundsatz der Datenminimierung gewährleistet wird. Die Weiterverarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt erst dann, wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen (wie z. B. die Pseudonymisierung von personenbezogenen Daten). Die Mitgliedstaaten sollten geeignete Garantien in Bezug auf die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorsehen. Es sollte den Mitgliedstaaten erlaubt sein, unter bestimmten Be-

dingungen und vorbehaltlich geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen in Bezug auf die Informationsanforderungen sowie der Rechte auf Berichtigung, Löschung, Vergessenwerden, zur Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie auf Widerspruch bei der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorzusehen. Im Rahmen der betreffenden Bedingungen und Garantien können spezifische Verfahren für die Ausübung dieser Rechte durch die betroffenen Personen vorgesehen sein — sofern dies angesichts der mit der spezifischen Verarbeitung verfolgten Zwecke angemessen ist — sowie technische und organisatorische Maßnahmen zur Minimierung der Verarbeitung personenbezogener Daten im Hinblick auf die Grundsätze der Verhältnismäßigkeit und der Notwendigkeit. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken sollte auch anderen einschlägigen Rechtsvorschriften, beispielsweise für klinische Prüfungen, genügen.

(157)Durch die Verknüpfung von Informationen aus Registern können Forscher neue Erkenntnisse von großem Wert in Bezug auf weit verbreiteten Krankheiten wie Herz-Kreislauferkrankungen, Krebs und Depression erhalten. Durch die Verwendung von Registern können bessere Forschungsergebnisse erzielt werden, da sie auf einen größeren Bevölkerungsanteil gestützt sind. Im Bereich der Sozialwissenschaften ermöglicht die Forschung anhand von Registern es den Forschern, entscheidende Erkenntnisse über den langfristigen Zusammenhang einer Reihe sozialer Umstände zu erlangen, wie Arbeitslosigkeit und Bildung mit anderen Lebensumständen. Durch Register erhaltene Forschungsergebnisse bieten solide, hochwertige Erkenntnisse, die die Basis für die Erarbeitung und Umsetzung wissensgestützter politischer Maßnahmen darstellen, die Lebensqualität zahlreicher Menschen verbessern und die Effizienz der Sozialdienste verbessern können. Zur Erleichterung der wissenschaftlichen Forschung können daher personenbezogene Daten zu wissenschaftlichen Forschungszwecken verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt sind.

(158)Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu Archivzwecken gelten, wobei darauf hinzuweisen ist, dass die Verordnung nicht für verstorbene Personen gelten sollte. Behörden oder öffentliche oder private Stellen, die Aufzeichnungen von öffentlichem Interesse führen, sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sein, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen. Es sollte den Mitgliedstaaten ferner erlaubt sein vorzusehen, dass personenbezogene Daten zu Archivzwecken weiterverarbeitet werden, beispielsweise im Hinblick auf die Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen, Völkermord, Verbrechen gegen die Menschlichkeit, insbesondere dem Holocaust, und Kriegsverbrechen.

(159)Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gelten. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Darüber hinaus sollte sie dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken zu genügen, sollten spezifische Bedingungen insbesondere hinsichtlich der Veröffentlichung oder sonstigen Offenlegung personenbezogener Daten im Kontext wissenschaftlicher Zwecke gelten. Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten.

(160)Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu historischen Forschungszwecken gelten. Dazu sollte auch historische Forschung und Forschung im Bereich der Genealogie zählen, wobei darauf hinzuweisen ist, dass diese Verordnung nicht für verstorbene Personen gelten sollte.

(161)Für die Zwecke der Einwilligung in die Teilnahme an wissenschaftlichen Forschungstätigkeiten im Rahmen klinischer Prüfungen sollten die einschlägigen Bestimmungen der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates gelten.

(162)Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu statistischen Zwecken gelten. Das Unionsrecht oder das Recht der Mitgliedstaaten sollte in den Grenzen dieser Verordnung den statistischen Inhalt, die Zugangskontrolle, die Spezifikationen für die Verarbeitung personenbezogener

Daten zu statistischen Zwecken und geeignete Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Sicherstellung der statistischen Geheimhaltung bestimmen. Unter dem Begriff „statistische Zwecke“ ist jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen. Diese statistischen Ergebnisse können für verschiedene Zwecke, so auch für wissenschaftliche Forschungszwecke, weiterverwendet werden. Im Zusammenhang mit den statistischen Zwecken wird vorausgesetzt, dass die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.

(163) Die vertraulichen Informationen, die die statistischen Behörden der Union und der Mitgliedstaaten zur Erstellung der amtlichen europäischen und der amtlichen nationalen Statistiken erheben, sollten geschützt werden. Die europäischen Statistiken sollten im Einklang mit den in Artikel 338 Absatz 2 AEUV dargelegten statistischen Grundsätzen entwickelt, erstellt und verbreitet werden, wobei die nationalen Statistiken auch mit dem Recht der Mitgliedstaaten übereinstimmen müssen. Die Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates enthält genauere Bestimmungen zur Vertraulichkeit europäischer Statistiken.

(164) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten durch Rechtsvorschriften regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen. Dies berührt nicht die bestehenden Verpflichtungen der Mitgliedstaaten zum Erlass von Vorschriften über das Berufsgeheimnis, wenn dies aufgrund des Unionsrechts erforderlich ist.

(165) Im Einklang mit Artikel 17 AEUV achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.

(166) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen. Delegierte Rechtsakte sollten insbesondere in Bezug auf die für Zertifizierungsverfahren geltenden Kriterien und Anforderungen, die durch standardisierte Bildsymbole darzustellenden Informationen und die Verfahren für die Bereitstellung dieser Bildsymbole erlassen werden. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt. Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission gewährleisten, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat gleichzeitig, rechtzeitig und auf angemessene Weise übermittelt werden.

(167) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden. In diesem Zusammenhang sollte die Kommission besondere Maßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen erwägen.

(168) Für den Erlass von Durchführungsrechtsakten bezüglich Standardvertragsklauseln für Verträge zwischen Verantwortlichen und Auftragsverarbeitern sowie zwischen Auftragsverarbeitern; Verhaltensregeln; technische Standards und Verfahren für die Zertifizierung; Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland, einem Gebiet oder bestimmten Sektor dieses Drittlands oder in einer internationalen Organisation; Standardschutzklauseln; Formate und Verfahren für den Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden im Hinblick auf verbindliche interne Datenschutzvorschriften; Amtshilfe; sowie Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollte das Prüfverfahren angewandt werden.

(169) Die Kommission sollte sofort geltende Durchführungsrechtsakte erlassen, wenn anhand vorliegender Beweise festgestellt wird, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau gewährleistet, und dies aus Gründen äußerster Dringlichkeit erforderlich ist.

(170)Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines gleichwertigen Datenschutzniveaus für natürliche Personen und des freien Verkehrs personenbezogener Daten in der Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(171)Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

(172)Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 7. März 2012 eine Stellungnahme abgegeben.

(173)Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

**KAPITEL I: Allgemeine Bestimmungen (Art. 1-4)**

Artikel 1
Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 2
Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b)durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

d)durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der

Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.
(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3
Räumlicher Anwendungsbereich
(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.
(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Artikel 4
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8.„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9.„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10.„Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

11.„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

12.„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

13.„genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

14.„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

15.„Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

16.„Hauptniederlassung“

a)im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

b)im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

17.„Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

18.„Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

19.„Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

20.„verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;

21.„Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

22.„betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil
a)der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

b)diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23.„grenzüberschreitende Verarbeitung“ entweder
a)eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

b)eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24.„maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25.„Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates;

26.„internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

**KAPITEL II: Grundsätze (Art. 5-11)**

Artikel 5
Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen
a)auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b)für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c)dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d)sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen

zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e)in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f)in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a)Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b)die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c)die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d)die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e)die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f)die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen

ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.
(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem
a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7
Bedingungen für die Einwilligung
(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.
(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Artikel 8
Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.
Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.
(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.
(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

Artikel 9
Verarbeitung besonderer Kategorien personenbezogener Daten
(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.
(2) Absatz 1 gilt nicht in folgenden Fällen:

a)Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b)die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c)die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d)die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e)die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f)die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g)die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h)die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i)die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j)die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 10
Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Artikel 11
Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist
(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.
(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

**KAPITEL III: Rechte der betroffenen Person (Art. 12-23)**

Abschnitt 1
Transparenz und Modalitäten

Artikel 12
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.
(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.
(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.
(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.
(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder
a)ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.
Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.
(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.
(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, ver-

ständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.
(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Abschnitt 2
Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:
a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.
(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 14
Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:
a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.
(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:
a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2
a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.
(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.
(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit
a) die betroffene Person bereits über die Informationen verfügt,

b)die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c)die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d)die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Artikel 15
Auskunftsrecht der betroffenen Person
(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:
a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c)die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d)falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e)das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g)wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h)das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.
(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.
(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 3
Berichtigung und Löschung

Artikel 16
Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Artikel 17
Recht auf Löschung („Recht auf Vergessenwerden“)
(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:
a)Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b)Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c)Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e)Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f)Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.
(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.
(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b)zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c)aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d)für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Artikel 18
Recht auf Einschränkung der Verarbeitung
(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:
a)die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,

b)die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c)der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die

betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d)die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Artikel 19

Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 20

Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a)die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 4

Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Artikel 21

Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.
(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Artikel 22
Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
(2) Absatz 1 gilt nicht, wenn die Entscheidung
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.
(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.
(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Abschnitt 5
Beschränkungen

Artikel 23
Beschränkungen
(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:
a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h)Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.
(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf
a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f)die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h)das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

**KAPITEL IV: Verantwortlicher und Auftragsverarbeiter (Art. 24-43)**

Abschnitt 1
Allgemeine Pflichten

Artikel 24
Verantwortung des für die Verarbeitung Verantwortlichen
(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.
(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Artikel 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.
(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 26
Gemeinsam für die Verarbeitung Verantwortliche
(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.
(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.
(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Artikel 27
Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern
(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union.
(2) Die Pflicht gemäß Absatz 1 des vorliegenden Artikels gilt nicht für
a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder

b) Behörden oder öffentliche Stellen.
(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden.
(4) Der Vertreter wird durch den Verantwortlichen oder den Auftragsverarbeiter beauftragt, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.
(5) Die Benennung eines Vertreters durch den Verantwortlichen oder den Auftragsverarbeiter erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst.

Artikel 28
Auftragsverarbeiter
(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht we-

gen eines wichtigen öffentlichen Interesses verbietet;

b)gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d)die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f)unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g)nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h)dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 29

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 30
Verzeichnis von Verarbeitungstätigkeiten
(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Artikel 31
Zusammenarbeit mit der Aufsichtsbehörde
Der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Abschnitt 2
Sicherheit personenbezogener Daten

Artikel 32
Sicherheit der Verarbeitung
(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auf-

tragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Artikel 34

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Abschnitt 3
Datenschutz-Folgenabschätzung und vorherige Konsultation

Artikel 35
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d)die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Artikel 36

Vorherige Konsultation

(1) Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

(2) Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.

(3) Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 1 folgende Informationen zur Verfügung:

a)gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

c)die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;

d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

(4) Die Mitgliedstaaten konsultieren die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen.

(5) Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

Abschnitt 4
Datenschutzbeauftragter

Artikel 37
Benennung eines Datenschutzbeauftragten
(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
a)die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b)die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c)die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.
(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Artikel 38
Stellung des Datenschutzbeauftragten
(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.
(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.
(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.
(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.
(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Artikel 39
Aufgaben des Datenschutzbeauftragten
(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:
a)Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die

Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Abschnitt 5
Verhaltensregeln und Zertifizierung

Artikel 40
Verhaltensregeln

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

(2) Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

a) faire und transparente Verarbeitung;

b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;

c) Erhebung personenbezogener Daten;

d) Pseudonymisierung personenbezogener Daten;

e) Unterrichtung der Öffentlichkeit und der betroffenen Personen;

f) Ausübung der Rechte betroffener Personen;

g) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;

h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;

i) die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;

j) die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder

k) außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79.

(3) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können Verhaltensregeln, die gemäß Absatz 5 des vorliegenden Artikels genehmigt wurden und gemäß Absatz 9 des vorliegenden Artikels allgemeine Gültigkeit besitzen, können auch von Verantwortlichen oder Auftragsverarbeitern, die gemäß Artikel 3 nicht unter diese Verordnung fallen, eingehalten werden, um geeigne-

te Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe des Artikels 46 Absatz 2 Buchstabe e zu bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

(4) Die Verhaltensregeln gemäß Absatz 2 des vorliegenden Artikels müssen Verfahren vorsehen, die es der in Artikel 41 Absatz 1 genannten Stelle ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen durch die Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen, unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde, die nach Artikel 55 oder 56 zuständig ist.

(5) Verbände und andere Vereinigungen gemäß Absatz 2 des vorliegenden Artikels, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, legen den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung der Aufsichtsbehörde vor, die nach Artikel 55 zuständig ist. Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist und genehmigt diesen Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung, wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien bietet.

(6) Wird durch die Stellungnahme nach Absatz 5 der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung genehmigt und beziehen sich die betreffenden Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht sie.

(7) Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die nach Artikel 55 zuständige Aufsichtsbehörde — bevor sie den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung genehmigt — ihn nach dem Verfahren gemäß Artikel 63 dem Ausschuss vor, der zu der Frage Stellung nimmt, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist oder — im Fall nach Absatz 3 dieses Artikels — geeignete Garantien vorsieht.

(8) Wird durch die Stellungnahme nach Absatz 7 bestätigt, dass der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist oder — im Fall nach Absatz 3 — geeignete Garantien vorsieht, so übermittelt der Ausschuss seine Stellungnahme der Kommission.

(9) Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass die ihr gemäß Absatz 8 übermittelten genehmigten Verhaltensregeln bzw. deren genehmigte Änderung oder Erweiterung allgemeine Gültigkeit in der Union besitzen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

(10) Die Kommission trägt dafür Sorge, dass die genehmigten Verhaltensregeln, denen gemäß Absatz 9 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

(11) Der Ausschuss nimmt alle genehmigten Verhaltensregeln bzw. deren genehmigte Änderungen oder Erweiterungen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Artikel 41

Überwachung der genehmigten Verhaltensregeln

(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 40 von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde.

(2) Eine Stelle gemäß Absatz 1 kann zum Zwecke der Überwachung der Einhaltung von Verhaltensregeln akkreditiert werden, wenn sie

a) ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

b) Verfahren festgelegt hat, die es ihr ermöglichen, zu bewerten, ob Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der Verhaltensregeln durch die Verantwortlichen und Auftragsverarbeiter zu überwachen und die Anwendung der Verhaltensregeln regelmäßig zu überprüfen;

c) Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht, und

d) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 63 an den Ausschuss.
(4) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde und der Bestimmungen des Kapitels VIII ergreift eine Stelle gemäß Absatz 1 vorbehaltlich geeigneter Garantien im Falle einer Verletzung der Verhaltensregeln durch einen Verantwortlichen oder einen Auftragsverarbeiter geeignete Maßnahmen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des Verantwortlichen oder Auftragsverarbeiters von den Verhaltensregeln. Sie unterrichtet die zuständige Aufsichtsbehörde über solche Maßnahmen und deren Begründung.
(5) Die zuständige Aufsichtsbehörde widerruft die Akkreditierung einer Stelle gemäß Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.
(6) Dieser Artikel gilt nicht für die Verarbeitung durch Behörden oder öffentliche Stellen.

Artikel 42
Zertifizierung
(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.
(2) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 5 des vorliegenden Artikels genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.
(3) Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.
(4) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.
(5) Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 oder — gemäß Artikel 63 — durch den Ausschuss genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.
(6) Der Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 43 oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.
(7) Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden. Die Zertifizierung wird gegebenenfalls durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.
(8) Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Artikel 43
Zertifizierungsstellen
(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde — damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h Gebrauch machen kann — die Zertifizierung. Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von einer oder beiden der folgenden Stellen akkreditiert werden:
a) der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde;

b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates (20) im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß

Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.

(2) Zertifizierungsstellen nach Absatz 1 dürfen nur dann gemäß dem genannten Absatz akkreditiert werden, wenn sie

a)ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben;

b)sich verpflichtet haben, die Kriterien nach Artikel 42 Absatz 5, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde oder — gemäß Artikel 63 — von dem Ausschuss genehmigt wurden, einzuhalten;

c)Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung sowie der Datenschutzsiegel und -prüfzeichen festgelegt haben;

d)Verfahren und Strukturen festgelegt haben, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgehen und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent machen, und

e)zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die Akkreditierung von Zertifizierungsstellen nach den Absätzen 1 und 2 erfolgt anhand der Kriterien, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde oder — gemäß Artikel 63 — von dem Ausschuss genehmigt wurden. Im Fall einer Akkreditierung nach Absatz 1 Buchstabe b des vorliegenden Artikels ergänzen diese Anforderungen diejenigen, die in der Verordnung (EG) Nr. 765/2008 und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.

(4) Die Zertifizierungsstellen nach Absatz 1 sind unbeschadet der Verantwortung, die der Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Zertifizierungsstelle die Anforderungen dieses Artikels erfüllt.

(5) Die Zertifizierungsstellen nach Absatz 1 teilen den zuständigen Aufsichtsbehörden die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

(6) Die Anforderungen nach Absatz 3 des vorliegenden Artikels und die Kriterien nach Artikel 42 Absatz 5 werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht. Die Aufsichtsbehörden übermitteln diese Anforderungen und Kriterien auch dem Ausschuss. Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise.

(7) Unbeschadet des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn eine Zertifizierungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die für die in Artikel 42 Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind.

(9) Die Kommission kann Durchführungsrechtsakte erlassen, mit denen technische Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur Förderung und Anerkennung dieser Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

## KAPITEL V: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen (Art. 44-50)

Artikel 44

Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 45
Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 46

Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder

b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

(4) Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 63 an, wenn ein Fall gemäß Absatz 3 des vorliegenden Artikels vorliegt.

(5) Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 47

Verbindliche interne Datenschutzvorschriften

(1) Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und

c) die in Absatz 2 festgelegten Anforderungen erfüllen.

(2) Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;

b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden

Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;

d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;

e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

i) die Beschwerdeverfahren;

j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;

k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;

m) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und

n) geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3) Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbei-

tern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

Artikel 48
Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung
Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Artikel 49
Ausnahmen für bestimmte Fälle
(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:
a)die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

b)die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,

c)die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

e)die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f)die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g)die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.
Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 — einschließlich der verbindlichen internen Datenschutzvorschriften — gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.
(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.
(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.
(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.
(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Ka-

tegorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.
(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

Artikel 50
Internationale Zusammenarbeit zum Schutz personenbezogener Daten
In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur
a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,

b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Meldungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,

c) Einbindung maßgeblicher Interessenträger in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten dienen,

d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten einschließlich Zuständigkeitskonflikten mit Drittländern.

**KAPITEL VI: Unabhängige Aufsichtsbehörden (Art. 51-59)**

Abschnitt 1
Unabhängigkeit

Artikel 51
Aufsichtsbehörde
(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde“).
(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII zusammen.
(3) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt, und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten.
(4) Jeder Mitgliedstaat teilt der Kommission bis spätestens 25. Mai 2018 die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

Artikel 52
Unabhängigkeit
(1) Jede Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.
(2) Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.
(3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.
(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.
(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

Artikel 53
Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde
(1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar
— vom Parlament,

— von der Regierung,

— vom Staatsoberhaupt oder

—von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.
(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.
(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.
(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt.

Artikel 54
Errichtung der Aufsichtsbehörde
(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor:
a) die Errichtung jeder Aufsichtsbehörde;

b)die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde;

c)die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde;

d)die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren; dies gilt nicht für die erste Amtszeit nach 24. Mai 2016, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;

e)die Frage, ob und — wenn ja — wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können;

f)die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.
(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während dieser Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Verordnung.

Abschnitt 2
Zuständigkeit, Aufgaben und Befugnisse

Artikel 55
Zuständigkeit
(1) Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.
(2) Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.

(3) Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 56
Zuständigkeit der federführenden Aufsichtsbehörde
(1) Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.
(2) Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.
(3) In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.
(4) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.
(5) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß den Artikeln 61 und 62.
(6) Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Artikel 57
Aufgaben
(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet
a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;

e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;

f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

i)maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

j)Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;

k)eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;

m)die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;

n)die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;

o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;

p)die Kriterien für die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;

q)die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;

r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;

s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;

t) Beiträge zur Tätigkeit des Ausschusses leisten;

u)interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58

Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a)den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,

b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,

c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,

d)den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,

e)von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,

f)gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a)einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,

b)einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,

c)den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,

d)den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

e)den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,

f)eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,

g)die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,

h)eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,

i)eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,

j)die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,

a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,

b)zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,

c)die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,

d)eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,

e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,

f)im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,

g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,

h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,

i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen

j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.
(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.
(6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

Artikel 59
Tätigkeitsbericht
Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Artikel 58 Absatz 2 enthalten kann. Diese Berichte werden dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Sie werden der Öffentlichkeit, der Kommission und dem Ausschuss zugänglich gemacht.

**KAPITEL VII: Zusammenarbeit und Kohärenz (Art. 60-76)**

Abschnitt 1
Zusammenarbeit

Artikel 60
Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden
(1) Die federführende Aufsichtsbehörde arbeitet mit den anderen betroffenen Aufsichtsbehörden im Einklang mit diesem Artikel zusammen und bemüht sich dabei, einen Konsens zu erzielen. Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen aus.
(2) Die federführende Aufsichtsbehörde kann jederzeit andere betroffene Aufsichtsbehörden um Amtshilfe gemäß Artikel 61 ersuchen und gemeinsame Maßnahmen gemäß Artikel 62 durchführen, insbesondere zur Durchführung von Untersuchungen oder zur Überwachung der Umsetzung einer Maßnahme in Bezug auf einen Verantwortlichen oder einen Auftragsverarbeiter, der in einem anderen Mitgliedstaat niedergelassen ist.
(3) Die federführende Aufsichtsbehörde übermittelt den anderen betroffenen Aufsichtsbehörden unverzüglich die zweckdienlichen Informationen zu der Angelegenheit. Sie legt den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vor und trägt deren Standpunkten gebührend Rechnung.
(4) Legt eine der anderen betroffenen Aufsichtsbehörden innerhalb von vier Wochen, nachdem sie gemäß Absatz 3 des vorliegenden Artikels konsultiert wurde, gegen diesen Beschlussentwurf einen maßgeblichen und begründeten Einspruch ein und schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder ist der Ansicht, dass der Einspruch nicht maßgeblich oder nicht begründet ist, so leitet die federführende Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 für die Angelegenheit ein.
(5) Beabsichtigt die federführende Aufsichtsbehörde, sich dem maßgeblichen und begründeten Einspruch anzuschließen, so legt sie den anderen betroffenen Aufsichtsbehörden einen überarbeiteten Beschlussentwurf zur Stellungnahme vor. Der überarbeitete Beschlussentwurf wird innerhalb von zwei Wochen dem Verfahren nach Absatz 4 unterzogen.
(6) Legt keine der anderen betroffenen Aufsichtsbehörden Einspruch gegen den Beschlussentwurf ein, der von der federführenden Aufsichtsbehörde innerhalb der in den Absätzen 4 und 5 festgelegten Frist vorgelegt wurde, so gelten die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden als mit dem Beschlussentwurf einverstanden und sind an ihn gebunden.
(7) Die federführende Aufsichtsbehörde erlässt den Beschluss und teilt ihn der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder gegebenenfalls des Auftragsverarbeiters mit und setzt die anderen betroffenen Aufsichtsbehörden und den Ausschuss von dem betreffenden Beschluss einschließlich einer Zusammenfassung der maßgeblichen Fakten und Gründe in Kenntnis. Die Aufsichtsbehörde, bei der eine Beschwerde eingereicht worden ist, unterrichtet den Beschwerdeführer über den Beschluss.
(8) Wird eine Beschwerde abgelehnt oder abgewiesen, so erlässt die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, abweichend von Absatz 7 den Beschluss, teilt ihn dem Beschwerdeführer mit und setzt den Verantwortlichen in Kenntnis.
(9) Sind sich die federführende Aufsichtsbehörde und die betreffenden Aufsichtsbehörden darüber einig, Teile der Beschwerde abzulehnen oder abzuweisen und bezüglich anderer Teile dieser Beschwerde tätig zu werden, so wird in dieser Angelegenheit für jeden dieser Teile ein eigener Beschluss erlassen. Die federführende Aufsichtsbehörde erlässt den Beschluss für den Teil, der das Tätigwerden in Bezug auf den Verantwortlichen betrifft, teilt

ihn der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats mit und setzt den Beschwerdeführer hiervon in Kenntnis, während die für den Beschwerdeführer zuständige Aufsichtsbehörde den Beschluss für den Teil erlässt, der die Ablehnung oder Abweisung dieser Beschwerde betrifft, und ihn diesem Beschwerdeführer mitteilt und den Verantwortlichen oder den Auftragsverarbeiter hiervon in Kenntnis setzt.
(10) Nach der Unterrichtung über den Beschluss der federführenden Aufsichtsbehörde gemäß den Absätzen 7 und 9 ergreift der Verantwortliche oder der Auftragsverarbeiter die erforderlichen Maßnahmen, um die Verarbeitungstätigkeiten all seiner Niederlassungen in der Union mit dem Beschluss in Einklang zu bringen. Der Verantwortliche oder der Auftragsverarbeiter teilt der federführenden Aufsichtsbehörde die Maßnahmen mit, die zur Einhaltung des Beschlusses ergriffen wurden; diese wiederum unterrichtet die anderen betroffenen Aufsichtsbehörden.
(11) Hat — in Ausnahmefällen — eine betroffene Aufsichtsbehörde Grund zu der Annahme, dass zum Schutz der Interessen betroffener Personen dringender Handlungsbedarf besteht, so kommt das Dringlichkeitsverfahren nach Artikel 66 zur Anwendung.
(12) Die federführende Aufsichtsbehörde und die anderen betroffenen Aufsichtsbehörden übermitteln einander die nach diesem Artikel geforderten Informationen auf elektronischem Wege unter Verwendung eines standardisierten Formats.

Artikel 61
Gegenseitige Amtshilfe
(1) Die Aufsichtsbehörden übermitteln einander maßgebliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Konsultation, um Vornahme von Nachprüfungen und Untersuchungen.
(2) Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um einem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu kann insbesondere auch die Übermittlung maßgeblicher Informationen über die Durchführung einer Untersuchung gehören.
(3) Amtshilfeersuchen enthalten alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.
(4) Die ersuchte Aufsichtsbehörde lehnt das Ersuchen nur ab, wenn
a)sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder

b)ein Eingehen auf das Ersuchen gegen diese Verordnung verstoßen würde oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt.
(5) Die ersuchte Aufsichtsbehörde informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen. Die ersuchte Aufsichtsbehörde erläutert gemäß Absatz 4 die Gründe für die Ablehnung des Ersuchens.
(6) Die ersuchten Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.
(7) Ersuchte Aufsichtsbehörden verlangen für Maßnahmen, die sie aufgrund eines Amtshilfeersuchens getroffen haben, keine Gebühren. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.
(8) Erteilt eine ersuchte Aufsichtsbehörde nicht binnen eines Monats nach Eingang des Ersuchens einer anderen Aufsichtsbehörde die Informationen gemäß Absatz 5, so kann die ersuchende Aufsichtsbehörde eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 55 Absatz 1 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 66 Absatz 1 ausgegangen, der einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Ausschuss gemäß Artikel 66 Absatz 2 erforderlich macht.
(9) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss, insbesondere das in Absatz 6 des vorliegenden Artikels genannte standardisierte Format, festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 62
Gemeinsame Maßnahmen der Aufsichtsbehörden
(1) Die Aufsichtsbehörden führen gegebenenfalls gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen durch, an denen Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.

(2) Verfügt der Verantwortliche oder der Auftragsverarbeiter über Niederlassungen in mehreren Mitgliedstaaten oder werden die Verarbeitungsvorgänge voraussichtlich auf eine bedeutende Zahl betroffener Personen in mehr als einem Mitgliedstaat erhebliche Auswirkungen haben, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, an den gemeinsamen Maßnahmen teilzunehmen. Die gemäß Artikel 56 Absatz 1 oder Absatz 4 zuständige Aufsichtsbehörde lädt die Aufsichtsbehörde jedes dieser Mitgliedstaaten zur Teilnahme an den gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme.
(3) Eine Aufsichtsbehörde kann gemäß dem Recht des Mitgliedstaats und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde Befugnisse einschließlich Untersuchungsbefugnisse übertragen oder, soweit dies nach dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Untersuchungsbefugnisse nach dem Recht des Mitgliedstaats der unterstützenden Aufsichtsbehörde auszuüben. Diese Untersuchungsbefugnisse können nur unter der Leitung und in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde.
(4) Sind gemäß Absatz 1 Bedienstete einer unterstützenden Aufsichtsbehörde in einem anderen Mitgliedstaat im Einsatz, so übernimmt der Mitgliedstaat der einladenden Aufsichtsbehörde nach Maßgabe des Rechts des Mitgliedstaats, in dessen Hoheitsgebiet der Einsatz erfolgt, die Verantwortung für ihr Handeln, einschließlich der Haftung für alle von ihnen bei ihrem Einsatz verursachten Schäden.
(5) Der Mitgliedstaat, in dessen Hoheitsgebiet der Schaden verursacht wurde, ersetzt diesen Schaden so, wie er ihn ersetzen müsste, wenn seine eigenen Bediensteten ihn verursacht hätten. Der Mitgliedstaat der unterstützenden Aufsichtsbehörde, deren Bedienstete im Hoheitsgebiet eines anderen Mitgliedstaats einer Person Schaden zugefügt haben, erstattet diesem anderen Mitgliedstaat den Gesamtbetrag des Schadenersatzes, den dieser an die Berechtigten geleistet hat.
(6) Unbeschadet der Ausübung seiner Rechte gegenüber Dritten und mit Ausnahme des Absatzes 5 verzichtet jeder Mitgliedstaat in dem Fall des Absatzes 1 darauf, den in Absatz 4 genannten Betrag des erlittenen Schadens anderen Mitgliedstaaten gegenüber geltend zu machen.
(7) Ist eine gemeinsame Maßnahme geplant und kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 Satz 2 des vorliegenden Artikels nach, so können die anderen Aufsichtsbehörden eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 55 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 66 Absatz 1 ausgegangen, der eine im Dringlichkeitsverfahren angenommene Stellungnahme oder einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Ausschusses gemäß Artikel 66 Absatz 2 erforderlich macht.

Abschnitt 2
Kohärenz

Artikel 63
Kohärenzverfahren
Um zur einheitlichen Anwendung dieser Verordnung in der gesamten Union beizutragen, arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.

Artikel 64
Stellungnahme Ausschusses
(1) Der Ausschuss gibt eine Stellungnahme ab, wenn die zuständige Aufsichtsbehörde beabsichtigt, eine der nachstehenden Maßnahmen zu erlassen. Zu diesem Zweck übermittelt die zuständige Aufsichtsbehörde dem Ausschuss den Entwurf des Beschlusses, wenn dieser

a) der Annahme einer Liste der Verarbeitungsvorgänge dient, die der Anforderung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 4 unterliegen,

b) eine Angelegenheit gemäß Artikel 40 Absatz 7 und damit die Frage betrifft, ob ein Entwurf von Verhaltensregeln oder eine Änderung oder Ergänzung von Verhaltensregeln mit dieser Verordnung in Einklang steht,

c) der Billigung der Kriterien für die Akkreditierung einer Stelle nach Artikel 41 Absatz 3 oder einer Zertifizierungsstelle nach Artikel 43 Absatz 3 dient,

d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 46 Absatz 2 Buchstabe d und Artikel 28 Absatz 8 dient,

e) der Genehmigung von Vertragsklauseln gemäß Artikels 46 Absatz 3 Buchstabe a dient, oder

f) der Annahme verbindlicher interner Vorschriften im Sinne von Artikel 47 dient.
(2) Jede Aufsichtsbehörde, der Vorsitz des Ausschuss oder die Kommission können beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 61 oder zu gemeinsamen Maßnahmen gemäß Artikel 62 nicht nachkommt.
(3) In den in den Absätzen 1 und 2 genannten Fällen gibt der Ausschuss eine Stellungnahme zu der Angelegenheit ab, die ihm vorgelegt wurde, sofern er nicht bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat. Diese Stellungnahme wird binnen acht Wochen mit der einfachen Mehrheit der Mitglieder des Ausschusses angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen verlängert werden. Was den in Absatz 1 genannten Beschlussentwurf angeht, der gemäß Absatz 5 den Mitgliedern des Ausschusses übermittelt wird, so wird angenommen, dass ein Mitglied, das innerhalb einer vom Vorsitz angegebenen angemessenen Frist keine Einwände erhoben hat, dem Beschlussentwurf zustimmt.
(4) Die Aufsichtsbehörden und die Kommission übermitteln unverzüglich dem Ausschuss auf elektronischem Wege unter Verwendung eines standardisierten Formats alle zweckdienlichen Informationen, einschließlich — je nach Fall — einer kurzen Darstellung des Sachverhalts, des Beschlussentwurfs, der Gründe, warum eine solche Maßnahme ergriffen werden muss, und der Standpunkte anderer betroffener Aufsichtsbehörden.
(5) Der Vorsitz des Ausschusses unterrichtet unverzüglich auf elektronischem Wege
a)unter Verwendung eines standardisierten Formats die Mitglieder des Ausschusses und die Kommission über alle zweckdienlichen Informationen, die ihm zugegangen sind. Soweit erforderlich stellt das Sekretariat des Ausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung und

b)je nach Fall die in den Absätzen 1 und 2 genannte Aufsichtsbehörde und die Kommission über die Stellungnahme und veröffentlicht sie.
(6) Die zuständige Aufsichtsbehörde nimmt den in Absatz 1 genannten Beschlussentwurf nicht vor Ablauf der in Absatz 3 genannten Frist an.
(7) Die in Absatz 1 genannte Aufsichtsbehörde trägt der Stellungnahme des Ausschusses s weitestgehend Rechnung und teilt dessen Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege unter Verwendung eines standardisierten Formats mit, ob sie den Beschlussentwurf beibehalten oder ändern wird; gegebenenfalls übermittelt sie den geänderten Beschlussentwurf.
(8) Teilt die betroffene Aufsichtsbehörde dem Vorsitz des Ausschusses innerhalb der Frist nach Absatz 7 des vorliegenden Artikels unter Angabe der maßgeblichen Gründe mit, dass sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen, so gilt Artikel 65 Absatz 1.

Artikel 65
Streitbeilegung durch den Ausschuss
(1) Um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung in Einzelfällen sicherzustellen, erlässt der Ausschuss in den folgenden Fällen einen verbindlichen Beschluss:
a)wenn eine betroffene Aufsichtsbehörde in einem Fall nach Artikel 60 Absatz 4 einen maßgeblichen und begründeten Einspruch gegen einen Beschlussentwurf der federführenden Behörde eingelegt hat oder die federführende Behörde einen solchen Einspruch als nicht maßgeblich oder nicht begründet abgelehnt hat. Der verbindliche Beschluss betrifft alle Angelegenheiten, die Gegenstand des maßgeblichen und begründeten Einspruchs sind, insbesondere die Frage, ob ein Verstoß gegen diese Verordnung vorliegt;

b)wenn es widersprüchliche Standpunkte dazu gibt, welche der betroffenen Aufsichtsbehörden für die Hauptniederlassung zuständig ist,

c)wenn eine zuständige Aufsichtsbehörde in den in Artikel 64 Absatz 1 genannten Fällen keine Stellungnahme des Ausschusses einholt oder der Stellungnahme des Ausschusses gemäß Artikel 64 nicht folgt. In diesem Fall kann jede betroffene Aufsichtsbehörde oder die Kommission die Angelegenheit dem Ausschuss vorlegen.
(2) Der in Absatz 1 genannte Beschluss wird innerhalb eines Monats nach der Befassung mit der Angelegenheit mit einer Mehrheit von zwei Dritteln der Mitglieder des Ausschusses angenommen. Diese Frist kann wegen der Komplexität der Angelegenheit um einen weiteren Monat verlängert werden. Der in Absatz 1 genannte Beschluss wird begründet und an die federführende Aufsichtsbehörde und alle betroffenen Aufsichtsbehörden übermittelt und ist für diese verbindlich.
(3) War der Ausschuss nicht in der Lage, innerhalb der in Absatz 2 genannten Fristen einen Beschluss anzunehmen, so nimmt er seinen Beschluss innerhalb von zwei Wochen nach Ablauf des in Absatz 2 genannten zweiten Monats mit einfacher Mehrheit der Mitglieder des Ausschusses an. Bei Stimmengleichheit zwischen den Mitgliedern des Ausschusses gibt die Stimme des Vorsitzes den Ausschlag.
(4) Die betroffenen Aufsichtsbehörden nehmen vor Ablauf der in den Absätzen 2 und 3 genannten Fristen keinen Beschluss über die dem Ausschuss vorgelegte Angelegenheit an.

(5) Der Vorsitz des Ausschusses unterrichtet die betroffenen Aufsichtsbehörden unverzüglich über den in Absatz 1 genannten Beschluss. Er setzt die Kommission hiervon in Kenntnis. Der Beschluss wird unverzüglich auf der Website des Ausschusses veröffentlicht, nachdem die Aufsichtsbehörde den in Absatz 6 genannten endgültigen Beschluss mitgeteilt hat.
(6) Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, trifft den endgültigen Beschluss auf der Grundlage des in Absatz 1 des vorliegenden Artikels genannten Beschlusses unverzüglich und spätestens einen Monat, nachdem der Europäische Datenschutzausschuss seinen Beschluss mitgeteilt hat. Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, setzt den Ausschuss von dem Zeitpunkt, zu dem ihr endgültiger Beschluss dem Verantwortlichen oder dem Auftragsverarbeiter bzw. der betroffenen Person mitgeteilt wird, in Kenntnis. Der endgültige Beschluss der betroffenen Aufsichtsbehörden wird gemäß Artikel 60 Absätze 7, 8 und 9 angenommen. Im endgültigen Beschluss wird auf den in Absatz 1 genannten Beschluss verwiesen und festgelegt, dass der in Absatz 1 des vorliegenden Artikels genannte Beschluss gemäß Absatz 5 auf der Website des Ausschusses veröffentlicht wird. Dem endgültigen Beschluss wird der in Absatz 1 des vorliegenden Artikels genannte Beschluss beigefügt.

Artikel 66
Dringlichkeitsverfahren
(1) Unter außergewöhnlichen Umständen kann eine betroffene Aufsichtsbehörde abweichend vom Kohärenzverfahren nach Artikel 63, 64 und 65 oder dem Verfahren nach Artikel 60 sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer von höchstens drei Monaten treffen, die in ihrem Hoheitsgebiet rechtliche Wirkung entfalten sollen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um Rechte und Freiheiten von betroffenen Personen zu schützen. Die Aufsichtsbehörde setzt die anderen betroffenen Aufsichtsbehörden, den Ausschuss und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis.
(2) Hat eine Aufsichtsbehörde eine Maßnahme nach Absatz 1 ergriffen und ist sie der Auffassung, dass dringend endgültige Maßnahmen erlassen werden müssen, kann sie unter Angabe von Gründen im Dringlichkeitsverfahren um eine Stellungnahme oder einen verbindlichen Beschluss des Ausschusses ersuchen.
(3) Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme oder gegebenenfalls einen verbindlichen Beschluss des Ausschusses ersuchen, wenn eine zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine geeignete Maßnahme getroffen hat, um die Rechte und Freiheiten von betroffenen Personen zu schützen.
(4) Abweichend von Artikel 64 Absatz 3 und Artikel 65 Absatz 2 wird eine Stellungnahme oder ein verbindlicher Beschluss im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen mit einfacher Mehrheit der Mitglieder des Ausschusses angenommen.

Artikel 67
Informationsaustausch
Die Kommission kann Durchführungsrechtsakte von allgemeiner Tragweite zur Festlegung der Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss, insbesondere des standardisierten Formats nach Artikel 64, erlassen.
Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.
Abschnitt 3
Europäischer Datenschutzausschuss

Artikel 68
Europäischer Datenschutzausschuss
(1) Der Europäische Datenschutzausschuss (im Folgenden „Ausschuss“) wird als Einrichtung der Union mit eigener Rechtspersönlichkeit eingerichtet.
(2) Der Ausschuss wird von seinem Vorsitz vertreten.
(3) Der Ausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern.
(4) Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Verordnung erlassenen Vorschriften zuständig, so wird im Einklang mit den Rechtsvorschriften dieses Mitgliedstaats ein gemeinsamer Vertreter benannt.
(5) Die Kommission ist berechtigt, ohne Stimmrecht an den Tätigkeiten und Sitzungen des Ausschusses teilzunehmen. Die Kommission benennt einen Vertreter. Der Vorsitz des Ausschusses unterrichtet die Kommission über die Tätigkeiten des Ausschusses.
(6) In den in Artikel 65 genannten Fällen ist der Europäische Datenschutzbeauftragte nur bei Beschlüssen stimmberechtigt, die Grundsätze und Vorschriften betreffen, die für die Organe, Einrichtungen, Ämter und Agenturen der Union gelten und inhaltlich den Grundsätzen und Vorschriften dieser Verordnung entsprechen.

Artikel 69
Unabhängigkeit
(1) Der Ausschuss handelt bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse gemäß den Artikeln 70 und 71 unabhängig.
(2) Unbeschadet der Ersuchen der Kommission gemäß Artikel 70 Absatz 1 Buchstabe b und Absatz 2 ersucht der Ausschuss bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse weder um Weisung noch nimmt er Weisungen entgegen.

Artikel 70
Aufgaben des Ausschusses
(1) Der Ausschuss stellt die einheitliche Anwendung dieser Verordnung sicher. Hierzu nimmt der Ausschuss von sich aus oder gegebenenfalls auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr:
a)Überwachung und Sicherstellung der ordnungsgemäßen Anwendung dieser Verordnung in den in den Artikeln 64 und 65 genannten Fällen unbeschadet der Aufgaben der nationalen Aufsichtsbehörden;

b)Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, einschließlich etwaiger Vorschläge zur Änderung dieser Verordnung;

c)Beratung der Kommission über das Format und die Verfahren für den Austausch von Informationen zwischen den Verantwortlichen, den Auftragsverarbeitern und den Aufsichtsbehörden in Bezug auf verbindliche interne Datenschutzvorschriften;

d)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zu Verfahren für die Löschung gemäß Artikel 17 Absatz 2 von Links zu personenbezogenen Daten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten;

e)Prüfung — von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission — von die Anwendung dieser Verordnung betreffenden Fragen und Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;

f)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen gemäß Artikel 22 Absatz 2;

g)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes für die Feststellung von Verletzungen des Schutzes personenbezogener Daten und die Festlegung der Unverzüglichkeit im Sinne des Artikels 33 Absätze 1 und 2, und zu den spezifischen Umständen, unter denen der Verantwortliche oder der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden hat;

h)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zu den Umständen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne des Artikels 34 Absatz 1 zur Folge hat;

i)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der in Artikel 47 aufgeführten Kriterien und Anforderungen für die Übermittlungen personenbezogener Daten, die auf verbindlichen internen Datenschutzvorschriften von Verantwortlichen oder Auftragsverarbeitern beruhen, und der dort aufgeführten weiteren erforderlichen Anforderungen zum Schutz personenbezogener Daten der betroffenen Personen;

j)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der Kriterien und Bedingungen für die Übermittlungen personenbezogener Daten gemäß Artikel 49 Absatz 1;

k)Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 58 Absätze 1, 2 und 3 und die Festsetzung von Geldbußen gemäß Artikel 83;

l)Überprüfung der praktischen Anwendung der unter den Buchstaben e und f genannten Leitlinien, Empfehlungen und bewährten Verfahren;

m)Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden

Absatzes zur Festlegung gemeinsamer Verfahren für die von natürlichen Personen vorgenommene Meldung von Verstößen gegen diese Verordnung gemäß Artikel 54 Absatz 2;

n) Förderung der Ausarbeitung von Verhaltensregeln und der Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und -prüfzeichen gemäß den Artikeln 40 und 42;

o) Akkreditierung von Zertifizierungsstellen und deren regelmäßige Überprüfung gemäß Artikel 43 und Führung eines öffentlichen Registers der akkreditierten Einrichtungen gemäß Artikel 43 Absatz 6 und der in Drittländern niedergelassenen akkreditierten Verantwortlichen oder Auftragsverarbeiter gemäß Artikel 42 Absatz 7;

p) Präzisierung der in Artikel 43 Absatz 3 genannten Anforderungen im Hinblick auf die Akkreditierung von Zertifizierungsstellen gemäß Artikel 42;

q) Abgabe einer Stellungnahme für die Kommission zu den Zertifizierungsanforderungen gemäß Artikel 43 Absatz 8;

r) Abgabe einer Stellungnahme für die Kommission zu den Bildsymbolen gemäß Artikel 12 Absatz 7;

s) Abgabe einer Stellungnahme für die Kommission zur Beurteilung der Angemessenheit des in einem Drittland oder einer internationalen Organisation gebotenen Schutzniveaus einschließlich zur Beurteilung der Frage, ob das Drittland, das Gebiet, ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet. Zu diesem Zweck gibt die Kommission dem Ausschuss alle erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlands, dem Gebiet oder spezifischen Sektor oder der internationalen Organisation;

t) Abgabe von Stellungnahmen im Kohärenzverfahren gemäß Artikel 64 Absatz 1 zu Beschlussentwürfen von Aufsichtsbehörden, zu Angelegenheiten, die nach Artikel 64 Absatz 2 vorgelegt wurden und um Erlass verbindlicher Beschlüsse gemäß Artikel 65, einschließlich der in Artikel 66 genannten Fälle;

u) Förderung der Zusammenarbeit und eines wirksamen bilateralen und multilateralen Austauschs von Informationen und bewährten Verfahren zwischen den Aufsichtsbehörden;

v) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit internationalen Organisationen;

w) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und -praxis mit Datenschutzaufsichtsbehörden in aller Welt;

x) Abgabe von Stellungnahmen zu den auf Unionsebene erarbeiteten Verhaltensregeln gemäß Artikel 40 Absatz 9 und

y) Führung eines öffentlich zugänglichen elektronischen Registers der Beschlüsse der Aufsichtsbehörden und Gerichte in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden.

(2) Die Kommission kann, wenn sie den Ausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist angeben.

(3) Der Ausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 93 genannten Ausschuss weiter und veröffentlicht sie.

(4) Der Ausschuss konsultiert gegebenenfalls interessierte Kreise und gibt ihnen Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Unbeschadet des Artikels 76 macht der Ausschuss die Ergebnisse der Konsultation der Öffentlichkeit zugänglich.

Artikel 71

Berichterstattung

(1) Der Ausschuss erstellt einen Jahresbericht über den Schutz natürlicher Personen bei der Verarbeitung in der Union und gegebenenfalls in Drittländern und internationalen Organisationen. Der Bericht wird veröffentlicht und dem Europäischen Parlament, dem Rat und der Kommission übermittelt.

(2) Der Jahresbericht enthält eine Überprüfung der praktischen Anwendung der in Artikel 70 Absatz 1 Buchstabe l genannten Leitlinien, Empfehlungen und bewährten Verfahren sowie der in Artikel 65 genannten verbindlichen Beschlüsse.

Artikel 72
Verfahrensweise
(1) Sofern in dieser Verordnung nichts anderes bestimmt ist, fasst der Ausschuss seine Beschlüsse mit einfacher Mehrheit seiner Mitglieder.
(2) Der Ausschuss gibt sich mit einer Mehrheit von zwei Dritteln seiner Mitglieder eine Geschäftsordnung und legt seine Arbeitsweise fest.

Artikel 73
Vorsitz
(1) Der Ausschuss wählt aus dem Kreis seiner Mitglieder mit einfacher Mehrheit einen Vorsitzenden und zwei stellvertretende Vorsitzende.
(2) Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre einmalige Wiederwahl ist zulässig.

Artikel 74
Aufgaben des Vorsitzes
(1) Der Vorsitz hat folgende Aufgaben:
a) Einberufung der Sitzungen des Ausschusses und Erstellung der Tagesordnungen,

b) Übermittlung der Beschlüsse des Ausschusses nach Artikel 65 an die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden,

c) Sicherstellung einer rechtzeitigen Ausführung der Aufgaben des Ausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 63.
(2) Der Ausschuss legt die Aufteilung der Aufgaben zwischen dem Vorsitzenden und dessen Stellvertretern in seiner Geschäftsordnung fest.

Artikel 75
Sekretariat
(1) Der Ausschuss wird von einem Sekretariat unterstützt, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird.
(2) Das Sekretariat führt seine Aufgaben ausschließlich auf Anweisung des Vorsitzes des Ausschusses aus.
(3) Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, unterliegt anderen Berichtspflichten als das Personal, das an der Wahrnehmung der dem Europäischen Datenschutzbeauftragten übertragenen Aufgaben beteiligt ist.
(4) Soweit angebracht, erstellen und veröffentlichen der Ausschuss und der Europäische Datenschutzbeauftragte eine Vereinbarung zur Anwendung des vorliegenden Artikels, in der die Bedingungen ihrer Zusammenarbeit festgelegt sind und die für das Personal des Europäischen Datenschutzbeauftragten gilt, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist.
(5) Das Sekretariat leistet dem Ausschuss analytische, administrative und logistische Unterstützung.
(6) Das Sekretariat ist insbesondere verantwortlich für
a) das Tagesgeschäft des Ausschusses,

b) die Kommunikation zwischen den Mitgliedern des Ausschusses, seinem Vorsitz und der Kommission,

c) die Kommunikation mit anderen Organen und mit der Öffentlichkeit,

d) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation,

e) die Übersetzung sachdienlicher Informationen,

f) die Vor- und Nachbereitung der Sitzungen des Ausschusses,

g) die Vorbereitung, Abfassung und Veröffentlichung von Stellungnahmen, von Beschlüssen über die Beilegung von Streitigkeiten zwischen Aufsichtsbehörden und von sonstigen vom Ausschuss angenommenen Dokumenten.

Artikel 76
Vertraulichkeit
(1) Die Beratungen des Ausschusses sind gemäß seiner Geschäftsordnung vertraulich, wenn der Ausschuss dies für erforderlich hält.

(2) Der Zugang zu Dokumenten, die Mitgliedern des Ausschusses, Sachverständigen und Vertretern von Dritten vorgelegt werden, wird durch die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates geregelt.

**KAPITEL VIII: Rechtsbehelfe, Haftung und Sanktionen (Art. 77-84)**

Artikel 77
Recht auf Beschwerde bei einer Aufsichtsbehörde
(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.
(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

Artikel 78
Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde
(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.
(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 55 und 56 zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 77 erhobenen Beschwerde in Kenntnis gesetzt hat.
(3) Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.
(4) Kommt es zu einem Verfahren gegen den Beschluss einer Aufsichtsbehörde, dem eine Stellungnahme oder ein Beschluss des Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.

Artikel 79
Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter
(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.
(2) Für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Artikel 80
Vertretung von betroffenen Personen
(1) Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz gemäß Artikel 82 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.
(2) Die Mitgliedstaaten können vorsehen, dass jede der in Absatz 1 des vorliegenden Artikels genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der gemäß Artikel 77 zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind.

Artikel 81
Aussetzung des Verfahrens
(1) Erhält ein zuständiges Gericht in einem Mitgliedstaat Kenntnis von einem Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter, das vor einem Gericht in einem anderen Mitgliedstaat anhängig ist, so nimmt es mit diesem Gericht Kontakt auf, um sich zu vergewissern, dass ein solches Verfahren existiert.
(2) Ist ein Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen.
(3) Sind diese Verfahren in erster Instanz anhängig, so kann sich jedes später angerufene Gericht auf Antrag einer Partei auch für unzuständig erklären, wenn das zuerst angerufene Gericht für die betreffenden Klagen zuständig ist und die Verbindung der Klagen nach seinem Recht zulässig ist.

Artikel 82
Haftung und Recht auf Schadenersatz
(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.
(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.
(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.
(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen
(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h)Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i)Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j)Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k)jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a)die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a)die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c)die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d)alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e)Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Artikel 84
Sanktionen
(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung — insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen — fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.
(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

**KAPITEL IX: Vorschriften für besondere Verarbeitungssituationen (Art. 85-91)**

Artikel 85
Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.
(2) Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.
(3) Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er aufgrund von Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Artikel 86
Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten
Personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, können von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die Behörde oder Einrichtung unterliegt, offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung in Einklang zu bringen.

Artikel 87
Verarbeitung der nationalen Kennziffer
Die Mitgliedstaaten können näher bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. In diesem Fall darf die nationale Kennziffer oder das andere Kennzeichen von allgemeiner Bedeutung nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung verwendet werden.

Artikel 88
Datenverarbeitung im Beschäftigungskontext
(1) Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarung en festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.
(2) Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

(3) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

Artikel 89
Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
(1) Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.
(2) Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.
(3) Werden personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18, 19, 20 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.
(4) Dient die in den Absätzen 2 und 3 genannte Verarbeitung gleichzeitig einem anderen Zweck, gelten die Ausnahmen nur für die Verarbeitung zu den in diesen Absätzen genannten Zwecken.

Artikel 90
Geheimhaltungspflichten
(1) Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber den Verantwortlichen oder den Auftragsverarbeitern, die nach Unionsrecht oder dem Recht der Mitgliedstaaten oder nach einer von den zuständigen nationalen Stellen erlassenen Verpflichtung dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in Bezug auf personenbezogene Daten, die der Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.
(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Vorschriften mit, die er aufgrund von Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

Artikel 91
Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften
(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.
(2) Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

## KAPITEL X: Delegierte Rechtsakte und Durchführungsrechtsakte (Art. 92-93)

Artikel 92
Ausübung der Befugnisübertragung
(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.
(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 wird der Kommission auf unbestimmte Zeit ab dem 24. Mai 2016 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.
(4) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.
(5) Ein delegierter Rechtsakt, der gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

Artikel 93
Ausschussverfahren
(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.
(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.
(3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

**KAPITEL XI: Schlussbestimmungen (Art. 94-99)**

Artikel 94
Aufhebung der Richtlinie 95/46/EG
(1) Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.
(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

Artikel 95
Verhältnis zur Richtlinie 2002/58/EG
Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Artikel 96
Verhältnis zu bereits geschlossenen Übereinkünften
Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 24. Mai 2016 abgeschlossen wurden und die im Einklang mit dem vor diesem Tag geltenden Unionsrecht stehen, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

Artikel 97
Berichte der Kommission
(1) Bis zum 25. Mai 2020 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Die Berichte werden öffentlich gemacht.
(2) Im Rahmen der Bewertungen und Überprüfungen nach Absatz 1 prüft die Kommission insbesondere die Anwendung und die Wirkungsweise
a) des Kapitels V über die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen insbesondere im Hinblick auf die gemäß Artikel 45 Absatz 3 der vorliegenden Verordnung erlassenen Beschlüsse sowie die gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen,

b) des Kapitels VII über Zusammenarbeit und Kohärenz.
(3) Für den in Absatz 1 genannten Zweck kann die Kommission Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern.

(4) Bei den in den Absätzen 1 und 2 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.
(5) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

Artikel 98
Überprüfung anderer Rechtsakte der Union zum Datenschutz
Die Kommission legt gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsakte der Union zum Schutz personenbezogener Daten vor, damit ein einheitlicher und kohärenter Schutz natürlicher Personen bei der Verarbeitung sichergestellt wird. Dies betrifft insbesondere die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung solcher Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Verkehr solcher Daten.

Artikel 99
Inkrafttreten und Anwendung
(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.
(2) Sie gilt ab dem 25. Mai 2018.
Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.
Geschehen zu Brüssel am 27. April 2016.
Im Namen des Europäischen Parlaments
Der Präsident
M. SCHULZ
Im Namen des Rates
Die Präsidentin
J.A. HENNIS-PLASSCHAERT

## II) Bundesdatenschutzgesetz

### Teil 1 Gemeinsame Bestimmungen (§§ 1-21)

*Kapitel 1: Anwendungsbereich und Begriffsbestimmungen*

§ 1 Anwendungsbereich des Gesetzes

(1) 1Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch 1.
öffentliche Stellen des Bundes,
2.
öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder
b)
als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.
2Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.
(2) 1Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. 2Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. 3Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) 1Dieses Gesetz findet Anwendung auf öffentliche Stellen. 2Auf nichtöffentliche Stellen findet es Anwendung, sofern 1.
der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland verarbeitet,
2.
die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters erfolgt oder
3.
der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat, er aber in den Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) fällt.
3Sofern dieses Gesetz nicht gemäß Satz 2 Anwendung findet, gelten für den Verantwortlichen oder Auftragsverarbeiter nur die §§ 8 bis 21, 39 bis 44.
(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt.

(6) 1Bei Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union gleich. 2Andere Staaten gelten insoweit als Drittstaaten.

(7) 1Bei Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. 2Andere Staaten gelten insoweit als Drittstaaten.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist.

§ 2 Begriffsbestimmungen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) 1Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn 1.
sie über den Bereich eines Landes hinaus tätig werden oder
2.
dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
2Andernfalls gelten sie als öffentliche Stellen der Länder.
(4) 1Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. 2Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(5) 1Öffentliche Stellen des Bundes gelten als nichtöffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. 2Als nichtöffentliche Stellen im Sinne dieses Gesetzes gelten auch öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

*Kapitel 2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten*

§ 3 Verarbeitung personenbezogener Daten durch öffentliche Stellen

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

§ 4 Videoüberwachung öffentlich zugänglicher Räume

(1) 1Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie 1.
zur Aufgabenerfüllung öffentlicher Stellen,
2.
zur Wahrnehmung des Hausrechts oder
3.
zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. 2Bei der Videoüberwachung von 1.
öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2.
Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs
gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) 1Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. 2Absatz 1 Satz 2 gilt entsprechend. 3Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) 1Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäß den Artikel 13 und 14 der Verordnung (EU) 2016/679. 2§ 32 gilt entsprechend.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

*Kapitel 3 Datenschutzbeauftragte öffentlicher Stellen*

§ 5 Benennung

(1) 1Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. 2Dies gilt auch für öffentliche Stellen nach § 2 Absatz 5, die am Wettbewerb teilnehmen.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 7 genannten Aufgaben.

(4) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

§ 6 Stellung

(1) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die öffentliche Stelle unterstützt die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben gemäß § 7, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) 1Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. 2Die oder der Datenschutzbeauftragte berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. 3Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) 1Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. 2Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. 3Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) 1Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. 2Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.

(6) 1Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. 2Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. 3Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 7 Aufgaben

(1) 1Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zumindest folgende Aufgaben: 1.
Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;
2.
Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;
3.
Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 67 dieses Gesetzes;
4.
Zusammenarbeit mit der Aufsichtsbehörde;
5.
Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 69 dieses Gesetzes, und gegebenenfalls Beratung zu allen sonstigen Fragen.
2Im Fall einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.
(2) 1Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. 2Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die oder der Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

*Kapitel 4 Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*

§ 8 Errichtung

(1) 1Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Bundesbeauftragte) ist eine oberste Bundesbehörde. 2Der Dienstsitz ist Bonn.

(2) Die Beamtinnen und Beamten der oder des Bundesbeauftragten sind Beamtinnen und Beamte des Bundes.

(3) 1Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen, soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht

beeinträchtigt wird. 2Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 9 Zuständigkeit

(1) 1Die oder der Bundesbeauftragte ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes, auch soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. 2Die Vorschriften dieses Kapitels gelten auch für Auftragsverarbeiter, soweit sie nichtöffentliche Stellen sind, bei denen dem Bund die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle des Bundes ist.

(2) Die oder der Bundesbeauftragte ist nicht zuständig für die Aufsicht über die von den Bundesgerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

§ 10 Unabhängigkeit

(1) 1Die oder der Bundesbeauftragte handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig. 2Sie oder er unterliegt weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen.

(2) Die oder der Bundesbeauftragte unterliegt der Rechnungsprüfung durch den Bundesrechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

§ 11 Ernennung und Amtszeit

(1) 1Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. 2Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen. 3Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. 4Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. 5Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst haben.

(2) 1Die oder der Bundesbeauftragte leistet vor der Bundespräsidentin oder dem Bundespräsidenten folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. 2So wahr mir Gott helfe. 3“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) 1Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. 2Einmalige Wiederwahl ist zulässig.

§ 12 Amtsverhältnis

(1) Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis.

(2) 1Das Amtsverhältnis beginnt mit der Aushändigung der Ernennungsurkunde. 2Es endet mit dem Ablauf der Amtszeit oder mit dem Rücktritt. 3Die Bundespräsidentin oder der Bundespräsident enthebt auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages die Bundesbeauftragte ihres oder den Bundesbeauftragten seines Amtes, wenn die oder der Bundesbeauftragte eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. 4Im Fall der Beendigung des Amtsverhältnisses oder der Amtsenthebung erhält die oder der Bundesbeauftragte eine von der Bundespräsidentin oder dem Bundespräsidenten vollzogene Urkunde. 5Eine Amtsenthebung wird mit der Aushändigung der Urkunde wirksam. 6Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist die oder der Bundesbeauftragte verpflichtet, auf Ersuchen der Präsidentin oder des Präsidenten des Bundestages die Geschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers für die Dauer von höchstens sechs Monaten weiterzuführen.

(3) 1Die Leitende Beamtin oder der Leitende Beamte nimmt die Rechte der oder des Bundesbeauftragten wahr, wenn die oder der Bundesbeauftragte an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder

sein Amtsverhältnis endet und sie oder er nicht zur Weiterführung der Geschäfte verpflichtet ist. 2§ 10 Absatz 1 ist entsprechend anzuwenden.

(4) 1Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Fall des Absatzes 2 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der Besoldungsgruppe B 11 sowie den Familienzuschlag entsprechend Anlage V des Bundesbesoldungsgesetzes. 2Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. 3Im Übrigen sind § 12 Absatz 6 sowie die §§ 13 bis 20 und 21a Absatz 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Absatz 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. 4Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Absatz 5 des Bundesministergesetzes berechnet sich das Ruhegehalt der oder des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und die oder der Bundesbeauftragte sich unmittelbar vor ihrer oder seiner Wahl zur oder zum Bundesbeauftragten als Beamtin oder Beamter oder als Richterin oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 11 zu durchlaufenden Amt befunden hat.

§ 13 Rechte und Pflichten

(1) 1Die oder der Bundesbeauftragte sieht von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen ab und übt während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. 2Insbesondere darf die oder der Bundesbeauftragte neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. 3Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(2) 1Die oder der Bundesbeauftragte hat der Präsidentin oder dem Präsidenten des Bundestages Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. 2Die Präsidentin oder der Präsident des Bundestages entscheidet über die Verwendung der Geschenke. 3Sie oder er kann Verfahrensvorschriften erlassen.

(3) 1Die oder der Bundesbeauftragte ist berechtigt, über Personen, die ihr oder ihm in ihrer oder seiner Eigenschaft als Bundesbeauftragte oder Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. 2Dies gilt auch für die Mitarbeiterinnen und Mitarbeiter der oder des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts die oder der Bundesbeauftragte entscheidet. 3Soweit das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Dokumenten von ihr oder ihm nicht gefordert werden.

(4) 1Die oder der Bundesbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. 2Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. 3Die oder der Bundesbeauftragte entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Bundesbeauftragten erforderlich. 4Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei einer Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. 5Für die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Mitarbeiterinnen und Mitarbeiter gelten die §§ 93, 97 und 105 Absatz 1, § 111 Absatz 5 in Verbindung mit § 105 Absatz 1 sowie § 116 Absatz 1 der Abgabenordnung nicht. 6Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben der oder des Auskunftspflichtigen oder der für sie oder ihn tätigen Personen handelt. 7Stellt die oder der Bundesbeauftragte einen Datenschutzverstoß fest, ist sie oder er befugt, diesen anzuzeigen und die betroffene Person hierüber zu informieren.

(5) 1Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde 1.
dem Wohl des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder ihre Beziehungen zu anderen Staaten, oder
2.
Grundrechte verletzen.

2Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten, darf die oder der Bundesbeauftragte nur im Benehmen mit der Bundesregierung aussagen. 3§ 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.
(6) Die Absätze 3 und 4 Satz 5 bis 7 gelten entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 14 Aufgaben

(1) 1Die oder der Bundesbeauftragte hat neben den in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben, 1.
die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,
2.
die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder besondere Beachtung finden,
3.
den Deutschen Bundestag und den Bundesrat, die Bundesregierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,
4.
die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten zu sensibilisieren,
5.
auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,
6.
sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 55 der Richtlinie (EU) 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,
7.
mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,
8.
Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,
9.
maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,
10.
Beratung in Bezug auf die in § 69 genannten Verarbeitungsvorgänge zu leisten und
11.
Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten.
2Im Anwendungsbereich der Richtlinie (EU) 2016/680 nimmt die oder der Bundesbeauftragte zudem die Aufgabe nach § 60 wahr.
(2) 1Zur Erfüllung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgabe kann die oder der Bundesbeauftragte zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an den Deutschen Bundestag oder einen seiner Ausschüsse, den Bundesrat, die Bundesregierung, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten. 2Auf Ersuchen des Deutschen Bundestages, eines seiner Ausschüsse oder der Bundesregierung geht die oder der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach.

(3) Die oder der Bundesbeauftragte erleichtert das Einreichen der in Absatz 1 Satz 1 Nummer 6 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(4) 1Die Erfüllung der Aufgaben der oder des Bundesbeauftragten ist für die betroffene Person unentgeltlich. 2Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die oder der Bundesbeauftragte eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. 3In diesem Fall trägt die oder der Bundesbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

§ 15 Tätigkeitsbericht

1Die oder der Bundesbeauftragte erstellt einen Jahresbericht über ihre oder seine Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen, einschließlich der verhängten Sanktionen und der Maßnahmen nach Artikel 58 Absatz 2 der Verordnung (EU) 2016/679, enthalten kann. 2Die oder der Bundesbeauftragte übermittelt den Bericht dem Deutschen Bundestag, dem Bundesrat und der Bundesregierung und macht ihn der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich.

§ 16 Befugnisse

(1) 1Die oder der Bundesbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 wahr. 2Kommt die oder der Bundesbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor der Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstabe b bis g, i und j der Verordnung (EU) 2016/679 gegenüber dem Verantwortlichen Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. 3Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. 4Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Bundesbeauftragten getroffen worden sind.

(2) 1Stellt die oder der Bundesbeauftragte bei Datenverarbeitungen durch öffentliche Stellen des Bundes zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der zuständigen obersten Bundesbehörde und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. 2Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. 3Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. 4Die oder der Bundesbeauftragte kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

(3) 1Die Befugnisse der oder des Bundesbeauftragten erstrecken sich auch auf 1.
von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und
2.
personenbezogene Daten, die einem besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.
2Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.
(4) Die öffentlichen Stellen des Bundes sind verpflichtet, der oder dem Bundesbeauftragten und ihren oder seinen Beauftragten 1.
jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren und
2.
alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen.

(5) 1Die oder der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 40 hin. 2§ 40 Absatz 3 Satz 1 zweiter Halbsatz gilt entsprechend.

*Kapitel 5 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union*

§ 17 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

(1) 1Gemeinsamer Vertreter im Europäischen Datenschutzausschuss und zentrale Anlaufstelle ist die oder der Bundesbeauftragte (gemeinsamer Vertreter). 2Als Stellvertreterin oder Stellvertreter des gemeinsamen Vertreters wählt der Bundesrat eine Leiterin oder einen Leiter der Aufsichtsbehörde eines Landes (Stellvertreter). 3Die Wahl erfolgt für fünf Jahre. 4Mit dem Ausscheiden aus dem Amt als Leiterin oder Leiter der Aufsichtsbehörde eines Landes endet zugleich die Funktion als Stellvertreter. 5Wiederwahl ist zulässig.

(2) Der gemeinsame Vertreter überträgt in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder allein das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss.

§ 18 Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

(1) 1Die oder der Bundesbeauftragte und die Aufsichtsbehörden der Länder (Aufsichtsbehörden des Bundes und der Länder) arbeiten in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zusammen. 2Vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Europäische Kommission oder den Europäischen Datenschutzausschuss geben sich die Aufsichtsbehörden des Bundes und der Länder frühzeitig Gelegenheit zur Stellungnahme. 3Zu diesem Zweck tauschen sie untereinander alle zweckdienlichen Informationen aus. 4Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikel 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.

(2) 1Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vor. 2Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, legt in Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder allein das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, der Stellvertreter den Vorschlag für einen gemeinsamen Standpunkt fest. 3In den übrigen Fällen fehlenden Einvernehmens nach Satz 2 legt der gemeinsame Vertreter den Standpunkt fest. 4Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. 5Der Bund und jedes Land haben jeweils eine Stimme. 6Enthaltungen werden nicht gezählt.

(3) 1Der gemeinsame Vertreter und dessen Stellvertreter sind an den gemeinsamen Standpunkt nach den Absätzen 1 und 2 gebunden und legen unter Beachtung dieses Standpunktes einvernehmlich die jeweilige Verhandlungsführung fest. 2Sollte ein Einvernehmen nicht erreicht werden, entscheidet in den in § 18 Absatz 2 Satz 2 genannten Angelegenheiten der Stellvertreter über die weitere Verhandlungsführung. 3In den übrigen Fällen gibt die Stimme des gemeinsamen Vertreters den Ausschlag.

§ 19 Zuständigkeiten

(1) 1Federführende Aufsichtsbehörde eines Landes im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der Verordnung (EU) 2016/679 ist die Aufsichtsbehörde des Landes, in dem der Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung im Sinne des Artikels 4 Nummer 16 der Verordnung (EU) 2016/679 oder seine einzige Niederlassung in der Europäischen Union im Sinne des Artikels 56 Absatz 1 der Verordnung (EU) 2016/679 hat. 2Im Zuständigkeitsbereich der oder des Bundesbeauftragten gilt Artikel 56 Absatz 1 in Verbindung mit Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 entsprechend. 3Besteht über

die Federführung kein Einvernehmen, findet für die Festlegung der federführenden Aufsichtsbehörde das Verfahren des § 18 Absatz 2 entsprechende Anwendung.

(2) 1Die Aufsichtsbehörde, bei der eine betroffene Person Beschwerde eingereicht hat, gibt die Beschwerde an die federführende Aufsichtsbehörde nach Absatz 1, in Ermangelung einer solchen an die Aufsichtsbehörde eines Landes ab, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. 2Wird eine Beschwerde bei einer sachlich unzuständigen Aufsichtsbehörde eingereicht, gibt diese, sofern eine Abgabe nach Satz 1 nicht in Betracht kommt, die Beschwerde an die Aufsichtsbehörde am Wohnsitz des Beschwerdeführers ab. 3Die empfangende Aufsichtsbehörde gilt als die Aufsichtsbehörde nach Maßgabe des Kapitels VII der Verordnung (EU) 2016/679, bei der die Beschwerde eingereicht worden ist, und kommt den Verpflichtungen aus Artikel 60 Absatz 7 bis 9 und Artikel 65 Absatz 6 der Verordnung (EU) 2016/679 nach.

*Kapitel 6 Rechtsbehelfe*

§ 20 Gerichtlicher Rechtsschutz

(1) 1Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und einer Aufsichtsbehörde des Bundes oder eines Landes über Rechte gemäß Artikel 78 Absatz 1 und 2 der Verordnung (EU) 2016/679 sowie § 61 ist der Verwaltungsrechtsweg gegeben. 2Satz 1 gilt nicht für Bußgeldverfahren.

(2) Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 7 anzuwenden.

(3) Für Verfahren nach Absatz 1 Satz 1 ist das Verwaltungsgericht örtlich zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat.

(4) In Verfahren nach Absatz 1 Satz 1 ist die Aufsichtsbehörde beteiligungsfähig.

(5) 1Beteiligte eines Verfahrens nach Absatz 1 Satz 1 sind 1.
die natürliche oder juristische Person als Klägerin oder Antragstellerin und
2.
die Aufsichtsbehörde als Beklagte oder Antragsgegnerin.
2§ 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt.
(6) Ein Vorverfahren findet nicht statt.

(7) Die Aufsichtsbehörde darf gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der Verwaltungsgerichtsordnung anordnen.

§ 21 Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen.

(2) 1Für Verfahren nach Absatz 1 ist der Verwaltungsrechtsweg gegeben. 2Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 6 anzuwenden.

(3) Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.

(4) 1In Verfahren nach Absatz 1 ist die Aufsichtsbehörde beteiligungsfähig. 2An einem Verfahren nach Absatz 1 ist die Aufsichtsbehörde als Antragstellerin beteiligt; § 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt. 3Das Bundesverwaltungsgericht kann der Europäischen Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit eines Beschlusses der Europäischen Kommission nach Absatz 1 bei dem Gerichtshof der Europäischen Union anhängig, so kann das Bundesverwaltungsgericht anord-

nen, dass die Verhandlung bis zur Erledigung des Verfahrens vor dem Gerichtshof der Europäischen Union auszusetzen sei.

(6) 1In Verfahren nach Absatz 1 ist § 47 Absatz 5 Satz 1 und Absatz 6 der Verwaltungsgerichtsordnung entsprechend anzuwenden. 2Kommt das Bundesverwaltungsgericht zu der Überzeugung, dass der Beschluss der Europäischen Kommission nach Absatz 1 gültig ist, so stellt es dies in seiner Entscheidung fest. 3Andernfalls legt es die Frage nach der Gültigkeit des Beschlusses gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor

## Teil 2 Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 (§§ 22-44)

*Kapitel 1 Rechtsgrundlagen der Verarbeitung personenbezogener Daten*

Abschnitt 1 Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

### § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig 1.
durch öffentliche und nichtöffentliche Stellen, wenn sie a)
erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,
b)
zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder
c)
aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,
2.
durch öffentliche Stellen, wenn sie a)
aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist,
b)
zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
c)
zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist oder
d)
aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist

und soweit die Interessen des Verantwortlichen an der Datenverarbeitung in den Fällen der Nummer 2 die Interessen der betroffenen Person überwiegen.

(2) 1In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. 2Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören: 1.

technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2.
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3.
Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4.
Benennung einer oder eines Datenschutzbeauftragten,
5.
Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6.
Pseudonymisierung personenbezogener Daten,
7.
Verschlüsselung personenbezogener Daten,
8.
Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9.
zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10.
spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

§ 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn 1.
offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2.
Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3.
sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
4.
sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
5.
sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
6.
sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 24 Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig, wenn 1.

sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder
2.
sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist,
sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.
(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 25 Datenübermittlungen durch öffentliche Stellen

(1) 1Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden. 2Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. 3Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 23 zulässig.

(2) 1Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nichtöffentliche Stellen ist zulässig, wenn 1.
sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden,
2.
der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder
3.
es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist
und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. 2Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.
(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Voraussetzungen des Absatzes 1 oder 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

Abschnitt 2 Besondere Verarbeitungssituationen

§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) 1Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. 2Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) 1Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. 2Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. 3Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. 4Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) 1Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. 2Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. 3§ 22 Absatz 2 gilt entsprechend.

(4) 1Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. 2Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(8) 1Beschäftigte im Sinne dieses Gesetzes sind: 1.
Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2.
zu ihrer Berufsbildung Beschäftigte,
3.
Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4.
in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5.
Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6.
Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7.
Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.
2Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.
zur Einzelansicht

§ 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) 1Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. 2Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) 1Die in den Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. 2Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU)

2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) 1Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. 2Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. 3Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 28 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) 1Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. 2Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) 1Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. 2Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. 3Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18 Absatz 1 Buchstabe a, b und d, den Artikel 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 29 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

(1) 1Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. 2Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. 3Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. 4Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(3) 1Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem

Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. 2Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

§ 30 Verbraucherkredite

(1) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(2) 1Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 1 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. 2Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. 3§ 37 bleibt unberührt.

§ 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

(1) Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, wenn 1.
die Vorschriften des Datenschutzrechts eingehalten wurden,
2.
die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
3.
für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt wurden und
4.
im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

(2) 1Die Verwendung eines von Auskunfteien ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen nur zulässig, soweit die Voraussetzungen nach Absatz 1 vorliegen und nur solche Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, berücksichtigt werden, 1.
die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2.
die nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden sind,
3.
die der Schuldner ausdrücklich anerkannt hat,
4.
bei denen a)
der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
b)
die erste Mahnung mindestens vier Wochen zurückliegt,
c)
der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist und
d)
der Schuldner die Forderung nicht bestritten hat oder
5.
deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist.
2Die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.

*Kapitel 2 Rechte der betroffenen Person*

§ 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung 1.
eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,
2.
im Fall einer öffentlichen Stelle die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,
3.
die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,
4.
die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder
5.
eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

(2) 1Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. 2Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. 3Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 4 und 5 keine Anwendung.

(3) Unterbleibt die Benachrichtigung in den Fällen des Absatzes 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 33 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information 1.
im Fall einer öffentlichen Stelle a)
die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde oder
b)
die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde
und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss, 2.
im Fall einer nichtöffentlichen Stelle a)
die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder
b)

die zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde; im Fall der Datenverarbeitung für Zwecke der Strafverfolgung bedarf es keiner Feststellung nach dem ersten Halbsatz.

(2) 1Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. 2Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

§ 34 Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn
1.
die betroffene Person nach § 33 Absatz 1 Nummer 1, 2 Buchstabe b oder Absatz 3 nicht zu informieren ist, oder
2.
die Daten a)
nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder
b)
ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen

und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) 1Die Gründe der Auskunftsverweigerung sind zu dokumentieren. 2Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. 3Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.

(3) 1Wird der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. 2Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

§ 35 Recht auf Löschung

(1) 1Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. 2In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verord-

nung (EU) 2016/679. 3Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) 1Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 gilt Absatz 1 Satz 1 und 2 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. 2Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 gilt Absatz 1 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.

§ 36 Widerspruchsrecht

Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 37 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und 1.
dem Begehren der betroffenen Person stattgegeben wurde oder
2.
die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens zum Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

(2) 1Entscheidungen nach Absatz 1 dürfen auf der Verarbeitung von Gesundheitsdaten im Sinne des Artikels 4 Nummer 15 der Verordnung (EU) 2016/679 beruhen. 2Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

*Kapitel 3 Pflichten der Verantwortlichen und Auftragsverarbeiter*

§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen

(1) 1Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. 2Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

§ 39 Akkreditierung

1Die Erteilung der Befugnis, als Zertifizierungsstelle gemäß Artikel 43 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 tätig zu werden, erfolgt durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle. 2§ 2 Absatz 3 Satz 2, § 4 Absatz 3 und § 10 Absatz 1 Satz 1 Nummer 3 des Akkreditierungsstellengesetzes finden mit der Maßgabe Anwendung, dass der Datenschutz als ein dem Anwendungsbereich des § 1 Absatz 2 Satz 2 unterfallender Bereich gilt.

*Kapitel 4 Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen*

§ 40 Aufsichtsbehörden der Länder

(1) Die nach Landesrecht zuständigen Behörden überwachen im Anwendungsbereich der Verordnung (EU) 2016/679 bei den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz.

(2) 1Hat der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen, findet für die Bestimmung der zuständigen Aufsichtsbehörde Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 entsprechende Anwendung. 2Wenn sich mehrere Behörden für zuständig oder für unzuständig halten oder wenn die Zuständigkeit aus anderen Gründen zweifelhaft ist, treffen die Aufsichtsbehörden die Entscheidung gemeinsam nach Maßgabe des § 18 Absatz 2. 3§ 3 Absatz 3 und 4 des Verwaltungsverfahrensgesetzes findet entsprechende Anwendung.

(3) 1Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten; hierbei darf sie Daten an andere Aufsichtsbehörden übermitteln. 2Eine Verarbeitung zu einem anderen Zweck ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn 1.
offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2.
sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist oder
3.
sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist.
3Stellt die Aufsichtsbehörde einen Verstoß gegen die Vorschriften über den Datenschutz fest, so ist sie befugt, die betroffenen Personen hierüber zu unterrichten, den Verstoß anderen für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. 4§ 13 Absatz 4 Satz 4 bis 7 gilt entsprechend.
(4) 1Die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben einer Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. 2Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. 3Der Auskunftspflichtige ist darauf hinzuweisen.

(5) 1Die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. 2Die Stelle ist insoweit zur Duldung verpflichtet. 3§ 16 Absatz 4 gilt entsprechend.

(6) 1Die Aufsichtsbehörden beraten und unterstützen die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. 2Sie können die Abberufung der oder des Datenschutzbeauftragten verlangen, wenn sie oder er die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Artikels 38 Absatz 6 der Verordnung (EU) 2016/679 ein schwerwiegender Interessenkonflikt vorliegt.

(7) Die Anwendung der Gewerbeordnung bleibt unberührt.

*Kapitel 5 Sanktionen*

§ 41 Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) 1Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. 2Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. 3§ 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn die festgesetzte Geldbuße den Betrag von einhunderttausend Euro übersteigt.

(2) 1Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. 2Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. 3§ 69 Absatz 4 Satz 2 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann.

§ 42 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, 1.
einem Dritten übermittelt oder
2.
auf andere Art und Weise zugänglich macht
und hierbei gewerbsmäßig handelt.
(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, 1.
ohne hierzu berechtigt zu sein, verarbeitet oder
2.
durch unrichtige Angaben erschleicht
und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
(3) 1Die Tat wird nur auf Antrag verfolgt. 2Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig 1.
entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2.
entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

*Kapitel 6 Rechtsbehelfe*

§ 44 Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

(1) 1Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person können bei dem Gericht des Ortes erhoben werden, an dem sich eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters befindet. 2Klagen nach Satz 1 können auch bei dem Gericht des Ortes erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.

(2) Absatz 1 gilt nicht für Klagen gegen Behörden, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden sind.

(3) 1Hat der Verantwortliche oder Auftragsverarbeiter einen Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt, gilt dieser auch als bevollmächtigt, Zustellungen in zivilgerichtlichen Verfahren nach Absatz 1 entgegenzunehmen. 2§ 184 der Zivilprozessordnung bleibt unberührt.

**Teil 3 Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 (§§45-85)**

*Kapitel 1 Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten*

§ 45 Anwendungsbereich

1Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. 2Die öffentlichen Stellen gelten dabei als Verantwortliche. 3Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. 4Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen, von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind. 5Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 46 Begriffsbestimmungen

Es bezeichnen die Begriffe: 1.
„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;
2.
„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3.
„Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
4.
„Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben,

der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
5.
„Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;
6.
„Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
7.
„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
8.
„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
9.
„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
10.
„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;
11.
„genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;
12.
„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;
13.
„Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
14.
„besondere Kategorien personenbezogener Daten“ a)
Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
b)
genetische Daten,
c)
biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
d)
Gesundheitsdaten und
e)
Daten zum Sexualleben oder zur sexuellen Orientierung;
15.
„Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;
16.
„internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

17.
„Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 47 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen 1.
auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2.
für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3.
dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,
4.
sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5.
nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
6.
in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

*Kapitel 2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten*

§ 48 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) 1Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. 2Geeignete Garantien können insbesondere sein 1.
spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,
2.
die Festlegung von besonderen Aussonderungsprüffristen,
3.
die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4.
die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,
5.
die von anderen Daten getrennte Verarbeitung,
6.
die Pseudonymisierung personenbezogener Daten,
7.
die Verschlüsselung personenbezogener Daten oder
8.
spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 49 Verarbeitung zu anderen Zwecken

1Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 genannten Zwecke handelt, der

Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. 2Die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 50 Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

1Personenbezogene Daten dürfen im Rahmen der in § 45 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. 2Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 51 Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) 1Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. 2Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. 3Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) 1Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. 2Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. 3Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. 4Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 52 Verarbeitung auf Weisung des Verantwortlichen

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 53 Datengeheimnis

1Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). 2Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. 3Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 54 Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

*Kapitel 3 Rechte der betroffenen Person*

§ 55 Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über 1.
die Zwecke der von ihm vorgenommenen Verarbeitungen,
2.
die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
3.
den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,
4.
das Recht, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, und
5.
die Erreichbarkeit der oder des Bundesbeauftragten.

§ 56 Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten: 1.
die in § 55 genannten Angaben,
2.
die Rechtsgrundlage der Verarbeitung,
3.
die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4.
gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5.
erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls 1.
die Erfüllung der in § 45 genannten Aufgaben,
2.
die öffentliche Sicherheit oder
3.
Rechtsgüter Dritter
gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.
(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 57 Absatz 7 entsprechend.

§ 57 Auskunftsrecht

(1) 1Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. 2Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über 1.
die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2.
die verfügbaren Informationen über die Herkunft der Daten,
3.
die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4.

die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,
5.
die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6.
das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,
7.
das Recht nach § 60, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, sowie
8.
Angaben zur Erreichbarkeit der oder des Bundesbeauftragten.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Von der Auskunftserteilung ist abzusehen, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 56 Absatz 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) 1Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. 2Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 56 Absatz 2 mit sich bringen würde. 3Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) 1Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Bundesbeauftragte oder den Bundesbeauftragten ausüben. 2Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 60 die Bundesbeauftragte oder den Bundesbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. 3Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. 4Die oder der Bundesbeauftragte hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie stattgefunden hat. 5Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. 6Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. 7Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. 8Die oder der Bundesbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 58 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) 1Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. 2Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. 3Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. 4In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wie-

der aufhebt. 5Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) 1Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn 1.
Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2.
die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 45 dienen, weiter aufbewahrt werden müssen oder
3.
eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.
2In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.
(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) 1Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. 2In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. 3Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(6) 1Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. 2Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 56 Absatz 2 mit sich bringen würde. 3Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(7) § 57 Absatz 7 und 8 findet entsprechende Anwendung.

§ 59 Verfahren für die Ausübung der Rechte der betroffenen Person

(1) 1Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. 2Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 57 Absatz 6 und des § 58 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) 1Die Erteilung von Informationen nach § 55, die Benachrichtigungen nach den §§ 56 und 66 und die Bearbeitung von Anträgen nach den §§ 57 und 58 erfolgen unentgeltlich. 2Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 57 und 58 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. 3In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 57 oder 58 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 60 Anrufung der oder des Bundesbeauftragten

(1) 1Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Bundesbeauftragte oder den Bundesbeauftragten wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 45 genannten Zwecken in ihren Rechten verletzt worden zu sein. 2Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese

die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. 3Die oder der Bundesbeauftragte hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 61 hinzuweisen.

(2) 1Die oder der Bundesbeauftragte hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiterzuleiten. 2Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 61 Rechtsschutz gegen Entscheidungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine verbindliche Entscheidung der oder des Bundesbeauftragten vorgehen.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Bundesbeauftragte mit einer Beschwerde nach § 60 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

*Kapitel 4 Pflichten der Verantwortlichen und Auftragsverarbeiter*

§ 62 Auftragsverarbeitung

(1) 1Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. 2Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) 1Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. 2Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. 3Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) 1Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. 2Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) 1Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. 2Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter 1.
nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;
2.
gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3.

den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;
4.
alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
5.
dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 76 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6.
Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;
7.
die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
8.
alle gemäß § 64 erforderlichen Maßnahmen ergreift und
9.
unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 64 bis 67 und § 69 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 63 Gemeinsam Verantwortliche

1Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. 2Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. 3Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. 4Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 64 Anforderungen an die Sicherheit der Datenverarbeitung

(1) 1Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. 2Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) 1Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. 2Die Maßnahmen nach Absatz 1 sollen dazu führen, dass 1.
die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2.
die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) 1Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken: 1.
Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2.

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3.
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4.
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5.
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6.
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7.
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8.
Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9.
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10.
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11.
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12.
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13.
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14.
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).
2Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 65 Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten

(1) 1Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Bundesbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. 2Erfolgt die Meldung an die Bundesbeauftragte oder den Bundesbeauftragten nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten: 1.
eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2.
den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,

3.
eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
4.
eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) 1Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. 2Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 42 Absatz 4 findet entsprechende Anwendung.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 66 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 65 Absatz 3 Nummer 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Von der Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn 1.
der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;

2.
der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Absatzes 1 mehr besteht, oder
3.
dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) 1Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Bundesbeauftragte förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. 2Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Absatzes 1 zur Folge hat.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 56 Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatzes 1 überwiegen.

(6) § 42 Absatz 4 findet entsprechende Anwendung.

§ 67 Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten: 1.
eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2.
eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3.
eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
4.
die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 68 Zusammenarbeit mit der oder dem Bundesbeauftragten

Der Verantwortliche hat mit der oder dem Bundesbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 69 Anhörung der oder des Bundesbeauftragten

(1) 1Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Bundesbeauftragte oder den Bundesbeauftragten anzuhören, wenn 1.
aus einer Datenschutz-Folgenabschätzung nach § 67 hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder
2.
die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.
2Die oder der Bundesbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.
(2) 1Der oder dem Bundesbeauftragten sind im Fall des Absatzes 1 vorzulegen: 1.
die nach § 67 durchgeführte Datenschutz-Folgenabschätzung,
2.
gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3.
Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,
4.
Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5.
Name und Kontaktdaten der oder des Datenschutzbeauftragten.
2Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) 1Falls die oder der Bundesbeauftragte der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. 2Die oder der Bundesbeauftragte kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. 3Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

(4) 1Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. 2In diesem Fall sind die Empfehlungen der oder des Bundesbeauftragten im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 70 Verzeichnis von Verarbeitungstätigkeiten

(1) 1Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. 2Dieses Verzeichnis hat die folgenden Angaben zu enthalten: 1.
den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,
2.
die Zwecke der Verarbeitung,
3.
die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4.
eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5.
gegebenenfalls die Verwendung von Profiling,
6.
gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7.
Angaben über die Rechtsgrundlage der Verarbeitung,
8.
die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9.
eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat: 1.
den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls der oder des Datenschutzbeauftragten,
2.
gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und
3.
eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Bundesbeauftragten zur Verfügung zu stellen.

§ 71 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) 1Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. 2Er hat hierbei den

Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. 3Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. 4Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren
, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) 1Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. 2Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. 3Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 72 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

1Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. 2Dies betrifft insbesondere folgende Kategorien: 1.
Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,
2.
Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,
3.
verurteilte Straftäter,
4.
Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5.
andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummer 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 73 Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

1Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. 2Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. 3Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 74 Verfahren bei Übermittlungen

(1) 1Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. 2Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. 3Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) 1Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. 2Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 75 Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) 1§ 58 Absatz 3 bis 5 ist entsprechend anzuwenden. 2Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 76 Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren: 1.
Erhebung,
2.
Veränderung,
3.
Abfrage,
4.
Offenlegung einschließlich Übermittlung,
5.
Kombination und
6.
Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die Bundesbeauftragte oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

§ 77 Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

*Kapitel 5 Datenübermittlungen an Drittstaaten und an internationale Organisationen*

§ 78 Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn 1.
die Stelle oder internationale Organisation für die in § 45 genannten Zwecke zuständig ist und
2.
die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) 1Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nummer 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. 2Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) 1Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. 2Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. 3Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) 1Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. 2Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. 3Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. 4Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 79 Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 78 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 auch dann zulässig, wenn 1.
in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2.
der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) 1Der Verantwortliche hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. 2Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. 3Sie ist der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

(3) 1Der Verantwortliche hat die Bundesbeauftragte oder den Bundesbeauftragten zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. 2In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 80 Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 78 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 79 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 auch dann zulässig, wenn die Übermittlung erforderlich ist
1.
zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2.
zur Wahrung berechtigter Interessen der betroffenen Person,
3.
zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4.
im Einzelfall für die in § 45 genannten Zwecke oder
5.

im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 45 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 79 Absatz 2 entsprechend.

§ 81 Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 78 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und 1.
im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2.
die Übermittlung an die in § 78 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3.
der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 78 Absatz 1 Nummer 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 79 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

*Kapitel 6 Zusammenarbeit der Aufsichtsbehörden*

§ 82 Gegenseitige Amtshilfe

(1) 1Die oder der Bundesbeauftragte hat den Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. 2Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Bundesbeauftragte hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Bundesbeauftragte darf Amtshilfeersuchen nur ablehnen, wenn 1.
sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder
2.
ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) 1Die oder der Bundesbeauftragte hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. 2Sie oder er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Bundesbeauftragte hat die Informationen, um die sie oder er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Bundesbeauftragte hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) 1Ein Amtshilfeersuchen der oder des Bundesbeauftragten hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. 2Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

*Kapitel 7 Haftung und Sanktionen*

§ 83 Schadensersatz und Entschädigung

(1) 1Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. 2Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(5) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 84 Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 45 Satz 1, 3 oder 4 findet § 42 entsprechende Anwendung.

**Teil 4 Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten (§ 85)**

§ 85 Verarbeitung personenbezogener Daten im Rahmen von nicht in die Anwendungs- bereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

(1) 1Die Übermittlung personenbezogener Daten an einen Drittstaat oder an über- oder zwischenstaatliche Stellen oder internationale Organisationen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten ist über die bereits gemäß der Verordnung (EU) 2016/679 zulässigen Fälle hinaus auch dann zulässig, wenn sie zur Erfüllung eigener Aufgaben aus zwingenden Gründen der Verteidigung oder zur Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist. 2Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden.

(2) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung gilt § 16 Absatz 4 nicht, soweit das Bundesministerium der Verteidigung im Einzelfall feststellt, dass die Erfüllung der dort genannten Pflichten die Sicherheit des Bundes gefährden würde.

(3) 1Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch öffentliche Stellen des Bundes besteht keine Informationspflicht gemäß Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679, wenn 1.
es sich um Fälle des § 32 Absatz 1 Nummer 1 bis 3 handelt oder

2.
durch ihre Erfüllung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse der betroffenen Person an der Erteilung der Information zurücktreten muss.
2Ist die betroffene Person in den Fällen des Satzes 1 nicht zu informieren, besteht auch kein Recht auf Auskunft.
3§ 32 Absatz 2 und § 33 Absatz 2 finden keine Anwendung.

## B. Urteile

### I) BVerfGE

### 1) BVerfGE 65, 1 – Volkszählung

*a) Sachverhalt*

Die Verfassungsbeschwerden richteten sich unmittelbar gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. 3. 1982 (BGBl I, 369) - VZG 1983 -. Es regelt in den §§ 1 bis 8 Programm und Durchführung der Erhebung; § 9 enthält besondere Regelungen über die Verwendung und Übermittlung der erhobenen Daten.
(Zusammenfassung nach NJW 1984, 419, beck-online)

*b) Leitsätze*

**1.** Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
**2.** Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.
**3.** Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.
Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.
**4.** Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§ 2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der PersönBVerfGE 65, 1 (1)BVerfGE 65, 1 (2)lichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung.
**5.** Die in VoZählG 1983 § 9 Abs. 1 bis 3 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (VoZählG 1983 § 9 Abs. 4) ist mit dem Grundgesetz vereinbar.
(Bearbeitung, zuletzt am 25. Sep. 2017, durch: A. Tschentscher; Sven Broichhagen, http://www.servat.unibe.ch/dfr/bv065001.html )

*c) Begründung*

Die Verfassungsbeschwerden sind - soweit zulässig - teilweise begründet. […]
II.
Prüfungsmaßstab ist in erster Linie das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht.
151
1. a) Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient - neben speziellen Freiheitsverbürgungen - das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann (vgl. BVerfGE 54, 148 [153]). Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend. Es umfaßt - wie bereits in der BVerfGE 65, 1 (41)BVerfGE 65, 1 (42)Entscheidung BVerfGE 54, 148 (155) unter Fortführung früherer Entscheidungen (BVerfGE 27, 1 [6] - Mikrozensus; 27, 344 [350f] - Scheidungsakten; 32, 373 [379] - Arztkartei; 35, 202 [220] - Lebach; 44, 353 [372f] - Suchtkrankenberatungsstelle) angedeutet worden ist - auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. ferner BVerfGE 56, 37 [41 ff.] - Selbstbezichtigung; 63, 131 [142f] - Gegendarstellung).
152

Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.

153

Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung BVerfGE 65, 1 (42)BVerfGE 65, 1 (43)tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

154

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

155

b) Dieses Recht auf "informationelle Selbstbestimmung" ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über BVerfGE 65, 1 (43)BVerfGE 65, 1 (44)"seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351f]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.

156

Diese Beschränkungen bedürfen nach Art. 2 Abs. 1 GG - wie in § 6 Abs. 1 des Bundesstatistikgesetzes auch zutreffend anerkannt worden ist - einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 45, 400 [420] m.w.N.). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist (BVerfGE 19, 342 [348]; st Rspr). Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (vgl. BVerfGE 53, 30 [65]; 63, 131 [143]).

157

2. Die Verfassungsbeschwerden geben keinen Anlaß zur erschöpfenden Erörterung des Rechts auf informationelle SelbstBVerfGE 65, 1 (44)BVerfGE 65, 1 (45)bestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr.

158

Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. Dabei ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben und verarbeitet werden (dazu unter a), und solchen, die für statistische Zwecke bestimmt sind (dazu unter b).

159

a) Schon bislang ist anerkannt, daß die zwangsweise Erhebung personenbezogener Daten nicht unbeschränkt statthaft ist, namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder der Gewährung von Sozialleistungen) verwendet werden sollen. Insoweit hat der Gesetzgeber bereits verschiedenartige Maßnahmen zum Schutz der Betroffenen vorgesehen, die in die verfassungsrechtlich gebotene Richtung weisen (vgl. beispielsweise die Regelungen in den Datenschutzgesetzen des Bundes und der Länder; §§ 30, 31 der Abgabenordnung - AO -; § 35 des Ersten Buches des Sozialgesetzbuches - SGB I - in Verbindung mit §§ 67 bis 86 SGB X). Wieweit das BVerfGE 65, 1 (45)BVerfGE 65, 1 (46)Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit sowie die Pflicht zu verfahrensrechtlichen Vorkehrungen den Gesetzgeber zu diesen Regelungen von Verfassungs wegen zwingen, hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Mißbrauchs ab (vgl. BVerfGE 49, 89 [142]; 53, 30 [61]). Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen. Nach dem bisherigen Erkenntnisstand und Erfahrungsstand erscheinen vor allem folgende Maßnahmen bedeutsam:

160

Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.

161

Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich.

162

Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.

163

BVerfGE 65, 1 (46)BVerfGE 65, 1 (47)b) Die Erhebung und Verarbeitung von Daten für statistische Zwecke weisen Besonderheiten auf, die bei der verfassungsrechtlichen Beurteilung nicht außer acht bleiben können.

164

aa) Die Statistik hat erhebliche Bedeutung für eine staatliche Politik, die den Prinzipien und Richtlinien des Grundgesetzes verpflichtet ist. Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, bedarf es einer umfassenden, kontinuierlichen sowie laufend aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammenhänge. Erst die Kenntnis der relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe der Chancen, die eine automatische Datenverarbeitung bietet, für die Statistik zu nutzen, schafft die für eine am Sozialstaatsprinzip orientierte staatliche Politik unentbehrliche Handlungsgrundlage (vgl. BVerfGE 27, 1 [9]).

165

Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. es gehört zum Wesen der Statistik, daß die Daten nach ihrer statistischen Aufbereitung für die

verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden sollen; demgemäß besteht auch ein Bedürfnis nach Vorratsspeicherung. Das Gebot einer konkreten Zweckumschreibung und das strikte Verbot der Sammlung personenbezogener Daten auf Vorrat kann nur für Datenerhebungen zu nichtstatistischen Zwecken gelten, nicht jedoch bei einer Volkszählung, die eine gesicherte Datenbasis für weitere statistische Untersuchungen ebenso wie für den politischen Planungsprozeß durch eine verläßliche Feststellung der Zahl und der Sozialstruktur der Bevölkerung vermitteln soll. Die Volkszählung muß Mehrzweckerhebung und Mehrzweckverarbeitung, also Datensammlung und Datenspeicherung auf Vorrat sein, wenn der Staat den Entwicklungen der industriellen Gesellschaft nicht unvorbereitet begegnen soll. Auch wären Weitergabeverbote und Verwertungsverbote für statistisch aufbereitete Daten zweckwidrig.

166

BVerfGE 65, 1 (47)BVerfGE 65, 1 (48)bb) Ist die Vielfalt der Verwendungsmöglichkeiten und Verknüpfungsmöglichkeiten damit bei der Statistik von der Natur der Sache her nicht im voraus bestimmbar, müssen der Informationserhebung und Informationsverarbeitung innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen. Es müssen klar definierte Verarbeitungsvoraussetzungen geschaffen werden, die sicherstellen, daß der Einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird. Beides, die mangelnde Anbindung an einen bestimmten, jederzeit erkennbaren und nachvollziehbaren Zweck sowie die multifunktionale Verwendung der Daten, verstärkt die Tendenzen, welche durch die Datenschutzgesetze aufgefangen und eingeschränkt werden sollen, die das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung konkretisieren. Gerade weil es von vornherein an zweckorientierten Schranken fehlt, die den Datensatz eingrenzen, bringen Volkszählungen tendenziell die schon im Mikrozensus-Beschluß (BVerfGE 27, 1 [6]) hervorgehobene Gefahr einer persönlichkeitsfeindlichen Registrierung und Katalogisierung des Einzelnen mit sich. Deshalb sind an die Datenerhebung und Datenverarbeitung für statistische Zwecke besondere Anforderungen zum Schutz des Persönlichkeitsrechts der auskunftspflichtigen Bürger zu stellen.

167

Unbeschadet des multifunktionalen Charakters der Datenerhebung und Datenverarbeitung zu statistischen Zwecken ist Voraussetzung, daß diese allein als Hilfe zur Erfüllung öffentlicher Aufgaben erfolgen. Es kann auch hier nicht jede Angabe verlangt werden. Selbst bei der Erhebung von Einzelangaben, die für statistische Zwecke gebraucht werden, muß der Gesetzgeber schon bei der Anordnung der Auskunftspflicht prüfen, ob sie insbesondere für den Betroffenen die Gefahr der sozialen Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer) hervorrufen können und ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann. Dies dürfte beispielsweise bei dem in § 2 Nr. 8 VZG 1983 geBVerfGE 65, 1 (48)BVerfGE 65, 1 (49)regelten Erhebungstatbestand der Fall sein, wonach die Volkszählung und Berufszählung im Anstaltsbereich die Eigenschaft als Insasse oder die Zugehörigkeit zum Personal oder zum Kreis der Angehörigen des Personals erfaßt. Diese Erhebung soll Anhaltspunkte über die Belegung der Anstalten liefern (BTDrucks 9/451, S. 9). Ein solches Ziel ist - abgesehen von der Gefahr sozialer Etikettierung - auch ohne Personenbezug zu erreichen. Es genügt, daß der Leiter der Anstalt verpflichtet wird, zum Stichtag der Volkszählung die zahlenmäßige Belegung nach den in § 2 Nr. 8 VZG 1983 aufgeführten Merkmalen ohne jeden Bezug auf die einzelne Person mitzuteilen. Eine personenbezogene Erhebung des Tatbestandes des § 2 Nr. 8 VZG 1983 wäre deshalb von vornherein ein Verstoß gegen das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte Persönlichkeitsrecht.

168

Zur Sicherung des Rechts auf informationelle Selbstbestimmung bedarf es ferner besonderer Vorkehrungen für Durchführung und Organisation der Datenerhebung und Datenverarbeitung, da die Informationen während der Phase der Erhebung - und zum Teil auch während der Speicherung - noch individualisierbar sind; zugleich sind Löschungsregelungen für solche Angaben erforderlich, die als Hilfsangaben (Identifikationsmerkmale) verlangt wurden und die eine Deanonymisierung leicht ermöglichen würden, wie Name, Anschrift, Kennummer und Zählerliste (vgl. auch § 11 Abs. 7 Satz 1 BStatG). Von besonderer Bedeutung für statistische Erhebungen sind wirksame Abschottungsregelungen nach außen. Für den Schutz des Rechts auf informationelle Selbstbestimmung ist - und zwar auch schon für das Erhebungsverfahren - die strikte Geheimhaltung der zu statistischen Zwecken erhobenen Einzelangaben unverzichtbar, solange ein Personenbezug noch besteht oder herstellbar ist (Statistikgeheimnis); das gleiche gilt für das Gebot einer möglichst frühzeitigen (faktischen) Anonymisierung, verbunden mit Vorkehrungen gegen eine Deanonymisierung.

169

Erst die vom Recht auf informationelle Selbstbestimmung geforderte und gesetzlich abzusichernde Abschottung der Statistik BVerfGE 65, 1 (49)BVerfGE 65, 1 (50)durch Anonymisierung der Daten und deren Geheimhaltung, soweit sie zeitlich begrenzt noch einen Personenbezug aufweisen, öffnet den Zugang der staatlichen Organe zu den für die Planungsaufgaben erforderlichen Informationen. Nur unter dieser Voraussetzung kann und darf vom Bürger erwartet werden, die von ihm zwangsweise verlangten Auskünfte zu erteilen. Dürften personenbezogene Daten, die zu statistischen Zwecken erhoben wurden, gegen den Willen oder ohne Kenntnis des Betroffenen weitergeleitet werden, so würde das nicht nur das verfassungsrechtlich gesicherte Recht auf informationelle Selbstbestimmung unzulässig einschränken, sondern auch die vom Grundgesetz selbst in Art. 73 Nr. 11 vorgese-

hene und damit schutzwürdige amtliche Statistik gefährden. Für die Funktionsfähigkeit der amtlichen Statistik ist ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig. Dieses Ziel kann nur erreicht werden, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner für statistische Zwecke erhobenen Daten geschaffen wird, ohne welche seine Bereitschaft, wahrheitsgemäße Angaben zu machen, nicht herzustellen ist (so bereits zutreffend die Begründung der Bundesregierung zum Entwurf des Volkszählungsgesetzes 1950; vgl. BTDrucks I/982, S. 20 zu § 10). Eine Staatspraxis, die sich nicht um die Bildung eines solchen Vertrauens durch Offenlegung des Datenverarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Mißtrauen entstünde. Da staatlicher Zwang nur begrenzt wirksam werden kann, wird ein die Interessen der Bürger überspielendes staatliches Handeln allenfalls kurzfristig vorteilhaft erscheinen; auf Dauer gesehen wird es zu einer Verringerung des Umfangs und der Genauigkeit der Informationen führen (BTDrucks I/982, a.a.O.). Läßt sich die hochindustrialisierte Gesellschaften kennzeichnende ständige Zunahme an Komplexität der Umwelt nur mit Hilfe einer zuverlässigen Statistik aufschlüsseln und für gezielte staatliche Maßnahmen aufbereiten, so läuft die Gefährdung der amtlichen StaBVerfGE 65, 1 (50)BVerfGE 65, 1 (51)tistik darauf hinaus, eine wichtige Voraussetzung sozialstaatlicher Politik in Frage zu stellen. Kann damit nur durch eine Abschottung der Statistik die Staatsaufgabe "Planung" gewährleistet werden, ist das Prinzip der Geheimhaltung und möglichst frühzeitigen Anonymisierung der Daten nicht nur zum Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für die Statistik selbst konstitutiv.

170

cc) Wird den erörterten Anforderungen in wirksamer Weise Rechnung getragen, ist die Erhebung von Daten zu ausschließlich statistischen Zwecken nach dem derzeitigen Erkenntnisstand und Erfahrungsstand verfassungsrechtlich unbedenklich. Es ist nicht erkennbar, daß das Persönlichkeitsrecht der Bürger beeinträchtigt werden könnte, wenn die erhobenen Daten nach ihrer Anonymisierung oder statistischen Aufbereitung (vgl. § 11 Abs. 5 und 6 BStatG) von Statistischen Ämtern anderen staatlichen Organen oder sonstigen Stellen zur Verfügung gestellt werden.

171

Besondere Probleme wirft eine etwaige Übermittlung (Weitergabe) der weder anonymisierten noch statistisch aufbereiteten, also noch personenbezogenen Daten auf. Erhebungen zu statistischen Zwecken umfassen auch individualisierte Angaben über den einzelnen Bürger, die für die statistischen Zwecke nicht erforderlich sind und die - davon muß der befragte Bürger ausgehen können - lediglich als Hilfsmittel für das Erhebungsverfahren dienen. Alle diese Angaben dürfen zwar kraft ausdrücklicher gesetzlicher Ermächtigung weitergeleitet werden, soweit und sofern dies zur statistischen Aufbereitung durch andere Behörden geschieht und dabei die zum Schutz des Persönlichkeitsrechts gebotenen Vorkehrungen, insbesondere das Statistikgeheimnis und das Gebot der frühzeitigen Anonymisierung, ebenso durch Organisation und Verfahren zuverlässig sichergestellt sind wie bei den Statistischen Ämtern des Bundes und der Länder. Eine Weitergabe der für statistische Zwecke erhobenen, nicht anonymisierten oder statistisch aufbereiteten Daten für Zwecke des Verwaltungsvollzugs kann hingegen in unzulässiger Weise in das Recht auf BVerfGE 65, 1 (51)BVerfGE 65, 1 (52)informationelle Selbstbestimmung eingreifen (vgl. ferner unten C IV 1).

172

III.

Den dargelegten verfassungsrechtlichen Anforderungen genügt das Erhebungsprogramm des Volkszählungsgesetzes 1980 im wesentlichen. Gegenstand der Nachprüfung sind insoweit die §§ 2 bis 4 in Verbindung mit § 5 Abs. 1 des Gesetzes mit Ausnahme der Frage nach der Eigenschaft als Anstaltsinsasse oder der Zugehörigkeit zum Anstaltspersonal (§ 2 Nr. 8 in Verbindung mit § 5 Abs. 1 Nr. 1 Halbsatz 2). Diese Vorschriften sind mit dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG mit der Maßgabe vereinbar, daß der Gesetzgeber ergänzend für bisher fehlende grundrechtssichernde Organisationsregelungen und Verfahrensregelungen sorgt und damit die an eine Totalerhebung nach Art der Volkszählung 1983 zu stellenden verfassungsrechtlichen Anforderungen gewährleistet.

173

1. Das Volkszählungsgesetz 1983 verpflichtet in § 5 die Beschwerdeführer unter Androhung einer Geldbuße (§ 14 in Verbindung mit § 10 BStatG) zur Auskunft über die in § 2 Nr. 1 bis 7, §§ 3, 4 VZG 1983 genannten Erhebungstatbestände. Dadurch greift es in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete Persönlichkeitsrecht ein. Die erhobenen Daten sollen auch für künftige, zur Zeit der Erhebung noch nicht vorhersehbare Aufgaben nutzbar sein. Diesen Informationseingriff hat der Auskunftspflichtige hinzunehmen. Er erfolgt im überwiegenden Interesse der Allgemeinheit und genügt den Geboten der Normenklarheit und der Verhältnismäßigkeit.

174

a) Das Erhebungsprogramm des Volkszählungsgesetzes 1983 führt nicht zu einer mit der Würde des Menschen unvereinbaren gänzlichen oder teilweisen Registrierung und Katalogisierung der Persönlichkeit.

175

Volkszählungen, Wohnungszählungen, Berufszählungen und Arbeitsstättenzählungen sollen nach der Begründung des Regierungsentwurfs (BTDrucks. BVerfGE 65, 1 (52)BVerfGE 65, 1 (53)9/451, S. 7 ff.) Angaben über

den neuesten Stand der Bevölkerung, ihre räumliche Verteilung und ihre Zusammensetzung nach demographischen und sozialen Merkmalen sowie über ihre wirtschaftliche Betätigung, also im Ergebnis lediglich entpersönlichte Aussagen liefern.

176

Das Erhebungsprogramm vermag zwar einzelne Lebensbereiche, zum Beispiel den Wohnbereich des Bürgers, jedoch nicht dessen Persönlichkeit abzubilden. Etwas anderes würde nur gelten, soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre; denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig (BVerfGE 27, 1 [6]). Derartigen Datenverbindungen - Totalabbildern - steht schon § 11 BStatG entgegen, der sogar die Übermittlung von nicht anonymisierten Einzelangaben zwischen den mit der Durchführung einer Bundesstatistik betrauten Personen und Stellen nur erlaubt, soweit dies zur Erstellung der Bundesstatistik erforderlich ist (§ 11 Abs. 2 BStatG).

177

Die Zusammenführung von im Rahmen der Volkszählung 1983 erhobenen Daten oder deren Verbindung mit bei den Statistischen Ämtern bereits vorhandenen Informationen ermöglicht es auch nicht, Teilabbilder der Persönlichkeit anzufertigen, die mit der Würde des Menschen nicht vereinbar sind. Einmal muß sich die Verarbeitung und Verwendung der Daten innerhalb des mit der Bezeichnung als Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung gekennzeichneten und gesetzlich festgelegten Zweckes der Befragung bewegen; zum anderen gilt der die amtliche Statistik generell verpflichtende Grundsatz, daß die Aufbereitung der Individualdaten immer zu einer "strukturierten" - anonymen - Form führen muß, so daß im Ergebnis die ErstelBVerfGE 65, 1 (53)BVerfGE 65, 1 (54)lung von "Bildern" mit Persönlichkeitsbezug auch in der Form von Teilabbildern unzulässig ist.

178

b) Das Erhebungsprogramm des Volkszählungsgesetzes 1983 genügt auch dem Gebot der Normenklarheit.

179

Hinreichend bestimmt ist ein Gesetz, wenn sein Zweck aus dem Gesetzestext in Verbindung mit den Materialien deutlich wird (BVerfGE 27, 1 [8]); dabei reicht es aus, wenn sich der Gesetzeszweck aus dem Zusammenhang ergibt, in dem der Text des Gesetzes zu dem zu regelnden Lebensbereich steht (vgl. BVerfGE 62, 169 [183f]). Diesen Anforderungen genügt die Beschreibung der zu erhebenden Merkmale im Volkszählungsgesetz 1983; der Bürger kann erkennen, über welche Grundtatbestände der Sozialstruktur er befragt werden soll. Die Hauptzwecke lassen sich aus der Art der Erhebung - einer Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung -, dem Erhebungsprogramm und den Gesetzesmaterialien hinreichend deutlich entnehmen. Nicht erforderlich ist, daß der Gesetzgeber zu jeder einzelnen gesetzlichen Verpflichtung auch den konkreten Zweck im Gesetz selbst erläutert. Dies gilt namentlich mit Rücksicht auf die Besonderheiten der Erhebung von Daten für statistische Zwecke, zumal bei einer Volkszählung; hier ist eine Auflistung der einzelnen Zwecke aufgrund ihrer multifunktionalen Zielsetzung unmöglich.

180

c) Das Erhebungsprogramm des Volkszählungsgesetzes 1983 entspricht, soweit es Prüfungsgegenstand ist, auch dem Grundsatz der Verhältnismäßigkeit. Danach muß eine Maßnahme zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein; der mit ihr verbundene Eingriff darf seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den vom Bürger hinzunehmenden Einbußen stehen (vgl. BVerfGE 27, 344 [352 f.]; st. Rspr).

181

Das Volkszählungsgesetz 1983 soll dem Staat die für künftiges Planen und Handeln benötigten Informationen verschaffen. Als Vorbedingung für die Planmäßigkeit staatlichen Handelns (vgl. BVerfGE 27, 1 [7]) dient die Volkszählung 1983 einem einleuchBVerfGE 65, 1 (54)BVerfGE 65, 1 (55)tenden, zur Erfüllung legitimer Staatsaufgaben angestrebten Zweck.

182

Mit dem eingesetzten Mittel der Volkszählung als Totalerhebung (Vollerhebung) und dem Fragenkatalog des § 2 Nr. 1 bis 7 und der §§ 3, 4 VZG 1983 ist die Bundesrepublik Deutschland ihrer Verpflichtung aufgrund der Richtlinien des Rates der Europäischen Gemeinschaften vom 22. November 1973 zur Synchronisierung der allgemeinen Volkszählungen - 73/403/EWG - (ABlEG Nr. L 347 vom 17.12.1973, S. 50) nachgekommen. Erhebungsmethode und Erhebungsprogramm sind geeignet und erforderlich, um den angestrebten Zweck zu erreichen, und für die Auskunftspflichtigen zumutbar.

183

aa) Es ist derzeit nicht zu beanstanden, wenn der Gesetzgeber davon ausgegangen ist, daß Erhebungen aufgrund von Stichproben auf ausnahmslos freiwilliger Basis oder eine Kombination von Vollprobenerhebung und Stichprobenerhebung die Volkszählung als Totalerhebung nicht zu ersetzen vermögen. Diese Alternativen zu einer

Totalerhebung sind noch mit zu großen Fehlerquellen behaftet. Außerdem setzen sie verläßliche Daten über die Gesamtbevölkerung voraus, die zur Zeit nur periodische Volkszählungen liefern können.

184

Diese Würdigung beruht auf dem gegenwärtigen Erkenntnisstand und Erfahrungsstand. Vor künftigen Entscheidungen für eine Erhebung wird sich der Gesetzgeber erneut mit dem dann erreichten Stand der Methodendiskussion auseinandersetzen müssen, um festzustellen, ob und in welchem Umfang die herkömmlichen Methoden der Informationserhebung und Informationsverarbeitung beibehalten werden können. Die Methoden der amtlichen Statistik und der Sozialforschung entwickeln sich stetig weiter. Diese Entwicklung darf der Gesetzgeber nicht unberücksichtigt lassen. Er muß ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können (BVerfGE 50, 290 [334]); bei einer sich später zeigenden Fehlprognose ist er zur Korrektur verpflichtet (vgl. BVerfGE, BVerfGE 65, 1 (55)BVerfGE 65, 1 (56)a.a.O. [335]). Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein (vgl. BVerfGE 56, 54 [78f] m.w.N.). Ebenso muß er bei der Anordnung einer statistischen Erhebung anhand des erreichbaren Materials prüfen, ob eine Totalerhebung trotz einer inzwischen fortgeschrittenen Entwicklung der statistischen und sozialwissenschaftlichen Methoden noch verhältnismäßig ist. Es reicht insoweit zur Begründung nicht aus, lediglich darauf zu verweisen, daß Volkszählungen schon immer in Form von Totalerhebungen durchgeführt worden seien.

185

In diesem Sinne hat der Deutsche Bundestag in einem Beschluß vom 15. Dezember 1982 zum Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens (Mikrozensusgesetz) die Bundesregierung ersucht darzulegen (BTDrucks 9/2261, S. 3),

186

"1. in welchem Umfang auf Erhebungen nach dem Mikrozensusgesetz wegen Reduzierung oder Wegfalls der sachlichen Notwendigkeit dieser Erhebung verzichtet werden kann,

187

2. in welchem Umfang Erhebungen nach dem Mikrozensusgesetz durch weniger kostenintensive und gleichwertige oder bessere Umfragemethoden ersetzt werden können.

188

Dabei sollen auch die neuesten Erkenntnisse der empirischen Sozialforschung und die Erfahrungen mit statistischen Erhebungen im Ausland bewertet und sofern sie auf anderen Systemen beruhen, ihre Geeignetheit für die Bundesrepublik Deutschland geprüft werden."

189

Wie aus den Stellungnahmen mehrerer Datenschutzbeauftragter hervorgeht, wird neuerdings im Inland und Ausland diskutiert, ob auf Totalerhebungen verzichtet werden kann. Diese Diskussion wird der Gesetzgeber aufmerksam zu verfolgen haben. Zur Zeit liegen aber noch keine sicheren Ergebnisse vor, die das Mittel der Totalerhebung schon jetzt unverhältnismäßig erscheinen las-sen.

190

bb) Auch die Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung ist keine zulässige Alternative zu der vorgesehenen Totalzählung. Denn die Nutzung von Daten aus verschiedenen Registern und Dateien würde voraussetzen, BVerfGE 65, 1 (56)BVerfGE 65, 1 (57)daß technische, organisatorische und rechtliche Maßnahmen getroffen werden, die es erst erlauben, diese Daten, bezogen auf bestimmte Personen oder Institutionen, zusammenzuführen. Eine solche Maßnahme wäre zum Beispiel die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substituts. Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren. Die Verknüpfung vorhandener Dateien wäre danach auch nicht das mildere Mittel.

191

cc) Auch die bei Wahlen und Abstimmungen geläufigen, der Briefwahl nachgebildeten und damit anonymeren Erhebungsformen sind allgemein kein Ersatz für die vorgesehene Zählung.

192

Eine vollständige und regional richtige Feststellung der Einwohner, Gebäude, Wohnungen und Arbeitsstätten setzt eine Begehung des Gemeindegebietes voraus. Ein Postversand der Fragebogen erreicht nicht alle Auskunftspflichtigen. Denn es müßte hierbei auf Adressen in vorhandenen Registern zurückgegriffen werden, die in aller Regel die Situation am Zählungsstichtag nicht vollständig wiedergeben.

193

Ein gegenüber dem bisher vorgesehenen Volkszählungsverfahren milderes Mittel besteht jedoch darin, die Zähler die Fragebogen lediglich austeilen und eine Adressenliste anlegen zu lassen, in der Namen und Anschriften der Auskunftspflichtigen aufgeführt sind, die Fragebogen erhalten haben. Die Auskunftspflichtigen hätten dann die ausgefüllten Bögen in verschlossenem Umschlag dem Zähler zu übergeben, bei der Zählungsdienststelle abzugeben oder an diese zurückzusenden. Diese Erhebungsmethode vermeidet die Gefährdungen, die durch die Einsichtnahme der Zähler in die personenbezogenen Angaben der Bürger entstehen. Sie berücksichtigt andererseits, daß zur vollständigen und richtigen Zählung das Gemeindegebiet begangen werden muß, und ermöglicht es, Unstimmigkeiten durch Rückfragen zu klären.

194

Eine solche Erhebungsmethode läßt § 5 Abs. 1 VZG 1983 in Verbindung mit § 10 Abs. 2 und 3 BStatG zu. Die AuskunftsBVerfGE 65, 1 (57)BVerfGE 65, 1 (58)pflicht besteht nach § 10 Abs. 2 BStatG gegenüber den mit der Durchführung der Bundesstatistik amtlich betrauten Stellen und Personen. Nach § 10 Abs. 3 BStatG ist die Antwort unter anderem kostenfrei und portofrei zu erteilen. Die Auskunftspflicht kann somit auf dem Postwege erfüllt werden; der Bürger ist berechtigt, den Erhebungsbogen zur Volkszählung im verschlossenen Umschlag kostenfrei und portofrei an die Zählungsdienststellen zu senden. Eine andere Auslegung hätte zur Folge, daß die Erhebungsform der Volkszählung 1983 unverhältnismäßig wäre und deshalb das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verletzen würde.

195

dd) Die Erhebungstatbestände des § 2 Nr. 1 bis 7 und der §§ 3, 4 VZG 1983 sind auch in ihrer Gesamtheit erforderlich, um den Zweck der Volkszählung zu erreichen. Die Volkszählung soll ein vielseitiges koordiniertes statistisches Gesamtbild von Gesellschaft und Wirtschaft liefern. Dazu werden die Daten aus allen Zählungsteilen - für die Volkszählung und Berufszählung sowie für die Gebäudezählung, Wohnungszählung und Arbeitsstättenzählung - in Verbindung miteinander benötigt. Die Erhebungstatbestände des Volkszählungsgesetzes 1983 dienen in der Regel mehreren nicht abschließend zu benennenden Zwecken. Das jeweilige Merkmal darf aber nicht isoliert gesehen werden. Denn nur in der Kombination mit weiteren Merkmalen - in Abhängigkeit von den jeweiligen Fragestellungen - sind die vielfältigen von der Bundesregierung in ihrer Stellungnahme im einzelnen genannten Zwecke zu erfüllen. Deshalb werden die Daten gerade in ihrer Gesamtheit benötigt.

196

2. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung noch ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung. Die verfassungsrechtlichen Anforderungen (oben C II 2 b bb) sind für die durch das Volkszählungsgesetz 1983 vorgesehene Erhebung nur zum Teil erfüllt. Zwar trägt § 11 BStatG dem Schutz des Rechts auf informationelle Selbstbestimmung BVerfGE 65, 1 (58)BVerfGE 65, 1 (59)durch eine Regelung über das Statistikgeheimnis Rechnung. Auch schreibt § 11 Abs. 7 Satz 1 BStatG die Löschung der zur Identifizierung dienenden Daten vor, sobald diese nicht mehr für statistische Zwecke des Bundes benötigt werden. Bis zu diesem Zeitpunkt sollen nach Satz 2 der Vorschrift Namen und Anschriften von den übrigen Angaben getrennt und unter besonderem Verschluß gehalten werden. Diese Bestimmungen reichen jedoch nicht aus, um für die Volkszählung verfassungsgemäße Bedingungen der Datenerhebung und Datenverarbeitung zu gewährleisten. Vielmehr hat der Gesetzgeber darüber hinaus für notwendige Sicherungsvorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts Sorge zu tragen. Er braucht nicht alles selbst zu regeln, muß aber dafür sorgen, daß das Notwendige geschieht. Im einzelnen sind folgende grundrechtssichernde Maßnahmen geboten:

197

a) Es bestehen Aufklärungspflichten und Belehrungspflichten. Zwar braucht der Auskunftspflichtige sich nicht mit anderen einem Haushalt zurechnen zu lassen, sondern wird, sofern er es wünscht, anhand eines eigenen Haushaltsbogens gezählt; denn § 5 Abs. 1 VZG 1983 sieht grundsätzlich eine persönliche Auskunftspflicht jedes einzelnen Bürgers vor. Auch steht diesem - wie bereits ausgeführt - das Recht zu, den ausgefüllten Erhebungsbogen in verschlossenem Umschlag dem Zähler zu übergeben, bei der Zählungsdienststelle abzugeben oder ihn ihr mit der Post zuzusenden. Diese Rechte sind für den Bürger bei Massenerhebungen der streitigen Art aber nur schwer erkennbar und der gesetzlichen Regelung erst im Wege der Auslegung zu entnehmen; die vorgesehene Durchführung der Erhebung lenkt von ihnen eher ab. Daher hat der Gesetzgeber sicherzustellen, daß die Bürger über diese Rechte schriftlich belehrt werden. Auch ist deutlich kenntlich zu machen, soweit bestimmte Angaben (wie etwa die Telefonnummer) lediglich auf freiwilliger Basis erhoben werden.

198

b) Die zur Identifizierung dienenden Merkmale (insbesondere Namen, Anschriften, Kennummern und Zählerlistennummern) sind zum frühest möglichen Zeitpunkt zu löschen und bis dahin von den übrigen Angaben getrennt unter Verschluß zu halten. BVerfGE 65, 1 (59)BVerfGE 65, 1 (60)Die Handhabung der Vorschrift des § 11 Abs. 7 BStatG, der insoweit grundrechtssichernde Funktion zukommt, darf nicht allein dem Ermessen der Verwaltung überlassen bleiben. Zugleich ist eine effektive Kontrolle durch die Datenschutzbeauftragten notwendig. Sinnvollerweise wird der Auskunftspflichtige genauer darüber zu belehren sein, welche Merkmale lediglich Hilfsmittel der Erhebung sind (vgl. § 5 des Mikrozensusgesetzes vom 21. Februar 1983 [BGBl. I S. 201]).

199

c) Den Bürgern treten Zähler entgegen, die Einblick in die Unterlagen erhalten, wenn der ausgefüllte Erhebungsbogen offen abgegeben wird. Deshalb müssen Maßnahmen getroffen werden, um Interessenkollisionen möglichst zu vermeiden. Dem Schutzbedürfnis wird zwar schon weitgehend durch die aufgeführten Möglichkeiten der Abgabe des ausgefüllten Fragebogens Rechnung getragen. Dies allein reicht jedoch bei einer Massenerhebung mit etwa 600.000 Zählern (vgl. BTDrucks 9/451, S. 10) für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung nicht aus. Mit Recht haben die Datenschutzbeauftragten deshalb in ihrer Besprechung vom 22. März 1983 angeregt, auf den Einsatz von Zählern zu verzichten, bei denen im Hinblick auf ihre dienstliche Tätigkeit Interessenkonflikte nicht auszuschließen sind. Als weitere Maßnahme ist eine Vorschrift geboten, daß Zähler - darüber besteht zwischen dem Bundesminister des Innern und den Datenschutzbeauftragten Einvernehmen - nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden sollen, damit in der Nachbarschaft die Auskunftsbereitschaft nicht beeinträchtigt wird.

200

d) Schließlich hat der Gesetzgeber dafür Sorge zu tragen, daß der Inhalt des Fragebogens mit dem Gesetz übereinstimmt. So ist es nicht angängig, alle Auskunftspflichtigen von vornherein nach Haushalten zu erfassen, obwohl § 5 VZG 1983 grundsätzlich eine persönliche Auskunftspflicht jedes Bürgers vorsieht. Auch darf der Inhalt der einzelnen Fragen im Fragebogen nicht weiter gehen, als der Gesetzestext es zuläßt. Die Entscheidung, wie die Erfüllung dieser Anforderungen an den Fragebogen sicherzustelBVerfGE 65, 1 (60)BVerfGE 65, 1 (61)len ist, hat der Gesetzgeber zu treffen. Dazu stehen ihm verschiedene Möglichkeiten offen, einschließlich der Ermächtigung, den Inhalt des Fragebogens durch eine Rechtsverordnung festzulegen.

201

IV.

1. Die zu statistischen Zwecken erhobenen, noch nicht anonymisierten, also noch personenbezogenen Daten dürfen - wie bereits ausgeführt (oben C II 2 cc) - kraft ausdrücklicher gesetzlicher Ermächtigung weitergeleitet werden, soweit und sofern dies zur statistischen Aufbereitung durch andere Behörden erfolgt und wenn dabei die zum Schutz des Persönlichkeitsrechts gebotenen Vorkehrungen, insbesondere das Statistikgeheimnis und das Gebot der Anonymisierung, in gleicher Weise zuverlässig sichergestellt sind wie bei den Statistischen Ämtern des Bundes und der Länder. Würden hingegen personenbezogene, nicht anonymisierte Daten, die zu statistischen Zwecken erhoben wurden und nach der gesetzlichen Regelung dafür bestimmt sind, für Zwecke des Verwaltungsvollzuges weitergegeben (Zweckentfremdung), würde in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingegriffen. Es kann offenbleiben, ob eine direkte Weiterleitung dieser Daten generell und selbst dann als unvereinbar mit dem Grundsatz der Trennung von Statistik und Vollzug zu beanstanden wäre, wenn der Gesetzgeber diese Weiterleitung ausdrücklich vorsähe. Es bedarf auch keiner abschließenden Erörterung, ob die gleichzeitige Durchführung einer an sich statthaften Erhebung personenbezogener Daten für statistische Zwecke mit einer an sich statthaften Erhebung personenbezogener Daten für bestimmte Zwecke des Verwaltungsvollzugs auf verschiedenen Bögen (kombinierte Erhebung) zulässig wäre. Sowohl die direkte Übermittlung von zu statistischen Zwecken erhobenen Daten als auch die kombinierte Erhebung wären schon deshalb nicht bedenkenfrei, weil die Verknüpfung zweier unterschiedlicher Zwecke mit unterschiedlichen Anforderungen den Bürger angesichts der für ihn undurchsichtigen Möglichkeiten der BVerfGE 65, 1 (61)BVerfGE 65, 1 (62)automatischen Datenverarbeitung in hohem Maße verunsichert und dadurch die Zuverlässigkeit der Angaben und deren Eignung für statistische Zwecke gefährden kann. Ferner wären die unterschiedlichen Voraussetzungen zu beachten: So gelten für die Erhebung und Verwertung zu statistischen Zwecken das Statistikgeheimnis, das Gebot der Anonymisierung und das Nachteilsverbot; für die Erhebung zu Verwaltungsvollzugszwecken ist dies hingegen nicht oder nicht in gleicher Weise der Fall; während für die Statistik Identifikationsmerkmale (etwa Name und Anschrift) nur als Hilfsmittel dienen, sind sie in aller Regel für die Erhebung zu Verwaltungsvollzugszwecken wesentlicher Bestandteil. Zudem wird dabei die auf statistische Datensammlung zugeschnittene Ermittlungsorganisation zugleich für andere Erhebungszwecke eingesetzt, die für sich allein eine solche Organisation schwerlich rechtfertigen würden. Auch wäre zu beachten, daß das Rechtsschutzverfahren bei den beiden Erhebungsarten auseinanderlaufen kann.

202

Eine Regelung, die dennoch beide Zwecke gleichzeitig erreichen will, ist zur Erreichung der beabsichtigten Zwecke jedenfalls dann untauglich und damit verfassungswidrig, wenn sie tendenziell Unvereinbares miteinander verbindet. In einem solchen Fall kann die Verbindung statistischer Zwecke mit Verwaltungsvollzugszwecken in einer Zählung nicht nur zu Unklarheit und Unverständlichkeit der Norm führen, sondern bewirkt darüber hinaus ihre Unverhältnismäßigkeit. Anders als bei Datenerhebungen zu ausschließlich statistischen Zwecken ist hier eine enge und konkrete Zweckbindung der weitergeleiteten Daten unerläßlich (oben C II 2 a). Zudem ist das Gebot der Normenklarheit von besonderer Bedeutung. Der Bürger muß aus der gesetzlichen Regelung klar erkennen können, daß seine Daten nicht allein zu statistischen Zwecken verwendet werden, für welche konkreten Zwecke des Verwaltungsvollzugs seine personenbezogenen Daten bestimmt und erforderlich sind und daß ihre Verwendung unter BVerfGE 65, 1 (62)BVerfGE 65, 1 (63)Schutz gegen Selbstbezichtigungen auf diesen Zweck begrenzt bleibt.

203

2. Die Kombination der Volkszählung für statistische Zwecke mit dem Melderegisterabgleich nach § 9 Abs. 1 VZG 1983 entspricht nicht den verfassungsrechtlichen Anforderungen.

204

a) Entgegen der Auffassung der Beschwerdeführer fehlt dem Bund zur Regelung des Melderegisterabgleichs allerdings nicht die Zuständigkeit; sie ist nach Art. 75 Nr. 5 GG gegeben.

205

Die Rahmengesetzgebungskompetenz des Bundes (Art. 75 GG) gestattet diesem nach der ständigen Rechtsprechung des Bundesverfassungsgerichts auch Vollregelungen für einzelne Teile einer Gesetzgebungsmaterie, sofern dem Landesgesetzgeber für die Gesamtmaterie noch ausreichender Regelungsspielraum verbleibt, den dieser aufgrund eigener Entschließung ausfüllen kann (vgl. BVerfGE 43, 291 [343] - Numerus clausus). Da § 9 Abs. 1 Satz 1 VZG 1983 nur die Möglichkeit des Melderegisterabgleichs einräumt, bleibt dem Landesgesetzgeber, der sowohl das Ob als auch das Wie des Abgleichs der Angaben der Volkszählung nach § 2 Nr. 1 und 2 VZG 1983 bestimmen kann, noch ausreichender Regelungsspielraum, den er aufgrund eigener Entschließung ausfüllen kann, aber nicht muß. Die Entscheidung darüber, ob ein Bedürfnis nach bundesgesetzlicher Regelung des Melderegisterabgleichs im Sinne des Art. 72 Abs. 2 GG besteht, ist in das Ermessen des Bundesgesetzgebers gestellt (vgl. BVerfGE 33, 224 [229]; st Rspr). Für den Melderegisterabgleich besteht nach der nicht zu beanstandenden Einschätzung des Gesetzgebers ein Bedürfnis nach bundesgesetzlicher Regelung zur Wahrung der Rechtseinheit oder Wirtschaftseinheit (Art. 72 Abs. 2 Nr. 3 GG); denn die Berichtigung der Melderegister sollte insbesondere im Hinblick auf § 12 Abs. 2 des Melderechtsrahmengesetzes (MRRG) vom 16. August 1980 (BGBl. I S. 1429) in allen Bundesländern zur gleichen Zeit und in gleichem Umfang erfolgen. Da somit die Zuständigkeit des Bundes zur Regelung des Melderegisterabgleichs nach Art. 75 Nr. 5 GG gegeben ist, kann dahingestellt bleiben, ob seine Zuständigkeit zu dieser Regelung auch aus Art. 73 Nr. 11 GG folgt.

206

BVerfGE 65, 1 (63)BVerfGE 65, 1 (64)b) § 9 Abs. 1 VZG 1983 verletzt aber das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gesicherte Recht auf informationelle Selbstbestimmung, weil die Regelung tendenziell Unvereinbares miteinander verbindet, deshalb zur Erreichung der angestrebten Zwecke ungeeignet, in ihrem Inhalt unklar und daher in ihrer Tragweite für den Bürger unverständlich ist.

207

§ 9 Abs. 1 Satz 1 VZG 1983 gestattet den Gemeinden, bestimmte Angaben aus den Erhebungsunterlagen mit den Melderegistern zu vergleichen und zu deren Berichtigung zu verwenden. Ausgewählte Personendaten der Volkszählung 1983 können so nicht nur zu statistischen Zwecken, sondern zusätzlich zu einem Verwaltungsvollzug verwandt werden, dem keine konkrete Zweckbindung entspricht. Zwar ergibt sich aus der gesetzlichen Regelung, daß die gemäß § 2 Nr. 1 und 2 VZG 1983 erhobenen Daten nicht nur zu statistischen Zwecken, sondern zusätzlich für den Melderegisterabgleich erhoben werden; es ist jedoch infolge der Aufgaben der Meldebehörden, die Daten ihrerseits nach Maßgabe des Vierten Abschnitts des Melderechtsrahmengesetzes und der entsprechenden Vorschriften der Länder weiterzugeben, nicht vorhersehbar, zu welchem konkreten Zweck welche Behörden die Daten verwenden. Dies hat zur Folge, daß sich die Zwecke beider Erhebungen (Statistik - Melderegisterabgleich) nicht nur gegenseitig beeinträchtigen, sondern sogar ausschließen; denn während die Effizienz der Statistik eine strenge Beachtung des Statistikgeheimnisses verlangt, ist dieses, wie die weitergehenden Übermittlungsregelungen des Melderechtsrahmengesetzes zeigen, mit den Aufgaben der Meldebehörden (§ 1 Abs. 3 MRRG) unvereinbar.

208

Wie sehr durch die gleichzeitige Verfolgung beider Zwecke die Funktionsfähigkeit der amtlichen Statistik gefährdet wird, die ein Kernstück der statistischen Bestandsaufnahme bildet (vgl. Begründung der Bundesregierung zu dem Entwurf eines Gesetzes über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung - Volkszählungsgesetz 1982 [BTDrucks 9/451, S. 7, A I]), hat auch der Gesetzgeber gesehen; denn in § 9 Abs. 1 Satz 2 hat er es ausdrücklich untersagt, aus den statistischen Einzelangaben BVerfGE 65, 1 (64)BVerfGE 65, 1 (65)gewonnene Erkenntnisse zu Maßnahmen gegen den einzelnen Auskunftspflichtigen zu verwenden. Dieses Nachteilsverbot verspricht jedoch mehr, als es leisten kann. Es vermag das Defizit für die Funktionsfähigkeit der Statistik und für den Schutz der Betroffenen nicht auszugleichen, das durch die Verbindung von Statistik und Vollzug entsteht. Das Verbot, das wörtlich aus § 1 Abs. 3 Satz 2 BStatG übernommen und welches auf das Statistikgeheimnis zugeschnitten ist, kann zwar einen ausreichenden Schutz gewähren, wenn die Daten allein zu statistischen Zwecken weitergegeben werden. Seine Übernahme in eine Vorschrift über den Melderegisterabgleich erhöht aber die Unverständlichkeit der gesamten Regelung und führt dazu, daß der auskunftspflichtige Bürger die Auswirkungen dieser Bestimmung nicht mehr zu übersehen vermag. Für den Betroffenen ist nicht erkennbar, daß seine statistischen Angaben nach Maßgabe der melderechtlichen Vorschriften in weitem Umfang an Behörden und öffentliche Stellen übermittelt werden können, ohne daß diese den statistischen Ursprung dieser Daten feststellen und dem Nachteilsverbot Rechnung tragen können. Damit kann das Nachteilsverbot (§ 9 Abs. 1 Satz 2 VZG 1983) seine Aufgabe nicht erfüllen; zugleich verletzt es das Gebot der Normenklarheit (oben C II 1 b).

209

3. Auch § 9 Abs. 2 VZG 1983 verstößt gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Diese Vorschrift gestattet die Übermittlung von personenbezogenen Einzelangaben an die fachlich zuständigen obersten Bundesbehörden und Landesbehörden sowie an die von ihnen bestimmten Stellen, soweit diese personenbezogenen Daten von den Empfängern zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben benötigt werden. Sie geht über § 11 Abs. 5 und 6 BStatG hinaus, da die Daten lediglich ohne Namen, nach § 9 Abs. 2 Satz 2 VZG 1983 auch ohne die Angaben der Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft übermittelt werden können und dem Betroffenen daher noch ohne Schwierigkeiten zuzuordnen sind. Ob die Übermittlung nur zu statistischen Zecken oder auch für den BVerfGE 65, 1 (65)BVerfGE 65, 1 (66)Verwaltungsvollzug zulässig ist, kann der Vorschrift nicht entnommen werden. Eine Begrenzung auf die Übermittlung zu statistischen Zwecken scheitert an der fehlenden Normenklarheit. Damit ist aber die Möglichkeit der Verwendung für Verwaltungsvollzugszwecke gegeben. Selbst wenn die Übermittlung von zu statistischen Zwecken erhobenen personenbezogenen Daten zu Verwaltungsvollzugszwecken oder eine Kombination einer für sich allein zulässigen statistischen Erhebung mit einer für sich allein zulässigen Erhebung zu Verwaltungsvollzugszwecken nicht von vornherein gegen das Persönlichkeitsrecht verstoßen sollte, verletzt § 9 Abs. 2 VZG 1983 die Bürger doch bereits deshalb in ihrem Recht auf informationelle Selbstbestimmung, weil weder aus der Vorschrift klar zu erkennen ist, daß diese überhaupt eine Weitergabe zu Verwaltungszwecken vorsieht, noch um welche konkreten, klar definierten Zwecke es sich dabei handelt, wie dies bei nicht anonymisierten Daten geboten ist. Wenn aber schon eine klare Zweckbestimmung fehlt, ist auch nicht mehr abzusehen, ob sich die Weitergabe in den Grenzen des zur Zweckerfüllung Erforderlichen hält.

210

4. § 9 Abs. 3 VZG 1983 verstößt ebenfalls gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

211

a) Satz 1 des § 9 Abs. 3 VZG 1983 ermöglicht es, die mit Hilfe der Gemeinden erhobenen personenbezogenen Daten ohne Namen auch dem kommunalen Bereich für bestimmte Verwaltungszwecke zur Verfügung zu stellen. Übermittelt werden dürfen die erforderlichen (personenbezogenen) Einzelangaben über die nach den §§ 2 bis 4 VZG 1983 erfaßten Tatbestände - mit Ausnahme der nach § 4 Nr. 1 Buchstabe c und § 4 Nr. 3 Buchstabe c VZG 1983 verlangten Angaben und des Merkmals der rechtlichen Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft - für Zwecke der Regionalplanung, des Vermessungswesens, der gemeindlichen Planung und des Umweltschutzes. Zu welchem konkreten Zweck die Daten indessen weitergegeben werden, insbesondere ob nur zu statistischen oder auch zu Verwaltungsvollzugszwecken, ist danach nicht hinreichend erkennBVerfGE 65, 1 (66)BVerfGE 65, 1 (67)bar. So besteht Regionalplanung auf gemeindlicher Ebene aus den Flächennutzungsplänen und den aus ihnen hervorgegangenen Bebauungsplänen. Diese sind ebenso Bestandteil gemeindlicher Planung und treffen für die im jeweiligen Planungsgebiet belegenen Grundstücke spezifizierte und eindeutige Festsetzungen über Art und Ausmaß der zugelassenen baulichen Nutzung, mithin Verwaltungsentscheidungen gegenüber dem einzelnen Bürger. Auch die für Zwecke des Vermessungswesens und des Umweltschutzes übermittelten personenbezogenen Einzelangaben können von den Übermittlungsadressaten nicht nur zu statistischen, sondern ebenso zu Verwaltungsvollzugszwecken verwendet werden. So wurde in der Berichterstattergruppe "Statistik" des Innenausschusses anläßlich der Beratung des Gesetzentwurfs der Bundesregierung ausdrücklich darauf hingewiesen, daß mit der Formulierung "für Zwecke des Vermessungswesens" gerade nicht nur eine statistische Aufbereitung für eine gemeindliche Planung gemeint sei, sondern mit Rücksicht auf die Landesvermessungsbehörden an einen Abgleich der Unterlagen und an eine Verbesserung der vorhandenen Liegenschaftskataster gedacht sei (vgl. S. 14 des Kurzprotokolls der 4. Sitzung der Berichterstattergruppe "Statistik" vom 8. Mai 1979). Überdies verfolgen der Umweltschutz und das Vermessungswesen im Bereich der Gemeinden weniger statistische, sondern eher Verwaltungsvollzugszwecke; hierauf hatte bereits der Bayerische Landesbeauftragte für den Datenschutz in seiner Stellungnahme vom 31. Mai 1979 an den Innenausschuß des Deutschen Bundestages ausdrücklich hingewiesen. § 9 Abs. 3 Satz 1 VZG 1983 verstößt daher bereits deshalb gegen das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht, weil die Vorschrift weder klar erkennen läßt, daß die übermittelten personenbezogenen Daten auch zu Verwaltungsvollzugszwecken verwendet werden können, noch um welche konkreten klar definierten Zwecke es sich dabei handelt. Angesichts der Unklarheit der vorgesehenen Zwecke ist es den Statistischen Ämtern des Bundes und der Länder auch nicht möglich festzustellen, ob zur BVerfGE 65, 1 (67)BVerfGE 65, 1 (68)Erfüllung der jeweiligen Zwecke nicht die Übermittlung - faktisch - anonymisierter Einzelangaben (§ 11 Abs. 5 BStatG) an die Gemeinden oder ihre Verbände genügt.

212

b) Auch Satz 2 des § 9 Abs. 3 VZG 1983 verstößt gegen das Recht auf informationelle Selbstbestimmung. Für eigene statistische Aufbereitungen können den Gemeinden und Gemeindeverbänden nach dieser Vorschrift die nach den §§ 2 bis 4 VZG 1983 erfaßten Tatbestände sogar einschließlich der Namen zur Verfügung gestellt werden.

213

Zwar begrenzt die Bestimmung damit die Verwendung personenbezogener Einzelangaben im kommunalen Bereich auf statistische Aufbereitungen. Unberücksichtigt bleibt jedoch, daß es zur Sicherung des informationellen Selbstbestimmungsrechts der Bürger darüber hinaus bei der Verarbeitung personenbezogener Daten auch außer-

halb der Statistischen Ämter einer Organisation bedarf, welche die Zweckbindung ebenso sichert wie innerhalb der Statistischen Ämter des Bundes und der Länder. Eine derartige Sicherung ist insbesondere deshalb geboten, weil in vielen Gemeinden keine für die Bearbeitung von Statistiken zuständigen Stellen vorhanden sind, so daß eine ausschließlich für statistische Zwecke vorgesehene Nutzung der Daten nicht als ausreichend gewährleistet angesehen werden kann. Hinzu kommt, daß die Kommunalstatistik im Gegensatz zur Bundesstatistik nicht gesetzlich geregelt und damit von anderen Verwaltungsaufgaben nicht von vornherein abgeschottet ist. Damit ist der Datenfluß personenbezogener Daten über die nach den §§ 2 bis 4 VZG 1983 erfaßten Tatbestände innerhalb der Kommunen und ihrer Verbände nur unzureichend allein durch die Verwendungsschranke "statistische Aufbereitungen" gehemmt. Diese Formulierung ist aber so ungenau, daß sie herangezogen werden kann, um die verschiedensten Aktivitäten zu decken. Im kommunalen Bereich sind die Grenzen statistischer Nutzung fließend: Darunter werden nicht nur herkömmliche Tabellenwerke verstanden, sondern auch Spezialaufbereitungen für Planungszwecke, die bei kleinräumigem Bezug - wegen des besonders großen Zusatzwissens BVerfGE 65, 1 (68)BVerfGE 65, 1 (69)der Kommunen - leicht an die Grenze der Deanonymisierung stoßen. Gemeindliche Statistik wird insoweit heute weitgehend als "Stadtentwicklung" oder "Stadtentwicklungsforschung" verstanden. Gerade wenn sich die Angaben - wie im gemeindlichen Bereich - auf kleinere Personengruppen beziehen, muß der Gesetzgeber für organisatorische Vorkehrungen sorgen, welche die vorgesehene Zweckbindung garantieren. Dazu ist die Trennung der Kommunalstatistik von anderen Aufgabenbereichen der Gemeinden und ihrer Verbände ("informationelle Gewaltenteilung") unerläßlich. Da § 9 Abs. 3 Satz 2 VZG 1983 eine Übermittlung von personenbezogenen Einzelangaben für statistische Aufbereitungen der Gemeinden und ihrer Verbände gestattet, ohne die Zweckbindung zu statistischen Zwecken wie in den Statistischen Ämtern des Bundes und der Länder zu sichern, ist die Vorschrift mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar.

214

5. Demgegenüber verletzt § 9 Abs. 4 VZG 1983 nicht das allgemeine Persönlichkeitsrecht. Diese Vorschrift gestattet für wissenschaftliche Zwecke die Übermittlung bestimmter Einzelangaben an Amtsträger und für den öffentlichen Dienst besonders Verpflichtete. Die Übermittlung hat sich in den Grenzen des für wissenschaftliche Zwecke Erforderlichen zu halten; Name und Anschrift dürfen überhaupt nicht weitergegeben werden. Die Regelung folgt damit der Erkenntnis, daß für die meisten Untersuchungsbereiche ein direkter Personenbezug nicht erforderlich ist; denn der Wissenschaftler ist regelmäßig nicht an der einzelnen Person interessiert, sondern an dem Individuum als Träger bestimmter Merkmale. Da bei den Übermittlungsadressaten des § 9 Abs. 4 VZG 1983 regelmäßig kaum Zusatzwissen vorhanden sein wird, ist nach dem derzeitigen Erkenntnisstand und Verfahrensstand nicht davon auszugehen, daß der Schutz des informationellen Selbstbestimmungsrechts bei der Verarbeitung von Daten nach § 9 Abs. 4 VZG 1983 über die durch § 5 BDSG, § 11 Abs. 5 BStatG, § 9 Abs. 5 VZG 1983 und die Kontrolle der Datenschutzbeauftragten des Bundes und der Länder gewährleisteten BVerfGE 65, 1 (69)BVerfGE 65, 1 (70)Sicherungen hinaus weitere Vorkehrungen von Verfassungs wegen erfordert. […]

**2) BVerfGE 109, 279 – Großer Lauschangriff**

*a) Sachverhalt*

Die Verfassungsbeschwerden richteten sich unmittelbar gegen Art. 13 III-VI GG sowie gegen Vorschriften der Strafprozessordnung, mit denen die akustische Überwachung von Wohnungen zu Strafverfolgungszwecken ermöglicht wird.

Die Bf. zu 1 wendeten sich mit ihrem Antrag unmittelbar gegen Art. 13 III-VI GG in der Fassung des Gesetzes vom 26. 3. 1998. Weiter richtete sich ihre Verfassungsbeschwerde gegen die gesetzliche Ermächtigung zum elektronischen Abhören in Wohnräumen in § 100c I Nr. 3 und II StPO sowie gegen die geänderten Benachrichtigungsvorschriften in § 101 I und IV StPO. Die Bf. sahen sich durch die angegriffenen Bestimmungen gegenwärtig und unmittelbar in ihren Grundrechten aus Art. 1 I und III, 2 I, 13 I i.V. mit Art. 19 II und 79 III sowie aus Art. 19 IV GG verletzt.

Die Bf. zu 2 wendeten sich unmittelbar gegen das Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität und mittelbar gegen das Gesetz zur Änderung des Art. 13 GG. Sie rügten die Verletzung ihrer Grundrechte aus Art. 1 I und III, 2 I, 13 I i.V. mit Art. 19 II und 79 III, 19 IV und 103 I GG. Sie hielten §§ 100c I Nr. 3, II 4 und 5, 100d II-V, 100e und 100f sowie § 101 I und IV StPO für verfassungswidrig.

(Zusammenfassung nach NJW 2004, 999, beck-online)

*b) Leitsätze*

**1.** Art. 13 Abs. 3 GG in der Fassung des Gesetzes zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) ist mit Art. 79 Abs. 3 GG vereinbar.

**2.** Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt.

**3.** Nicht jede akustische Überwachung von Wohnraum verletzt den Menschenwürdegehalt des Art. 13 Abs. 1 GG.
**4.** Die auf die Überwachung von Wohnraum gerichtete gesetzliche Ermächtigung muss Sicherungen der Unantastbarkeit der Menschenwürde enthalten sowie den tatbestandlichen Anforderungen des Art. 13 Abs. 3 GG und den übrigen Vorgaben der Verfassung entsprechen.
**5.** Führt die auf eine solche Ermächtigung gestützte akustische Wohnraumüberwachung gleichwohl zur Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung, muss sie abgebrochen werden und Aufzeichnungen müssen gelöscht werden; jede Verwertung solcher Informationen ist ausgeschlossen.
**6.** Die Vorschriften der Strafprozessordnung zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung genügen den verfassungsrechtlichen Anforderungen im Hinblick auf denBVerfGE 109, 279 (279) BVerfGE 109, 279 (280)Schutz der Menschenwürde (Art. 1 Abs. 1 GG), den vom Rechtsstaatsprinzip umfassten Grundsatz der Verhältnismäßigkeit, die Gewährung effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) und den Anspruch auf rechtliches Gehör (Art. 103 Abs. 1 GG) nicht in vollem Umfang.
(Bearbeitung, zuletzt am 13. Sep. 2017, durch: A. Tschentscher; Dominika Blonski, http://www.servat.unibe.ch/dfr/bv109279.html )

*c) Begründung*

Die Verfassungsbeschwerden sind, soweit zulässig, teilweise begründet. Zwar erfüllt die in Art. 13 Abs. 3 GG vorgenommene Verfassungsänderung die Anforderungen des Art. 79 GG. Die angegriffenen Vorschriften der Strafprozessordnung stehen demgegenüber nicht in vollem Umfang im Einklang mit dem Grundgesetz. […]
II.
Die gesetzliche Ermächtigung zur Durchführung der akustischen Wohnraumüberwachung in § 100 c Abs. 1 Nr. 3, Abs. 2 und 3 StPO sowie die Regelung der Beweiserhebungs- und Beweisverwertungsverbote in § 100 d Abs. 3 StPO tragen den Anforderungen, die nach Art. 13 Abs. 1 und 3 GG sowie Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG im Hinblick auf den Schutz des unantastbaren Bereichs privater Lebensgestaltung, auf die Ausgestaltung des Straftatenkatalogs und auf die Beachtung des Grundsatzes der Verhältnismäßigkeit im Übrigen zu stellen sind, nicht hinreichend Rechnung. Sie sind nur teilweise mit dem Grundgesetz vereinbar.

157

1. Maßstab zur Prüfung der Verfassungsmäßigkeit der in der Strafprozessordnung enthaltenen Ermächtigungen zur akustischen Wohnraumüberwachung sind vor allem Art. 13 Abs. 1 und 3 GG und daneben Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Von den durch die Normen ermöglichten Maßnahmen können aber auch andere Grundrechte, wie insbesondere Art. 4 Abs. 1 und 2 sowie Art. 6 Abs. 1 und 2 GG, betroffen sein.

158

a) Das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende allgemeine Persönlichkeitsrecht kommt neben Art. 13 Abs. 1 GG allerdings nicht zur Anwendung, soweit Eingriffe in die räumliche Privatsphäre des Wohnungsinhabers zu überprüfen sind.

159

Art. 13 Abs. 1 GG enthält eine spezielle Gewährleistung des Schutzes vor staatlicher akustischer Überwachung der räumlichen Privatsphäre, die die allgemeinere Vorschrift insoweit verdrängt (vgl. BVerfGE 100, 313 [358] zu Art. 10 GG). Diese Spezialität wirkt sich wegen des weiten Schutzbereichs von Art. 13 GG nicht nur gegenüber der staatlichen Überwachung selbst aus, sondern erBVerfGE 109, 279 (325)BVerfGE 109, 279 (326)streckt sich auch auf notwendige Vorbereitungsakte und auf den Informations- und Datenverarbeitungsprozess, der sich an die Erhebung anschließt, sowie auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 [359]).

160

Mit dem Recht, in der Wohnung ungestört zu sein, und dem Recht am eigenen in der Wohnung gesprochenen Wort schützt Art. 13 Abs. 1 GG gerade den Teil der Privatsphäre, den sonst das allgemeine Persönlichkeitsrecht gewährleistet. Dieses Recht ergänzt als unbenanntes Freiheitsrecht die speziellen Freiheitsrechte, die ebenfalls konstituierende Elemente der Persönlichkeit schützen (vgl. BVerfGE 54, 148 [153 f.]), nur insoweit, als Letztere keinen Schutz gewähren.

161

b) Der Schutz des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG greift hingegen ein, soweit von der Wohnraumüberwachung Personen betroffen werden, die sich nicht auf Art. 13 Abs. 1 GG berufen können. Grundrechtsträger des Art. 13 Abs. 1 GG ist jeder Inhaber oder Bewohner eines Wohnraums, unabhängig davon, auf welchen Rechtsverhältnissen die Nutzung des Wohnraums beruht. Bei mehreren Bewohnern einer Wohnung steht das Grundrecht jedem Einzelnen, bei Familien mithin jedem Familienmitglied zu. Maßnahmen der Wohnraumüberwachung können aber nicht nur Wohnungsinhaber, sondern auch zufällig in einer Wohnung Anwesende erfassen. Diese Personen sind zwar nicht in ihrem Grundrecht aus Art. 13 Abs. 1 GG, wohl aber in ihrem allgemeinen Persönlichkeitsrecht betroffen. Der Schutz aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG kann insofern allerdings nicht weiter reichen als derjenige aus Art. 13 Abs. 1 und 3 GG.

162

c) Der Schutz der räumlichen Privatsphäre und des allgemeinen Persönlichkeitsrechts kann schließlich in Einzelfällen durch weitere Grundrechtsgarantien ergänzt sein. So wird das Gespräch zwischen Eheleuten in der eigenen Wohnung nicht nur von Art. 13 Abs. 1 GG, sondern zusätzlich durch Art. 6 Abs. 1 GG geschützt. Auch in Bezug auf die Kommunikation mit Berufsgeheimnisträgern können neben dem grundrechtlichen Schutz der räumlichen Privatsphäre Grundrechte in Betracht kommen, die -- wie etwa Art. 4 GG im HinblickBVerfGE 109, 279 (326) BVerfGE 109, 279 (327)auf das Gespräch mit einem Geistlichen -- der besonderen Schutzbedürftigkeit der Kommunizierenden Rechnung tragen.

163

2. Die angegriffene gesetzliche Ermächtigung zum Abhören und Aufzeichnen von Wohnraumgesprächen ermöglicht Eingriffe in die Grundrechte aus Art. 13 Abs. 1 und aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

164

a) Ein Eingriff in das Grundrecht der Unverletzlichkeit der Wohnung liegt sowohl im physischen Eindringen in den Wohnraum und in dem Anbringen von technischen Mitteln in den geschützten Räumen, als auch im Belauschen der Vorgänge in der Wohnung mit akustischen Hilfsmitteln (siehe oben C I 1). Er wird durch die Speicherung und Verwendung der gewonnenen Informationen sowie durch deren Weitergabe an andere Stellen fortgesetzt.

165

Einen Eingriff stellt jede Form akustischer oder optischer Wohnraumüberwachung dar, einerlei, ob er durch technische Mittel erfolgt, die in den geschützten Räumen angebracht oder von außerhalb der Wohnung eingesetzt werden, etwa unter Nutzung von Richtmikrophonen (vgl. Verfassungsgerichtshof des Freistaates Sachsen, LVerfGE 4, 303 [383]). Dies gilt allerdings nur insoweit, als die Überwachung von außen solche innerhalb der Wohnung stattfindenden Vorgänge erfasst, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind. Zwar kann auch die Wahrnehmung der aus der Wohnung nach außen dringenden und ohne technische Hilfsmittel hörbaren Kommunikation deren Privatheit beeinträchtigen. Solche Lebensäußerungen nehmen aber nicht am grundrechtlichen Schutz des Art. 13 GG teil, weil der Betroffene die räumliche Privatsphäre nicht zu seinem Schutz nutzt, wenn er die Wahrnehmbarkeit der Kommunikation von außen selbst ermöglicht.

166

b) Die akustische Wohnraumüberwachung greift darüber hinaus in das allgemeine Persönlichkeitsrecht ein, soweit Personen betroffen werden, die sich als zufällig Anwesende in einer überwachten Wohnung nicht auf das speziellere Grundrecht aus Art. 13 Abs. 1 GG berufen können (siehe oben C II 1 b).

167

3. Die gesetzliche Ermächtigung zur Durchführung der akustischen Wohnraumüberwachung zu Strafverfolgungszwecken ist nur teilweise verfassungsgemäß.BVerfGE 109, 279 (327)

168

BVerfGE 109, 279 (328)a) Die gesetzlichen Vorschriften müssen hinreichende Vorkehrungen dafür treffen, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben und damit die Menschenwürde gewahrt wird. Wird dieses Verbot verletzt oder greift eine Maßnahme unerwartet in den absolut geschützten Kernbereich privater Lebensgestaltung ein, muss sie abgebrochen werden, und es muss durch Löschungspflichten und Verwertungsverbote vorgesorgt sein, dass die Folgen beseitigt werden. Diesen Anforderungen wird § 100 d Abs. 3 StPO nicht in hinreichender Weise gerecht.

169

aa) Der Gesetzgeber hat die mit Blick auf den Kernbereich privater Lebensgestaltung verfassungsrechtlich gebotenen Überwachungs- und Erhebungsverbote nicht in ausreichender Weise gesetzlich konkretisiert.

170

(1) Art. 13 Abs. 3 GG ermächtigt ausschließlich zum Erlass von gesetzlichen Regelungen, die gewährleisten, dass die akustische Wohnraumüberwachung den Kernbereich privater Lebensgestaltung unberührt lässt (siehe oben C I 3 b cc). Die gesetzlichen Regelungen müssen deshalb das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes in Wohnungen untersagen, wenn Anhaltspunkte dafür bestehen, dass absolut geschützte Gespräche erfasst werden.

171

Die Grenzen des unantastbaren Kernbereichs privater Lebensgestaltung sind oben (C I 3 b dd) umschrieben worden. Der Schutzbedarf von Räumlichkeiten hängt von ihrer konkreten Nutzung ab. Die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung sind umso strenger, je größer die Wahrscheinlichkeit ist, dass mit ihnen Gespräche höchstpersönlichen Inhalts erfasst würden (vgl. auch Bericht des Bundestagsrechtsausschusses, BTDrucks 13/9660, S. 4). Eine solche Wahrscheinlichkeit ist typischerweise beim Abhören von Gesprächen mit engsten Familienangehörigen, sonstigen engsten Vertrauten und einzelnen Berufsgeheimnisträgern gegeben. Bei diesem Personenkreis dürfen Überwachungsmaßnahmen nur ergriffen werden, wenn konkrete Anhaltspunkte dafür bestehen, dass die Gesprächsinhalte zwischen dem Beschuldigten und diesen Personen keinen absoluten Schutz erfordern, insbesondere bei einer Tatbeteiligung der das Gespräch führenden Personen.BVerfGE 109, 279 (328) BVerfGE 109, 279 (329)Ein konkreter Verdacht auf solche Gesprächsinhalte muss schon zum Zeit-

punkt der Anordnung bestehen. Er kann nicht erst durch eine akustische Wohnraumüberwachung begründet werden.

172

(2) Die danach verfassungsrechtlich gebotenen gesetzlichen Beschränkungen der Ermächtigung sind in § 100 d Abs. 3 StPO nur teilweise enthalten. Der Vorschrift liegt zwar die allgemeine Erwägung zu Grunde, dass die akustische Wohnraumüberwachung ausscheidet, wenn ein Sachverhalt dem unantastbaren Bereich der privaten Lebensgestaltung zuzuordnen ist. § 100 d Abs. 3 StPO konkretisiert diese verfassungsrechtlichen Grenzen jedoch nur unzureichend.

173

(a) Soweit Gespräche zwischen dem Beschuldigten und Berufsgeheimnisträgern nach § 53 StPO von Verfassungs wegen einem Verbot der Überwachung unterliegen, ist dem in § 100 d Abs. 3 Satz 1 StPO durch ein umfassendes Erhebungsverbot Rechnung getragen worden. Ob es verfassungsrechtlich geboten war, sämtliche Berufsgeheimnisträger nach § 53 StPO einem absoluten Überwachungsverbot zu unterstellen, bedarf vorliegend keiner Entscheidung. Jedenfalls ist der Gesetzgeber nicht gehindert, mit Blick auf den verfassungsrechtlichen Schutz besonderer Vertrauensverhältnisse zusätzliche Beweisermittlungsverbote zu begründen.

174

(b) § 100 d Abs. 3 StPO sichert hingegen nicht, dass eine Überwachung jedenfalls dann ausgeschlossen bleibt, wenn sich der Beschuldigte allein mit seinen engsten Familienangehörigen oder anderen engsten Vertrauten in der Wohnung aufhält und keine Anhaltspunkte für deren Tatbeteiligung bestehen.

175

Für Zeugnisverweigerungsberechtigte nach § 52 StPO, zu denen insbesondere die engsten Familienangehörigen zählen, ist nach § 100 d Abs. 3 Satz 3 StPO kein generelles Überwachungsverbot, sondern nur ein Beweisverwertungsverbot nach Maßgabe des Verhältnismäßigkeitsgrundsatzes vorgesehen. Für Gespräche mit engsten Vertrauten, die nicht dem Kreis der Zeugnisverweigerungsberechtigten angehören, enthält § 100 d Abs. 3 StPO keinerlei Einschränkungen.

176

Auch durch § 100 d Abs. 3 Satz 2 StPO wird ein Überwachungsverbot für Gespräche mit engsten Vertrauten nicht in ausreichender Weise gewährleistet. Zwar ist danach die akustische WohnraumBVerfGE 109, 279 (329)BVerfGE 109, 279 (330)überwachung unzulässig, wenn zu erwarten ist, dass sämtliche aus der Maßnahme zu gewinnenden Erkenntnisse einem Verwertungsverbot unterliegen. Solche Verwertungsverbote können sich nicht nur aus § 100 d Abs. 3 Satz 3 StPO im Hinblick auf Zeugnisverweigerungsberechtigte ergeben, sondern auch unmittelbar aus den Grundrechten, insbesondere bei einer Berührung des Kernbereichs privater Lebensgestaltung (vgl. Nack, in: Karlsruher Kommentar zur Strafprozessordnung, 5.Aufl., 2003, § 100 c Rn. 24; Rudolphi/Wolter, Systematischer Kommentar zur Strafprozessordnung, § 100 d Rn. 38, Stand: April 2001). Allerdings zielt die Regelung weder nach der gesetzgeberischen Intention noch nach ihrem Wortlaut auf ein Überwachungsverbot in Situationen, in denen eine Wahrscheinlichkeit dafür besteht, dass mit den Abhörmaßnahmen absolut geschützte Gespräche erfasst werden. Mit ihr sollte allein der auch für andere Ermittlungsmaßnahmen geltende Grundsatz klargestellt werden, dass eine Maßnahme, die nur zur Gewinnung unverwertbarer Erkenntnisse führen kann, bereits nicht geeignet ist, das mit einer strafprozessualen Maßnahme verfolgte Ziel der Gewinnung von verwertbaren Erkenntnissen zu erreichen (vgl. Bericht des Bundestagsrechtsausschusses, BTDrucks 13/9661, S. 7).

177

Ein Überwachungsverbot besteht nach dem ausdrücklichen Wortlaut der Vorschrift zudem nur, wenn sämtliche Erkenntnisse einem Verwertungsverbot unterliegen würden. Das wird aber auch bei der Überwachung des Beschuldigten, der sich allein mit seinen engsten Familienangehörigen und Vertrauten in der Wohnung aufhält, praktisch niemals anzunehmen sein. Bei strikter Auslegung würde § 100 d Abs. 3 Satz 2 StPO dazu führen, dass ein Überwachungsverbot allenfalls höchst ausnahmsweise besteht, weil Gespräche in der Regel durch eine Gemengelage unterschiedlicher Inhalte geprägt sind. Es genügt nicht den verfassungsrechtlichen Anforderungen, wenn der Gesetzgeber die Unzulässigkeit der akustischen Wohnraumüberwachung nur für den Fall vorsieht, dass sämtliche Erkenntnisse einem Verwertungsverbot unterliegen. Eine restriktive Auslegung, die zu einem verfassungsrechtlich befriedigenden Ergebnis führen würde, ist angesichts des klaren Wortlauts ("sämtliche Erkenntnisse") ausgeschlossen.BVerfGE 109, 279 (330)

178

BVerfGE 109, 279 (331)bb) Der Gesetzgeber hat in § 100 d Abs. 3 StPO auch keine hinreichenden Vorkehrungen dafür getroffen, dass die Überwachung abgebrochen wird, wenn unerwartet eine Situation eintritt, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen ist. Die Fortsetzung der Überwachung ist in solchen Fällen rechtswidrig.

179

cc) Ebenfalls fehlen ausreichende Regelungen dahingehend, dass eine Verwertung unterbleibt, wenn Erkenntnisse unter Verletzung des Kernbereichs privater Lebensgestaltung erlangt worden sind, und dass in diesem Fall schon erhobene Daten gelöscht werden.

180

(1) Das Grundgesetz stellt in beiden Hinsichten Anforderungen an den Gesetzgeber.

181

(a) Die Verfassung verlangt Regeln darüber, dass Daten nicht verwertet werden dürfen, die aus dem Kernbereich privater Lebensgestaltung stammen.

182

Das mit der akustischen Wohnraumüberwachung verbundene Risiko des Eingriffs in den Kernbereich privater Lebensgestaltung kann verfassungsrechtlich nur hingenommen werden, wenn Vorkehrungen dagegen bestehen, dass keine weiteren Folgen aus ausnahmsweise erfolgten Verletzungen entstehen. Es ist zu sichern, dass die durch den Eingriff erlangten Erkenntnisse keinerlei Verwendung im weiteren Ermittlungsverfahren oder auch in anderen Zusammenhängen finden.

183

Eines umfassenden Verwertungsverbots bedarf es zunächst für den Fall, dass die Strafverfolgungsbehörden unter Überschreitung der Ermächtigung die akustische Wohnraumüberwachung durchführen, etwa obwohl eine Wahrscheinlichkeit dafür besteht, dass mit ihr absolut geschützte Gespräche erfasst werden. Die in dem Zeitraum des Bestehens des Erhebungsverbots gewonnenen Informationen dürfen insgesamt und ungeachtet ihres Inhalts im Strafverfahren nicht verwertet werden. Das gilt nicht nur im Hinblick auf ihre Verwendung als Beweismittel im Hauptsacheverfahren, sondern auch, soweit sie als Spurenansätze für Ermittlungen in weiteren Zusammenhängen in Betracht kommen.

184

Ein Verwertungsverbot besteht ebenfalls dann, wenn nach den Umständen nicht von einem Erhebungsverbot ausgegangen werdenBVerfGE 109, 279 (331) BVerfGE 109, 279 (332)kann, sich während der Durchführung der akustischen Wohnraumüberwachung aber gleichwohl eine Situation ergibt, die zum Abhören von höchstpersönlichen Gesprächen führt. Es wird in der Praxis immer wieder zu Fällen kommen, in denen keine ausreichenden äußeren Anzeichen bestehen, die zur Klärung führen, ob absolut geschützte Gespräche innerhalb der Wohnung zu erwarten sind oder nicht. Auch der Verdacht der Tatbeteiligung eines sich in der Wohnung aufhaltenden engsten Familienangehörigen wird nicht immer zweifelsfrei beurteilt werden können. Sichere Prognosen werden von den Strafverfolgungsbehörden insbesondere dort nicht gegeben werden können, wo eindeutige Zuordnungen nach dem sozialen Umfeld des Beschuldigten trotz entsprechender Bemühungen -- etwa durch vorherige Beobachtung -- nicht möglich sind. Ob es sich um Gespräche mit möglichen Tatbeteiligten handelt, wird sich nicht immer im Vorhinein feststellen lassen. Deshalb ist in Ergänzung zu dem Beweiserhebungsverbot ein Verbot der Verwertung für einen umfassenden Kernbereichsschutz unerlässlich. Daten aus Handlungen, die den unantastbaren Bereich privater Lebensgestaltung betreffen, unterliegen von Verfassungs wegen einem absoluten Verwertungsverbot und dürfen weder im Hauptsacheverfahren verwertet werden noch Anknüpfungspunkt weiterer Ermittlungen sein (vgl. BVerfGE 44, 353 [383 f.]).

185

(b) Soweit aus dem Kernbereich privater Lebensgestaltung stammende Informationen erhoben worden sind, müssen sie unverzüglich gelöscht werden. Das Gebot effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG steht dem nicht entgegen. Insofern ist entscheidend, dass jede weitere Aufbewahrung von höchstpersönlichen Daten, die nicht hätten erhoben werden dürfen, zu dem Risiko einer Vertiefung der Persönlichkeitsverletzung führt. Auch im Rahmen des nachträglichen Rechtsschutzes könnte insoweit nur die Feststellung getroffen werden, dass das Abhören und Aufzeichnen der gelöschten Informationen rechtswidrig gewesen ist und eine Pflicht zur Datenvernichtung besteht. Dieses Anliegen ist jedoch auch mit einer sofortigen Löschung in verfassungsrechtlich hinreichender Weise erreicht, wenn der Löschung die Feststellung der Behörde zu Grunde liegt, dass die Aufzeichnung rechtswidrig gewesen ist. UnBVerfGE 109, 279 (332)BVerfGE 109, 279 (333)befriedigt bleibt allerdings ein mögliches Interesse der Betroffenen auf vollständige Kenntnis darüber, welche Gesprächsinhalte von den Strafverfolgungsbehörden überwacht worden sind. Dieses Anliegen vermag jedoch die mit der weiteren Aufbewahrung verbundenen Risiken weiterer Grundrechtsverletzungen nicht zu rechtfertigen.

186

Zu löschen ist sowohl das Originalband als auch eine gegebenenfalls zwischenzeitlich erstellte Kopie. Die Strafverfolgungsbehörden trifft im Hinblick auf Art. 19 Abs. 4 GG die Pflicht, schriftlich festzuhalten, dass es zur Aufnahme absolut geschützter Gesprächsinhalte gekommen ist und die diesbezüglichen Aufzeichnungen deswegen vollständig gelöscht worden sind.

187

(2) Eine diesen verfassungsrechtlichen Vorgaben genügende gesetzliche Regelung hat der Gesetzgeber nur teilweise getroffen.

188

(a) § 100 d Abs. 3 Satz 1 StPO kann zwar dahingehend ausgelegt werden, dass ein Verwertungsverbot besteht, wenn Gespräche mit Berufsgeheimnisträgern nach § 53 StPO unter Verstoß gegen das gesetzliche Verbot abgehört und aufgezeichnet werden (vgl. etwa Bludovsky, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO, 2002, S. 331). Für andere Sachverhalte fehlen demgegenüber absolute Verwertungsverbote. Der Gesetzgeber hat sich vielmehr

darauf beschränkt, die Bedeutung des Verhältnismäßigkeitsgrundsatzes für die Verwertung von Gesprächen mit Zeugnisverweigerungsberechtigten nach den §§ 52 und 53 a StPO herauszustellen.

189

(b) Die Beachtung von Verfassungs wegen bestehender Beweisverwertungsverbote bedarf außerdem einer ergänzenden verfahrensrechtlichen Sicherung. Auch daran fehlt es.

190

Der Schutz des Kernbereichs privater Lebensgestaltung ist angesichts der regelmäßig fehlenden Möglichkeit von Rechtsschutz durch die Betroffenen selbst -- wenn nicht eine sofortige Löschung erfolgt -- nur dann hinreichend gewährleistet, wenn es nicht allein den Strafverfolgungsbehörden obliegt, die Verwertbarkeit der von ihnen gewonnenen Erkenntnisse im Hauptsacheverfahren oder gar als Ermittlungsansätze in anderen Verfahren zu beurteilen, sondernBVerfGE 109, 279 (333) BVerfGE 109, 279 (334)wenn hierüber eine unabhängige, auch die Interessen der Betroffenen wahrnehmende Stelle entscheidet.

191

§ 100 d Abs. 3 Satz 5 StPO trifft eine solche verfahrensrechtliche Sicherung nicht in hinreichender Weise. Nach dieser Vorschrift entscheidet im vorbereitenden Verfahren das anordnende Gericht zwar über die Verwertbarkeit der gewonnenen Erkenntnisse. Die Regelung bezieht sich jedoch nach der Begründung des Rechtsausschusses des Bundestags (vgl. BTDrucks 13/9661, S. 7) und nach ihrer systematischen Stellung allein auf solche Maßnahmen, bei denen Gespräche des Beschuldigten mit Personen abgehört worden sind, denen ein Zeugnisverweigerungsrecht zusteht. Die Vorschrift hat also einen beschränkten Anwendungsbereich.

192

Vor allem fehlt es an einer eindeutigen Regelung, wer diese Entscheidung zu beantragen hat und dass eine Verpflichtung zur Einschaltung des Gerichts besteht. Die von der akustischen Wohnraumüberwachung Betroffenen haben in diesem Verfahrensstadium regelmäßig noch keine Kenntnis von der Maßnahme erlangt und können daher nicht selbst aktiv werden. Ob eine gerichtliche Entscheidung nach § 100 d Abs. 3 Satz 5 StPO eingeholt wird, liegt in der Hand der Strafverfolgungsbehörden. Weder für das anordnende Gericht noch für die Strafverfolgungsbehörden sieht § 100 d Abs. 3 Satz 5 StPO nach seinem Wortlaut eine Verpflichtung vor, eine Entscheidung über die Verwertbarkeit der Erkenntnisse im vorbereitenden Verfahren von Amts wegen herbeizuführen.

193

Die Einhaltung der Verwertungsverbote kann auf der Grundlage dieser Norm nicht gewährleistet werden. Zur Herstellung eines verfassungsgemäßen Zustandes bedarf es einer Regelung, nach der eine Verwendung von Informationen, die durch eine akustische Wohnraumüberwachung erlangt worden sind, nur dann zulässig ist, wenn die Verwertbarkeit der Informationen zuvor von einer unabhängigen Stelle, etwa dem in § 100 d Abs. 3 Satz 5 StPO bezeichneten Gericht, überprüft worden ist.

194

(c) Das Gebot der Löschung von erhobenen Daten, die aus dem Kernbereich der privaten Lebensgestaltung stammen, ist nicht in § 100 d Abs. 1 Satz 2 in Verbindung mit § 100 b Abs. 6 StPO geregelt. Diese Normen betreffen nur die Vernichtung der rechtmäßigBVerfGE 109, 279 (334) BVerfGE 109, 279 (335)erlangten Daten, wenn sie nicht mehr zur Strafverfolgung benötigt werden (siehe unten C VIII). Das Fehlen eines Gebots der unverzüglichen Löschung kernbereichsrelevanter Daten führt nach dem Ergebnis der mündlichen Verhandlung zu erheblichen Unsicherheiten im Umgang mit den Daten. In der Folge kommt es insbesondere zu einer häufig lang anhaltenden Aufbewahrung von Originalaufzeichnungen. Die Lückenhaftigkeit der Regelung gefährdet den Grundrechtsschutz.

195

(d) Gesetzliche Regelungen sind im vorliegenden Zusammenhang nicht allein deshalb entbehrlich, weil das Verwertungsverbot und das Löschungsgebot aus der Verfassung abzuleiten sind. Der Gesetzgeber findet bei der Erfüllung der verfassungsrechtlichen Vorgaben einen Spielraum vor, so dass die Gerichte seine Gestaltungsmacht zu respektieren haben. Die verbleibenden Lücken könnten -- wenn überhaupt -- allenfalls teilweise im Zuge der analogen Anwendung des § 100 d Abs. 3 und 6 StPO oder durch entsprechende verfassungskonforme Auslegung geschlossen werden. Weiteres gesetzgeberisches Handeln bleibt daher erforderlich.

196

b) Soweit die akustische Wohnraumüberwachung nicht den absolut geschützten Kernbereich privater Lebensgestaltung betrifft, setzt ihre Verfassungsmäßigkeit die Beachtung des Grundsatzes der Verhältnismäßigkeit voraus, der in Art. 13 Abs. 3 GG zum Teil näher spezifiziert worden ist. Diesen Anforderungen werden die angegriffenen Regelungen nicht in vollem Umfang gerecht. Sie verfolgen zwar einen legitimen Zweck (aa) und sind zu dessen Erreichung auch geeignet (bb) sowie erforderlich (cc). Die Beschränkung der Einsetzbarkeit der akustischen Wohnraumüberwachung auf besonders schwere Straftaten durch Art. 13 Abs. 3 GG ist vom Gesetzgeber in § 100 c Abs. 1 Nr. 3 StPO aber nur teilweise beachtet worden (dd). Im Übrigen begegnet die gesetzliche Ermächtigung bei restriktiver Auslegung keinen verfassungsrechtlichen Bedenken (ee).

197

aa) Die angegriffene Ermächtigung zur Durchführung der akustischen Wohnraumüberwachung verfolgt einen verfassungsrechtlich legitimen Zweck.

198

Mit der Ermächtigung verfolgt der Gesetzgeber neben dem allgemeinen Zweck der Aufklärung schwerer Straftaten insbesondereBVerfGE 109, 279 (335) BVerfGE 109, 279 (336)das Ziel, das rechtliche Instrumentarium zur Bekämpfung der Organisierten Kriminalität zu verbessern. Nach der Begründung des Gesetzentwurfes soll die akustische Wohnraumüberwachung es ermöglichen, in den inneren Kreis entsprechender krimineller Organisationen einzudringen und deren Strukturen aufzuhellen (vgl. BTDrucks 13/8651, S. 1, 9). Eine Erweiterung des Instrumentariums um die akustische Wohnraumüberwachung wurde dafür als unverzichtbar angesehen, vor allem zum Zwecke der Ermittlung und für die Überführung der Hauptverantwortlichen, der Organisatoren, der Finanziers und Drahtzieher (vgl. BTDrucks 13/8651, S. 9 f., 12 f.). Allerdings ist das Gesetz seinem Anwendungsbereich nach nicht auf Fälle der Organisierten Kriminalität begrenzt worden.

199

Das Bundesverfassungsgericht hat wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren -- zur Überführung von Straftätern ebenso wie zur Entlastung Unschuldiger -- betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (vgl. BVerfGE 77, 65 [76]; 80, 367 [375]; 100, 313 [389]; 107, 299 [316]).

200

bb) Die akustische Wohnraumüberwachung auf der Grundlage des § 100 c Abs. 1 Nr. 3 StPO ist zur Verfolgung der in dieser Vorschrift aufgeführten Straftaten grundsätzlich auch geeignet.

201

Ein Gesetz ist zur Zweckerreichung geeignet, wenn mit seiner Hilfe der erstrebte Erfolg gefördert werden kann. Bei der Beurteilung der Eignung des gewählten Mittels sowie bei der in diesem Zusammenhang vorzunehmenden Prognose und Einschätzung der der Allgemeinheit drohenden Gefahren steht dem Gesetzgeber ein Spielraum zu (vgl. BVerfGE 77, 84 [106]; 90, 145 [173]). Im Einzelnen wird die Einschätzungsprärogative des Gesetzgebers von der Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden, und der Bedeutung der auf dem Spiel stehenden Rechtsgüter beeinflusst (vgl. BVerfGE 50, 290 [332 f.]; 88, 203 [262]; 90, 145 [173]).

202

(1) Verfassungsrechtlich tragfähige Zweifel an der grundsätzliBVerfGE 109, 279 (336)BVerfGE 109, 279 (337)chen Eignung der akustischen Wohnraumüberwachung zur Ermittlung von Straftaten bestehen nicht.

203

Dies bestätigen die jährlichen Berichte und der zusammenfassende Erfahrungsbericht der Bundesregierung zu den Wirkungen der akustischen Wohnraumüberwachung. In den Berichtsjahren 1998 bis 2000 wurden in insgesamt 70 Verfahren 78 Wohnungen abgehört. In 41 der insgesamt 70 betroffenen Fälle waren die aus der Maßnahme gewonnenen Erkenntnisse nicht für das Ermittlungsverfahren von Bedeutung. Ein ähnliches Bild ergibt sich für das Jahr 2001. In diesem Berichtszeitraum sind in 17 Fällen Anordnungen zur akustischen Überwachung von Wohnungen getroffen worden. In neun und damit wiederum mehr als der Hälfte aller Fälle waren die Abhörmaßnahmen ohne Relevanz für das weitere Ermittlungsverfahren.

204

Als Gründe für den bisher seltenen Einsatz der akustischen Wohnraumüberwachung werden der hohe personelle und finanzielle Aufwand sowie Probleme bei der technischen Realisierung der Maßnahme angeführt. In einigen Fällen sei es nicht zu verfahrensrelevanten Erkenntnissen gekommen, weil die Maßnahmen schon technisch gescheitert seien. Ferner weist die Bundesregierung darauf hin, dass sich vor allem die Einbringung der notwendigen technischen Mittel in die Wohnung des Beschuldigten oder des Dritten teilweise als schwierig erwiesen habe (vgl. BTDrucks 14/8155, S. 7 und 13). Nicht ersichtlich ist hingegen, dass entsprechende Gegenmaßnahmen der Verdächtigen den Erfolg der akustischen Wohnraumüberwachung in erheblichem Umfang vereitelt hätten.

205

Den Ermittlungsmaßnahmen ohne Relevanz steht aber auch eine Reihe von Wohnraumüberwachungen gegenüber, die nach Aussagen von mehreren Landesjustizverwaltungen Erkenntnisse zu Tage gefördert haben, die für das Strafverfahren von entscheidender Bedeutung gewesen sind. Dies habe insbesondere Fälle betroffen, in denen sich der Beschuldigte auch in Telefongesprächen äußerst konspirativ und bedeckt verhalten habe. In solchen Fällen habe im Wesentlichen die Auswertung der akustischen Wohnraumüberwachung zum angestrebten Ermittlungserfolg geführt. Auch die vom Senat angehörten Sachverständigen, Oberstaatsanwalt Dr. Thiel,BVerfGE 109, 279 (337) BVerfGE 109, 279 (338)die Professoren Dr. Pfeiffer und Dr. Kerner sowie Privatdozent Dr. Kinzig, gehen davon aus, dass die akustische Wohnraumüberwachung als verdeckte Ermittlungsmethode dazu beitragen kann, die damit verfolgten Straftaten aufzuklären.

206

Hat eine Maßnahme der Strafverfolgung jedenfalls zum Teil Erfolg, verletzt sie das Eignungsgebot nicht.

207

(2) Der Gesetzgeber verfolgt mit der Eingriffsermächtigung allerdings auch den besonderen Zweck, in die Strukturen und in den Innenbereich der Organisierten Kriminalität einzudringen. Dieser Zweck ist im Laufe der Entstehungsgeschichte des Art. 13 Abs. 3 GG sowie der Ermächtigungen in der Strafprozessordnung immer wieder

als tragende, wenn auch nicht ausschließliche Rechtfertigung der Überwachungsmaßnahmen genannt worden. Die Aufdeckung der Strukturen der Organisierten Kriminalität soll dazu beitragen, diese zu zerschlagen und dadurch auch die Begehung weiterer Straftaten zu verhindern. Damit knüpft der Gesetzgeber an den auch von vielen Kriminologen unter Einschluss der vom Gericht angehörten Sachverständigen betonten Befund an, dass Repression und Prävention bei der Bekämpfung der Organisierten Kriminalität eng miteinander verflochten sind. Das intensiv in Grundrechte eingreifende Mittel der Wohnraumüberwachung wird gerade damit gerechtfertigt, dass es über die Repression auch Präventionszwecke in einem als besonders gefährlich eingeschätzten Kriminalitätsbereich erfüllen hilft, und zwar durch Einblick in dessen Strukturen und durch deren Zerschlagung.

208

(a) Das Phänomen der Organisierten Kriminalität lässt sich allerdings nur schwer fassen, so dass gegenwärtig nur begrenzte Aussagen möglich sind, wie weit das vom Gesetzgeber angestrebte besondere Ziel erreicht werden kann.

209

Schon die Definition des Begriffs der Organisierten Kriminalität fällt schwer. In der öffentlichen Diskussion wird meist der Begriffsbestimmung der gemeinsamen Arbeitsgruppe der Innenminister- und der Justizministerkonferenz gefolgt. Danach versteht man unter Organisierter Kriminalität "die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wennBVerfGE 109, 279 (338) BVerfGE 109, 279 (339)mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken" (MBl.NW 1990, S. 1721). Diese Begriffsbestimmung zeigt, dass als Organisierte Kriminalität nicht ein eingrenzbarer Straftatbestand oder die Summe einzelner Straftatbestände, sondern eine komplexe Erscheinungsform abweichenden Verhaltens verstanden werden soll.

210

Zur Unbestimmtheit des Begriffs treten Ungewissheiten über das in Deutschland bestehende Ausmaß und die Erscheinungsform der Organisierten Kriminalität hinzu. Das Phänomen ist trotz mehrerer Untersuchungen, insbesondere des Kriminalistischen Instituts des Bundeskriminalamtes, kriminologisch nur begrenzt aufgeklärt. In der jüngsten, bisher umfassendsten, wenn auch nicht repräsentativen Untersuchung zur Organisierten Kriminalität in Deutschland kommt der vom Gericht als Sachverständiger angehörte Privatdozent Dr. Kinzig zu einer skeptischen Einschätzung (näher dazu Kinzig, Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, 2003). Er hat in seinen Untersuchungen ein gegenüber herkömmlichen Kriminalitätsfeldern deutlich gesteigertes Bedrohungspotential in den von ihm analysierten Fällen nicht oder allenfalls vereinzelt finden können. Als Unterschiede zu Fällen gewöhnlicher Kriminalität benennt er: die Begehung so genannter opferloser Delikte, ein hoher Ausländeranteil sowie die Internationalität der Tatbegehung. Hinzu träten eine gewisse Arbeitsteilung und Dauerhaftigkeit sowie Planmäßigkeit, Professionalität und Konspirativität.

211

(b) Ob damit Strukturen gegeben sind, zu deren Durchdringung die akustische Wohnraumüberwachung als Mittel der Strafverfolgung in besonderer Weise beitragen kann, lässt sich gegenwärtig nicht abschließend beurteilen. Die Bundesländer gehen in den von der Bundesregierung eingeholten und dem Gericht vorgelegten Stellungnahmen allerdings übereinstimmend davon aus, dass die Ermittlungsmaßnahme in der Praxis grundsätzlich geeignet ist,BVerfGE 109, 279 (339) BVerfGE 109, 279 (340)nicht nur Delikte aus dem Bereich der Organisierten Kriminalität aufzuklären, sondern auch in deren kriminelle Organisationsstrukturen einzudringen.

212

Es ist verfassungsrechtlich nicht zu beanstanden, dass der Gesetzgeber von einer entsprechenden Einschätzung ausgegangen ist. Die verbleibende Unsicherheit macht es erforderlich, die Entwicklung zu beobachten und fortlaufend zu prüfen, ob das Ermittlungsinstrument tatsächlich geeignet ist, auch das mit ihm verfolgte spezielle Ziel in hinreichendem Maße zu erreichen (zur Überprüfung gesetzlicher Regelungen vgl. BVerfGE 33, 171 [189 f.]; 37, 104 [118]; 88, 203 [310]).

213

Der Gesetzgeber hat dafür schon Vorkehrungen getroffen. Eine fortlaufende Prüfung wird insbesondere durch die nach Art. 13 Abs. 6 GG in Verbindung mit § 100 e StPO bestehenden Berichtspflichten sichergestellt. Darüber hinaus hat die Bundesregierung zur weiteren Unterrichtung des Parlaments eine rechtstatsächliche Untersuchung zu den Wirkungen der akustischen Wohnraumüberwachung in Auftrag gegeben, die im Mai 2004 abgeschlossen sein soll.

214

cc) Das angegriffene Gesetz ist zur Erreichung seines Zwecks auch erforderlich. Ein gleich wirksames, aber die Grundrechte weniger beeinträchtigendes Mittel steht nicht zur Verfügung (1). Im Übrigen hat der Gesetzgeber die Wahrung der Erforderlichkeit der akustischen Wohnraumüberwachung durch normative Vorgaben des Eingriffstatbestandes hinreichend sichergestellt (2).

215

(1) Es sind keine Ermittlungsmaßnahmen ersichtlich, die generell weniger belastend und zur Erreichung desselben Aufklärungszwecks ebenso geeignet wären.

216

Auch bei der Beurteilung der Erforderlichkeit des gewählten Mittels zur Erreichung der erstrebten Ziele steht dem Gesetzgeber ein Beurteilungsspielraum zu, dessen Handhabung vom Bundesverfassungsgericht nur in begrenztem Umfang überprüft werden kann (vgl. BVerfGE 90, 145 [173]). Nach der Einschätzung des Gesetzgebers haben zur Einführung der akustischen Wohnraumüberwachung keine weniger grundrechtsbeeinträchtigenden Alternativen bestanden. Herkömmliche Ermittlungsmethoden, einschließlichBVerfGE 109, 279 (340) BVerfGE 109, 279 (341)der Telefonüberwachung, würden in der Regel nicht ausreichen, um bei organisiert vorgehenden Banden, die sich fast völlig nach außen abschotteten, die Ermittlungsmaßnahmen in den Kernbereich der Organisierten Kriminalität hineinzutragen. Aus der zunehmenden Bedrohung von Bürgern und Staat folge das dringende Erfordernis, über die bisherigen Strafverfolgungsmaßnahmen hinaus auch den Einsatz technischer Mittel zum Abhören von Wohnungen zuzulassen (vgl. BTDrucks 13/8650, S. 4 und 13/8651, S. 9, 10 und 13). Diese Einschätzung ist zumindest nach derzeitigem Erkenntnisstand über die Erscheinungsformen Organisierter Kriminalität verfassungsrechtlich nicht zu beanstanden.

217

Der Aufklärungszweck ist von der konkreten Ermittlungssituation abhängig, so dass sich nur im Einzelfall zuverlässig beurteilen lässt, ob eine weniger belastende Alternative tatsächlich besteht. So kann der Einsatz eines verdeckten Ermittlers jedenfalls dann kein gleich geeignetes milderes Mittel sein, wenn es um Ermittlungen in einem konspirativ abgeschotteten Feld der Organisierten Kriminalität mit ethnisch homogenen Führungsebenen geht. Das Abhören von Telefonen kann ebenfalls nicht stets den gleichen Erfolg bringen, weil damit nur Gespräche abgehört werden können, die telefonisch geführt werden. Auf entscheidende Gespräche der Führungsebene einer Organisation wird dies jedoch häufig nicht zutreffen. Auch die Personenobservation ist generell kein gleich geeignetes Mittel. Mit ihr lässt sich zwar das Umfeld eines Beschuldigten ermitteln, nicht aber eine Kenntnis von den Inhalten der Kommunikation des Beschuldigten erlangen.

218

(2) Der Gesetzgeber hat darüber hinaus rechtliche Sicherungen dafür eingeführt, dass die akustische Wohnraumüberwachung nur als letztes Mittel eingesetzt wird.

219

Schon Art. 13 Abs. 3 GG bestimmt, dass die akustische Wohnraumüberwachung nur eingesetzt werden darf, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Diese Subsidiaritätsregelung ist in die angegriffene Vorschrift des § 100 c Abs. 1 Nr. 3 StPO aufgenommen worden. Die akustische Wohnraumüberwachung ist danach nur als letztes Mittel der Strafverfolgung zulässig.BVerfGE 109, 279 (341)

220

BVerfGE 109, 279 (342)(a) Art. 13 Abs. 3 GG erlaubt die akustische Wohnraumüberwachung, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert wäre. Das Merkmal "unverhältnismäßig erschwert" umschreibt den Ermittlungsaufwand, der voraussichtlich benötigt würde, wenn die Strafverfolgungsbehörden auf die akustische Wohnraumüberwachung im konkreten Fall verzichteten und stattdessen andere Ermittlungsmaßnahmen ergriffen. Die Strafprozessordnung kennt in den bisher bestehenden Subsidiaritätsklauseln für prozessuale Eingriffsbefugnisse die Begriffe "erschwert" und "wesentlich erschwert". Die unverhältnismäßige Erschwernis enthält gegenüber diesen Merkmalen eine weitere Steigerung und bringt damit eine Rangfolge zum Ausdruck, in der die akustische Wohnraumüberwachung als letztes Mittel gekennzeichnet ist (vgl. auch BTDrucks 13/8650, S. 5). Der ultima ratio-Gedanke setzt die Aussichtslosigkeit anderer Ermittlungsmaßnahmen voraus und ist auch für die Erschwernisprognose maßgeblich. Dem verfassungsändernden Gesetzgeber kam es darauf an, die ermittlungstaktischen Notwendigkeiten in besonderer Weise gegen das Gewicht der Rechtsgutbeeinträchtigung abzuwägen. Es sind bis zum Grade der Unverhältnismäßigkeit Erschwernisse in der Ermittlungsarbeit hinzunehmen, ehe auf das Mittel der Wohnraumüberwachung zurückgegriffen werden darf.

221

(b) Die akustische Wohnraumüberwachung ist auch hinsichtlich des Merkmals der Aussichtslosigkeit in der Konkurrenz mit anderen Ermittlungsmaßnahmen das letzte Mittel der Strafverfolgung.

222

Neben dem Abhören und Aufzeichnen des in der Wohnung nichtöffentlich gesprochenen Wortes sind allerdings die Telefonüberwachung, das Abhören außerhalb von Wohnungen und der Einsatz des verdeckten Ermittlers ebenfalls nur gesetzlich zulässig, wenn die Sachverhaltserforschung auf andere Weise aussichtslos wäre. Bei wortgetreuer Auslegung entstünde auf diese Weise ein Ringverweis zwischen denjenigen Normen, die die Aussichtslosigkeit anderer Ermittlungsmaßnahmen als Subsidiaritätsmerkmal enthalten. Dies entspräche dem Sinn der Regelung nicht.

223

Die akustische Wohnraumüberwachung tritt gegenüber sämtlichen anderen Ermittlungsmaßnahmen bereits von Verfassungs weBVerfGE 109, 279 (342)BVerfGE 109, 279 (343)gen zurück. Sie soll nur dort zum Einsatz gelangen, wo andere Ermittlungsmaßnahmen versagen. Die Absicht des verfassungsändernden Gesetzgebers, die

akustische Wohnraumüberwachung wegen der Schwere des Eingriffs mit Hilfe der gewählten Subsidiaritätsklausel als ultima ratio der Strafverfolgung auszugestalten, bezieht sich insoweit nicht nur auf das Merkmal der unverhältnismäßigen Erschwernis, sondern in gleicher Weise auf das Merkmal der Aussichtslosigkeit. Der verfassungsändernde Gesetzgeber hat die Subsidiaritätsklausel unmittelbar in den Art. 13 Abs. 3 GG aufgenommen und ihr damit gegenüber anderen einfachgesetzlichen Subsidiaritätsklauseln ein verfassungsrechtliches und damit besonderes Gewicht gegeben.

224

dd) Soweit die akustische Wohnraumüberwachung den absolut geschützten Kernbereich privater Lebensgestaltung nicht betrifft, hat der verfassungsändernde Gesetzgeber unter Konkretisierung des Grundsatzes der Verhältnismäßigkeit in Art. 13 Abs. 3 GG besondere Anforderungen an die Rechtmäßigkeit aufgestellt. Der Straftatenkatalog des § 100 c Abs. 1 Nr. 3 StPO genügt diesen verfassungsrechtlichen Anforderungen insoweit allerdings nicht, als er sich nicht auf besonders schwere Straftaten im Sinne des Art. 13 Abs. 3 GG beschränkt.

225

Der verfassungsändernde Gesetzgeber hat die Ermächtigung in Art. 13 Abs. 3 GG dahingehend eingeschränkt, dass der Verdacht sich auf eine durch Gesetz einzeln bestimmte besonders schwere Straftat beziehen muss. In der Folge ist die Ermächtigung in § 100 c Abs. 1 Nr. 3 StPO auf so genannte Katalogtaten begrenzt worden. Das Erfordernis, dass der intensive Eingriff in das Grundrecht des Art. 13 Abs. 1 GG nur bei einer besonderen Schwere der Straftat gerechtfertigt ist, hat der Gesetzgeber ausweislich der Gesetzesmaterialien zwar erkannt (vgl. BTDrucks 13/8650, S. 3; 13/8651, S. 13; 13/9642, S. 4; 13/9661, S. 6), aber nicht in stimmiger Weise umgesetzt. Anhand des Straftatenkatalogs des § 100 c Abs. 1 Nr. 3 StPO wird nicht erkennbar, nach welchen Kriterien die dort aufgeführten verschiedenartigen Vergehen und Verbrechen ausgewählt worden sind. Die in Bezug genommenen Normen dienen dem Schutz je unterschiedlicher Rechtsgüter, und die Straftaten weisen je unterBVerfGE 109, 279 (343)BVerfGE 109, 279 (344)schiedliche Unrechtsgehalte auf. Eine besondere Schwere der Straftat wird auch nicht stets durch den jeweiligen Strafrahmen indiziert. Aufgeführt werden Straftaten, für die Geldstrafen oder Freiheitsstrafen ab drei Monaten als Mindeststrafen vorgesehen sind, und solche mit Höchststrafen bis zu drei Jahren, aber auch bis zu lebenslänglich. Dieser Straftatenkatalog wird dem verfassungsrechtlichen Erfordernis der Beschränkung der Wohnraumüberwachung auf die Verfolgung besonders schwerer Straftaten nur teilweise gerecht.

226

(1) Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale und Tatfolgen. Sie allein müssen bereits die besondere, deutlich über dem Durchschnitt liegende Schwere des jeweiligen Straftatbestandes begründen.

227

(a) Der verfassungsrechtliche Begriff der besonders schweren Straftat kann nicht mit dem strafprozessualen Begriff einer Straftat von erheblicher Bedeutung gleichgesetzt werden. In der Strafprozessordnung gibt es neben der akustischen Wohnraumüberwachung weitere Eingriffsmaßnahmen, die ein bestimmtes Gewicht der aufzuklärenden Tat voraussetzen. So sind der genetische Fingerabdruck (§ 81 g), die Rasterfahndung (§ 98 a), die Auskunft über Verbindungsdaten der Telekommunikation (§ 100 g) und der Einsatz eines verdeckten Ermittlers (§ 110 a) nur zulässig, wenn das zu verfolgende Delikt eine Straftat von erheblicher Bedeutung ist. Eine solche Straftat muss mindestens der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vgl. BVerfGE 103, 21 [34]; 107, 299 [322]).

228

Die von Art. 13 Abs. 3 GG vorausgesetzten "besonders schweren Straftaten" müssen den mittleren Kriminalitätsbereich deutlich übersteigen. Es würde dem Sinn und Zweck des Art. 13 Abs. 3 GG nicht entsprechen, die akustische Wohnraumüberwachung nur von Voraussetzungen abhängig zu machen, die für Ermittlungsmaßnahmen geringerer Eingriffstiefe vorgesehen sind. Während beim Einsatz eines verdeckten Ermittlers die Informationserlangung mit dem -- wenn auch auf Täuschung beruhenden -- Einverständnis des BeBVerfGE 109, 279 (344)BVerfGE 109, 279 (345)troffenen erfolgt, wird die akustische Wohnraumüberwachung ohne Wissen des Betroffenen durchgeführt. Die Auskunft über die Verbindungsdaten der Telekommunikation stellt zwar einen erheblichen Eingriff in das Fernmeldegeheimnis dar (vgl. BVerfGE 107, 299 [318]), führt jedoch nicht zur Kenntnisnahme von Gesprächsinhalten und weist deshalb eine geringere Nähe zum Kernbereich privater Lebensgestaltung auf. Nach der Einschätzung des verfassungsändernden Gesetzgebers stellt die akustische Wohnraumüberwachung im Spektrum der strafprozessualen Maßnahmen einen besonders schweren Grundrechtseingriff dar, der deshalb auch im Hinblick auf die Schwere der zu verfolgenden Straftat an besonders strenge Eingriffsvoraussetzungen gebunden worden ist.

229

(b) Damit ist der Gesetzgeber indes nicht auf die Auswahl von Tatbeständen beschränkt, die als Verbrechen im Sinne des § 12 StGB einzuordnen sind. Hätte der verfassungsändernde Gesetzgeber sich an der Einteilung der Straftaten nach Verbrechen und Vergehen orientieren wollen, hätte es nahe gelegen, den Art. 13 Abs. 3 GG entsprechend zu formulieren. Auch die Aufnahme von Vergehenstatbeständen in den Straftatenkatalog der angegrif-

fenen Vorschrift ist nach Art. 13 Abs. 3 GG zulässig, wenn die Tatbestände das Merkmal der besonders schweren Straftat ausfüllen.

230

(c) Bei der Auswahl der in Betracht kommenden Delikte ist der Gesetzgeber durch Art. 13 Abs. 3 GG nicht auf solche Straftaten beschränkt worden, die typische Erscheinungsformen der Organisierten Kriminalität darstellen oder im konkreten Einzelfall in diesem Umfeld begangen werden. Zwar war und ist die Bekämpfung der Organisierten Kriminalität Hintergrund und Anlass der Änderung des Art. 13 GG. Das hat in Absatz 3 jedoch nicht zu einer Beschränkung des Straftatenkatalogs auf ausschließlich der Organisierten Kriminalität zurechenbare Delikte geführt.

231

Andererseits können Straftaten nicht allein deshalb als besonders schwer angesehen werden, weil sie für die Organisierte Kriminalität typisch sind. In ihrem Umfeld werden sowohl schwere wie auch leichte Straftaten begangen. Den Anforderungen des Art. 13 Abs. 3 GG ist nicht schon dadurch Genüge getan, dass ein Delikt im Rahmen der Organisierten Kriminalität erfolgt, wenn sich diese BegeBVerfGE 109, 279 (345)BVerfGE 109, 279 (346)hungsform nicht im Tatbestand niederschlägt und zugleich das besonders schwere Unrecht der Tat begründet.

232

(d) Art. 13 Abs. 3 Satz 1 GG fordert, dass die aufgezählten Katalogtaten schon als solche und nicht nur im Einzelfall besonders schwer sind. Würde bereits das mögliche schwere Tatunrecht eines Delikts im Einzelfall als ausreichend für eine Aufnahme in den Straftatenkatalog angesehen werden, käme dem Merkmal der besonders schweren Straftat in Art. 13 Abs. 3 GG keine eingriffsbegrenzende Funktion mehr zu, weil letztlich nahezu jedes Delikt des Strafgesetzbuchs im Einzelfall besonders schwer sein kann und damit Aufnahme in den Straftatenkatalog finden könnte. Die Gestaltung des Katalogs wäre bei dieser Auslegung des Art. 13 Abs. 3 GG beliebig und vor allem auch beliebig erweiterbar.

233

(e) Der Eingriff durch akustische Wohnraumüberwachung hat in einengender Auslegung des § 100 c Abs. 1 Nr. 3 StPO zur Voraussetzung, dass der Verdacht einer abstrakt schweren Katalogstraftat auch im konkreten Fall besonders schwer wiegt (vgl. -- zu § 100 g StPO -- BVerfGE 107, 299 [322]). Denn der Eingriff in das Wohnungsgrundrecht muss auch im Einzelfall mit dem Blick auf die von der Straftat ausgehende Rechtsgutsverletzung gerechtfertigt sein.

234

Ein Anhaltspunkt für die Schwere sind die Folgen der Tat für betroffene Rechtsgüter. Bei bestimmten Straftaten -- wie Mord und Totschlag -- ist die hinreichende Schwere auch im Einzelfall schon durch das verletzte Rechtsgut indiziert, bei anderen bedarf sie der eigenständigen Feststellung. Die besondere Schwere der Tat im Einzelfall kann insbesondere durch die faktische Verzahnung mit anderen Katalogstraftaten oder durch das Zusammenwirken mit anderen Straftätern begründet werden. Diese Lage ist bei einem arbeitsteiligen, gegebenenfalls auch vernetzt erfolgenden Zusammenwirken mehrerer Täter im Zuge der Verwirklichung eines komplexen, mehrere Rechtsgüter verletzenden kriminellen Geschehens gegeben, wie es der verfassungsändernde Gesetzgeber für die Organisierte Kriminalität als typisch angesehen hat. Für die ebenfalls aufgeführten Straftaten des Friedensverrats, des Hochverrats und bestimmter Delikte der Gefährdung des demokratischen Rechtsstaats kann Gleiches gelten. Dass der Gesetzgeber an solche Tatkomplexe geBVerfGE 109, 279 (346)BVerfGE 109, 279 (347)dacht hat, wird insbesondere daraus ersichtlich, dass er ausweislich der Gesetzesmaterialien hoffte, mit dem Instrumentarium des Art. 13 Abs. 3 GG auch an Hauptverantwortliche, Organisatoren, Finanziers und Drahtzieher heranzukommen (vgl. BTDrucks 13/8651, S. 9). Zwar kann sich die Schwere der Straftat nur auf die jeweils begangene Tat beziehen, nicht etwa auf erst zukünftig zu erwartende Taten. Insoweit aber kann der Unrechtsgehalt des gesamten Tatkomplexes auf die Bewertung der Tat als schwer zurückwirken.

235

(2) Der Gesetzgeber hat die Normierung der Katalogtaten nicht auf Straftaten begrenzt, die bei abstrakter Betrachtung besonders schwer im Sinne des Art. 13 Abs. 3 GG sind. Soweit dies nicht geschehen ist, genügt § 100 c Abs. 1 Nr. 3 StPO nicht Art. 13 Abs. 3 GG. Der Überprüfung unterliegen insoweit gemäß § 78 Satz 2, § 82 Abs. 1 BVerfGG, die im Verfassungsbeschwerdeverfahren entsprechend anzuwenden sind (vgl. BVerfGE 18, 288 [300]), auch die nach Erhebung der Verfassungsbeschwerde erfolgten Gesetzesänderungen.

236

(a) Aus dem Strafrahmen der Deliktsnorm ergibt sich, ob die Tat vom Gesetzgeber als besonders schwer eingestuft worden ist. Der Straftatenkatalog des § 100 c Abs. 1 Nr. 3 StPO umfasst neben Verbrechenstatbeständen Vergehenstatbestände, darunter auch solche, deren Strafrahmen keinen überdurchschnittlichen Unrechtsgehalt zum Ausdruck bringt. Die Mindeststrafen reichen von Geldstrafen über Freiheitsstrafen von drei oder von sechs Monaten bis zu solchen von einem Jahr, von zwei, drei, fünf oder zehn Jahren. Auch die Höchststrafen variieren von drei Jahren über fünf und zehn Jahre bis zu lebenslänglich.

237

Der Gesetzgeber verfügt über einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung, welche Straftaten Anlass für die akustische Wohnraumüberwachung sein sollen.

Bezogen auf Art. 13 Abs. 3 GG muss es sich abstrakt um eine besonders schwere Straftat handeln. Dafür gibt der Strafrahmen einen maßgebenden Anhaltspunkt. Von der besonderen Schwere einer Straftat im Sinne des Art. 13 Abs. 3 GG ist nur auszugehen, wenn sie der Gesetzgeber jedenfalls mit einerBVerfGE 109, 279 (347) BVerfGE 109, 279 (348)höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat. Nach der gesetzlichen Systematik wird in Tatbeständen mit einem fünf Jahre übersteigenden oberen Strafmaß sogleich eine Höchststrafe von zehn Jahren Freiheitsentzug oder mehr normiert. Sie ist denjenigen Delikten vorbehalten, die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen.

238

(b) Unter Anwendung dieses Maßstabs erweist sich die Bezugnahme des § 100 c Abs. 1 Nr. 3 StPO auf solche Straftatbestände als verfassungswidrig, die ausweislich ihrer Strafandrohung allenfalls dem mittleren Kriminalitätsbereich zugeordnet werden können. Dazu zählen in der aktuell geltenden Fassung des § 100 c Abs. 1 Nr. 3 Buchstabe a StPO: Vorbereitung einer Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Europaschecks (§ 152 b Abs. 5 i.V.m. § 149 Abs. 1 StGB); Vorbereitung einer Verschleppung (§ 234 a Abs. 3 StGB); Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte (§ 261 Abs. 1, 2 StGB); Bestechlichkeit (§ 332 Abs. 1, auch i.V.m. Abs. 3 StGB); Bestechung (§ 334 StGB). In § 100 c Abs. 1 Nr. 3 Buchstabe b StPO sind betroffen: § 51 (mit Ausnahme der Qualifikation nach Abs. 2) sowie § 52 Abs. 1 Nr. 1, 2 Buchstabe c und d, Abs. 6 Waffengesetz; § 34 Abs. 1 bis 3 Außenwirtschaftsgesetz; § 19 Abs. 1 und 3 Nr. 1 sowie § 22 a Abs. 1 und 3 Kriegswaffenkontrollgesetz. Aus § 100 c Abs. 1 Nr. 3 Buchstabe c wird erfasst: § 30 b Betäubungsmittelgesetz in Verbindung mit § 129 StGB. Aus § 100 c Abs. 1 Nr. 3 Buchstabe d StPO genügen den Anforderungen nicht: Aufstacheln zum Angriffskrieg (§ 80 a StGB); Verstoß gegen ein Vereinigungsverbot (§ 85 StGB); Agententätigkeit zu Sabotagezwecken (§ 87 StGB); verfassungsfeindliche Sabotage (§ 88 StGB); Offenbaren von Staatsgeheimnissen (§ 95 Abs. 1 StGB); Auskundschaften von Staatsgeheimnissen (§ 96 Abs. 2 StGB); landesverräterische Agententätigkeit (§ 98 Abs. 1 Satz 1 StGB); geheimdienstliche Agententätigkeit (§ 99 Abs. 1 StGB); landesverräterische Fälschung (§ 100 a Abs. 1 und 2 StGB). Schließlich genügen in § 100 c Abs. 1 Nr. 3 Buchstabe e StPO nicht den Anforderungen: Bildung einer kriminellen Vereinigung in einem besonders schweren Fall (§ 129 Abs. 4 i.V.m. Abs. 1BVerfGE 109, 279 (348) BVerfGE 109, 279 (349)StGB); Unterstützung einer terroristischen Vereinigung (§ 129 a Abs. 3 sowie Abs. 5 Satz 1 2. Halbsatz und Satz 2, jeweils auch i.V.m. § 129 b Abs. 1 StGB).

239

Verfassungswidrig waren auch der Verweis in § 100 c Abs. 1 Nr. 3 Buchstabe a StPO auf § 152 a Abs. 5 in Verbindung mit § 149 Abs. 1 StGB und die in § 100 c Abs. 1 Nr. 3 Buchstabe b StPO erfolgte Bezugnahme auf § 52 a des Waffengesetzes in der Fassung des Gesetzes zur Änderung des Waffenrechts vom 31. Mai 1978 (BGBl. I S. 641) mit Ausnahme der Qualifikation nach Absatz 2 sowie auf § 53 Abs. 1 Satz 1 Nr. 1, 2, Satz 2 des Waffengesetzes in der Fassung des Gesetzes zur Änderung des Waffengesetzes vom 4. März 1976 (BGBl. I S. 417). Gleiches gilt für die Verweisung des § 100 c Abs. 1 Nr. 3 Buchstabe b StPO auf § 22 a Abs. 1 und 3 Kriegswaffenkontrollgesetz in der Fassung des Gesetzes zur Änderung des Waffenrechts vom 31. Mai 1978 (BGBl. I S. 641; damals § 16). Ebenfalls verfassungswidrig waren die Bezugnahmen in § 100 c Abs. 1 Nr. 3 Buchstabe e StPO auf § 129 a Abs. 3 StGB in der Fassung des Sechsten Gesetzes zur Reform des Strafrechts vom 26. Januar 1998 (BGBl. I S. 164) sowie auf § 129 a Abs. 3 StGB in der bis zum 27. Dezember 2003 geltenden Fassung des Gesetzes zur Einführung des Völkerstrafgesetzbuches vom 26. Juni 2002 (BGBl. I S. 2254).

240

Soweit eine Höchststrafe von über fünf Jahren vorgesehen ist, entspricht die Bezugnahme auf den Straftatenkatalog den verfassungsrechtlichen Vorgaben. Keinen verfassungsrechtlichen Bedenken ist der Verweis auf solche Qualifikationstatbestände ausgesetzt, die eine höhere Höchststrafe als fünf Jahre unter spezifischen, in einem Qualifikationstatbestand zumindest mit einem Regelbeispiel näher umschriebenen tatbestandlichen Voraussetzungen vorsehen, wie etwa § 261 Abs. 4 StGB oder § 51 Abs. 2 WaffG. Erfüllt der Grundtatbestand die Anforderungen, so fällt er aus dem Katalog nicht insoweit heraus, als in minder schweren, vom Gesetzgeber tatbestandlich nicht näher festgelegten Fällen eine niedrigere Höchststrafe als fünf Jahre Freiheitsentzug vorgesehen worden ist.

241

ee) Die gesetzliche Ermächtigung trägt im Übrigen den Anforderungen des Art. 13 Abs. 3 GG und des Grundsatzes der VerhältnisBVerfGE 109, 279 (349)BVerfGE 109, 279 (350)mäßigkeit im engeren Sinne jedenfalls bei restriktiver Auslegung hinreichend Rechnung.

242

(1) In dem Spannungsverhältnis zwischen der Pflicht des Staates zur Gewährleistung einer rechtsstaatlichen Strafrechtspflege und dem Interesse des Beschuldigten und der Drittbetroffenen an der Wahrung ihrer verfassungsrechtlich verbürgten Rechte ist es zunächst Aufgabe des Gesetzgebers, einen abstrakten Ausgleich der widerstreitenden Interessen zu erreichen. Ferner haben die Gerichte im Rahmen der Auslegung und Anwendung grundrechtsbeschränkender Normen für die Angemessenheit der von ihnen getroffenen konkreten Entscheidung Sorge zu tragen. Gleiches gilt für die Behörden, die Überwachungsmaßnahmen ausführen. Dabei ist der Verhältnismäßigkeitsgrundsatz auch insoweit maßgebend, als Art. 13 Abs. 3 GG keine ausdrücklichen Vorgaben für die

Ausgestaltung der angegriffenen strafprozessualen Eingriffsbefugnis und ihrer Anwendung im Einzelfall getroffen hat.

243

(2) § 100 c Abs. 1 Nr. 3 StPO ist nach diesen Grundsätzen -- abgesehen von dem überschießenden Straftatenkatalog -- bei restriktiver Auslegung verfassungsrechtlich nicht zu beanstanden.

244

(a) Der in § 100 c Abs. 1 Nr. 3 StPO festgelegte Verdachtsgrad begegnet keinen verfassungsrechtlichen Bedenken.

245

Gemäß § 100 c Abs. 1 Nr. 3 StPO ist eine akustische Wohnraumüberwachung zulässig, wenn "bestimmte Tatsachen den Verdacht" der Begehung einer besonders schweren Straftat begründen. Die angegriffene Vorschrift wiederholt wortgleich die Formulierung des Art. 13 Abs. 3 GG, so dass die Vereinbarkeit des Gesetzes mit der verfassungsrechtlichen Grundrechtsschranke insoweit nicht in Zweifel steht.

246

Der durch bestimmte Tatsachen begründete Verdacht unterliegt zwar höheren Anforderungen als der bloße Anfangsverdacht, erreicht jedoch nicht bereits den Grad eines "hinreichenden" oder gar "dringenden" Tatverdachts, den andere Normen der Strafprozessordnung vorsehen. § 100 c Abs. 1 Nr. 3 StPO erfordert eine konkretisierte Verdachtslage. Hierfür reicht das bloße Vorliegen von Anhaltspunkten nicht aus. Es müssen vielmehr konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den VerBVerfGE 109, 279 (350)BVerfGE 109, 279 (351)dacht vorhanden sein (vgl. BVerfGE 100, 313 [395]). Nur bereits ermittelte und in Antrag und Anordnung genannte Tatsachen kommen für die jeweilige Bewertung in Betracht. Da sich die akustische Wohnraumüberwachung nur gegen den Beschuldigten richten und erst als letztes Mittel der Strafverfolgung eingesetzt werden darf, muss auf Grund der bereits vorliegenden Erkenntnisse eine erhöhte Wahrscheinlichkeit für die Begehung der besonders schweren Katalogstraftat bestehen.

247

(b) Eine Anhebung der in § 100 c Abs. 1 Nr. 3 StPO enthaltenen Verdachtsstufe ist aus Gründen der Verhältnismäßigkeit nicht geboten. Neben der Schwere der Tat ist zwar auch die Stärke des Tatverdachts mitentscheidend dafür, ob eine strafprozessuale Ermittlungsmaßnahme in einem angemessenen Verhältnis zu dem Gewicht der Grundrechtsbeeinträchtigung steht (vgl. BVerfGE 107, 299 [322]). Es ist jedoch auch in Anbetracht der Eingriffsintensität der akustischen Wohnraumüberwachung nicht verfassungsrechtlich geboten, die Maßnahme vom Vorliegen eines Verdachtsgrades abhängig zu machen, der für andere Maßnahmen gilt. So ist es Sinn und Zweck des Ermittlungsverfahrens, den zureichenden Verdacht im Sinne des § 152 Abs. 2 StPO zu einem für die Anklageerhebung erforderlichen Tatverdacht gemäß § 170 Abs. 1 StPO zu erhärten oder den Beschuldigten zu entlasten. Die Verhängung der Untersuchungshaft nach § 112 Abs. 1 Satz 1 StPO setzt voraus, dass der Straftatverdacht dringend ist, das heißt nach dem gegenwärtigen Stand der Ermittlungen eine hohe Wahrscheinlichkeit für die Verurteilung des Beschuldigten besteht. In solchen Fällen liegt der Sachverhalt offen zutage. Folglich bedarf es seiner Erforschung durch den Einsatz technischer Mittel zur akustischen Wohnraumüberwachung regelmäßig nicht mehr. Wäre für die akustische Wohnraumüberwachung ein dringender Tatverdacht zu fordern, entfiele damit auch die Tauglichkeit des Mittels weitgehend.

248

Als Mittel der Sachverhaltserforschung soll die akustische Wohnraumüberwachung den für weitere Schritte, insbesondere eine Anklageerhebung (§ 170 Abs. 1 StPO) oder später den Eröffnungsbeschluss (§ 203 StPO), erforderlichen hinreichenden oder gar den für die Verhängung der Untersuchungshaft (§ 112 Abs. 1 Satz 1 StPO)BVerfGE 109, 279 (351) BVerfGE 109, 279 (352)geforderten dringenden Tatverdacht erst noch erbringen. Sie kann ihn deshalb nicht für ihre Zulässigkeit voraussetzen.

249

(3) § 100 c Abs. 1 Nr. 3 StPO ist auch insoweit mit Art. 13 Abs. 3 GG und den Anforderungen der Verhältnismäßigkeit vereinbar, als er neben der Erforschung des Sachverhalts auch die Ermittlung des Aufenthaltsorts des "Täters" zulässt.

250

Art. 13 Abs. 3 GG erwähnt als Fahndungsziel allein die Erforschung des Sachverhalts. Zudem erlaubt er nur die Überwachung von Wohnungen, in denen sich der Beschuldigte vermutlich aufhält. Die akustische Wohnraumüberwachung darf sich daher nur gegen den Beschuldigten, nicht auch gegen andere Personen richten. Dies setzt aber voraus, dass bekannt ist oder zumindest vermutet werden kann, dass sich der Beschuldigte in der Wohnung aufhält. Allerdings kann die Maßnahme dazu dienen, Informationen über den ständigen Aufenthalt des Täters zu gewinnen, soweit dies zur Sachverhaltsermittlung erforderlich ist. Darüber hinaus kommt sie zur Ermittlung des Aufenthalts von Mittätern in Betracht. Nach der Begründung des Gesetzentwurfs sieht der verfassungsändernde Gesetzgeber die Ermittlung des Aufenthalts von Mittätern als Teil der Erforschung des Sachverhalts und damit als zulässiges Ermittlungsziel einer akustischen Wohnraumüberwachung zu Strafverfolgungszwecken an (vgl. BTDrucks 13/8650, S. 5 sowie BTDrucks 13/8651, S. 13).

251

(4) Bei einer restriktiven Auslegung der angegriffenen Vorschrift des § 100 c Abs. 1 Nr. 3, Abs. 2 Satz 4 und 5 und Abs. 3 StPO kann auch sichergestellt werden, dass unverdächtige Dritte von der akustischen Wohnraumüberwachung nur in einem Maße betroffen werden, das in einem angemessenen Verhältnis zu den mit der Ermittlungsmaßnahme verfolgten Allgemeininteressen einer effektiven Strafverfolgung steht. Eine Überwachung Dritter scheidet allerdings -- wie stets -- von vornherein aus, wenn die Kommunikation den Kernbereich ihrer privaten Lebensgestaltung betrifft. Dies wird nicht der Fall sein, wenn sich der Tatverdächtige in einer von einem Dritten angemieteten konspirativen Wohnung aufhält. Demgegenüber ist der Kernbereich eher betroffen, wenn der Beschuldigte die Wohnung eines Dritten, etwa eines Freundes oder Familienmitglieds, nur vorübergehend und besuchsweise aufsucht.BVerfGE 109, 279 (352)

252

BVerfGE 109, 279 (353)(a) Für die Angemessenheit einer grundrechtsbeschränkenden Maßnahme ist die Eingriffsintensität mitentscheidend. Daher ist bedeutsam, wie viele Personen wie intensiven Beeinträchtigungen ausgesetzt sind und ob diese Personen hierfür einen Anlass gegeben haben (vgl. BVerfGE 100, 313 [376]). Das Gewicht der Beeinträchtigung hängt davon ab, ob die Betroffenen als Personen anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden können und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden (vgl. BVerfGE 100, 313 [376]; 107, 299 [320]). Auch macht es einen Unterschied, ob die Ermittlungsmaßnahmen in einer Privatwohnung oder in Betriebs- und Geschäftsräumen stattfinden und ob und in welcher Zahl unverdächtige Dritte mitbetroffen werden.

253

(a) Die akustische Wohnraumüberwachung ist ein besonders schwerwiegender Grundrechtseingriff. Bei ihrer Durchführung können in erheblichem Umfang solche Personen betroffen sein, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, aber mit dem Täter in Verbindung stehen oder sich in derselben Wohnung aufhalten.

254

Drittbetroffene in diesem Sinne sind diejenigen, die nicht selbst Zielpersonen der Maßnahme sind. Dazu gehören die Gesprächspartner des Beschuldigten, andere Personen, die sich in dessen Wohnung vorübergehend oder dauerhaft aufhalten, und nicht zuletzt auch diejenigen, die von Überwachungsmaßnahmen in Büro- und Geschäftsräumen betroffen werden. Außer dem Beschuldigten werden ferner solche Personen beeinträchtigt, deren Wohnung wegen des vermuteten Aufenthalts des Beschuldigten zum Objekt einer Überwachung wird. Auch insoweit sind diejenigen betroffen, die sich zu irgendeinem Zeitpunkt während der Durchführung der Maßnahme in der überwachten Wohnung aufhalten. Wird die Kommunikation Unverdächtiger erfasst, so schafft die akustische Wohnraumüberwachung für sie das Risiko, Gegenstand staatlicher Ermittlungen zu sein, das zu dem allgemeinen Risiko hinzutritt, einem unberechtigten Verdacht ausgesetzt zu werden (vgl. BVerfGE 107, 299 [321]).BVerfGE 109, 279 (353)

255

BVerfGE 109, 279 (354)Dass mit der Durchführung der akustischen Wohnraumüberwachung die Beeinträchtigung Unverdächtiger auch tatsächlich in erheblicher Anzahl verbunden ist, zeigt der Anteil der Nichtbeschuldigten an den insgesamt von Maßnahmen nach § 100 c Abs. 1 Nr. 3 StPO Betroffenen. Im Durchschnitt ergibt sich nach den jährlichen Berichten der Bundesregierung ein Anteil Nichtbeschuldigter an den formell Betroffenen von annähernd 50 vom Hundert. Hierbei ist jedoch zu berücksichtigen, dass als Betroffene nur die Beschuldigten und diejenigen Personen erfasst werden, die Inhaber des Schutzguts Wohnung sind. In den statistischen Angaben sind diejenigen Personen nicht enthalten, die sich zufällig in der überwachten Wohnung aufhalten (vgl. BTDrucks 14/8155, S. 8). Deren Anzahl kann aber auch bei der Überwachung einer Privatwohnung beträchtlich sein. Daher ist der Anteil der Nichtbeschuldigten, die von der Maßnahme erfasst werden, wahrscheinlich noch deutlich höher als die Statistik angibt.

256

Neben der hohen Anzahl der unverdächtig Betroffenen begründen vor allem Inhalt und Umfang der Kommunikation, die im Rahmen einer akustischen Wohnraumüberwachung abgehört wird, die besondere Intensität des Eingriffs. Zum Gegenstand der Überwachung kann die gesamte Alltagskommunikation werden, die innerhalb des Überwachungszeitraums in der Wohnung stattfindet. Daher ist der Anteil der überwachten Gespräche, deren Inhalt keinerlei strafrechtliche Relevanz aufweist, wahrscheinlich hoch.

257

(b) Die heimliche Überwachung des nichtöffentlich gesprochenen Wortes in Wohnungen betrifft nicht nur den Einzelnen, sondern kann sich auch auf die Kommunikation der Gesellschaft insgesamt auswirken. Von der Möglichkeit zur akustischen Wohnraumüberwachung können Einschüchterungseffekte ausgehen, denen insbesondere auch der Unverdächtige ausgesetzt ist, weil auch er nach den gesetzlichen Regelungen jederzeit und ohne sein Wissen von der Ermittlungsmaßnahme betroffen werden kann. Allein die Befürchtung einer Überwachung kann aber schon zu einer Befangenheit in der Kommunikation führen. Art. 13 GG schützt den Einzelnen vor staatlichen Eingriffen in die räumliche Privatsphäre und gewährleistet damit in seinem objektivrechtlichen Gehalt die VertrauBVerfGE 109, 279 (354)BVerfGE 109, 279 (355)lichkeit der Kommunikation auch in ihrer gesamtgesellschaftlichen Bedeutung. Die zum Schutze des einzelnen Grundrechtsträgers geschaffenen verfassungsrechtli-

chen und gesetzlichen Vorkehrungen kommen auch dem Vertrauen der Allgemeinheit in eine grundrechtsschonende Überwachungspraxis zugute (vgl. BVerfGE 107, 299 [328]).

258

(g) Soweit Art. 13 Abs. 3 GG nur die vermutliche Anwesenheit des Beschuldigten in der zu überwachenden Wohnung verlangt, formuliert er eine Mindestanforderung an die Wahrscheinlichkeit, dass der Beschuldigte sich in der Wohnung aufhält. Die Angemessenheit der akustischen Wohnraumüberwachung bleibt mit Blick auf die Eingriffstiefe allerdings nur dann gewahrt, wenn die Überwachungsmaßnahme von vornherein ausschließlich auf Gespräche des Beschuldigten gerichtet ist, weil nur insoweit angenommen werden kann, dass die Gespräche einen hinreichenden Bezug zur verfolgten Straftat aufweisen. Dies aber bedeutet zugleich, dass die akustische Wohnraumüberwachung nur bei aktueller, wenn auch gegebenenfalls nur vermuteter Anwesenheit des Beschuldigten in der zu überwachenden Wohnung zulässig ist. Dies kommt auch dem Schutz unverdächtiger Dritter entgegen.

259

(b) Diesen verfassungsrechtlichen Anforderungen an die Begrenzung der Eingriffe gegen unverdächtige Dritte werden die gesetzlichen Vorschriften gerecht.

260

(a) § 100 c Abs. 1 Nr. 3 StPO nimmt eine Eingrenzung auf das Abhören und die Aufzeichnung des nichtöffentlich gesprochenen Wortes des Beschuldigten vor. Hieraus kann zwar nicht hergeleitet werden, dass Worte anderer Personen einem Abhörverbot unterliegen, weil die Ermittlungsmaßnahme wegen der zwangsläufigen Beteiligung Dritter an Gesprächen des Beschuldigten dann nicht mehr durchgeführt werden könnte. Die Formulierung bringt aber gleichwohl zum Ausdruck, dass auch in der Wohnung des Beschuldigten allein die Aufnahme von Gesprächen erlaubt ist, an denen der Beschuldigte selbst als Gesprächsteilnehmer mitwirkt.

261

(b) § 100 c Abs. 2 Satz 5 StPO begrenzt die Möglichkeit, die Wohnung eines Nichtbeschuldigten in eine Überwachung einzubeziehen, in angemessener Weise.BVerfGE 109, 279 (355)

262

BVerfGE 109, 279 (356)§ 100 c Abs. 2 Satz 5 StPO gestattet es, die Wohnungen Nichtbeschuldigter nur abzuhören, "wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte sich in diesen aufhält, die Maßnahme in Wohnungen des Beschuldigten allein nicht zur Erforschung des Sachverhalts ... führen wird und dies auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre". Nach dem Wortlaut dieser Regelung bedarf es zunächst eines konkretisierten Verdachts, dass sich der Beschuldigte zur Zeit der Maßnahme in der Wohnung einer anderen Person aufhält. Dies ist gegebenenfalls durch andere Maßnahmen, wie eine Observation, sicherzustellen. Nicht auf konkrete Anhaltspunkte gestützte Vermutungen für die Anwesenheit des Beschuldigten in der Wohnung des Dritten reichen daher für den Beginn der Maßnahme nicht aus.

263

Dass darüber hinaus die aktuelle Anwesenheit des Beschuldigten während der Dauer der Durchführung der Maßnahme gefordert ist, folgt unmittelbar aus § 100 c Abs. 1 Nr. 3 StPO, da hiernach nur Gespräche des Beschuldigten abgehört und aufgezeichnet werden dürfen. Dieses Erfordernis wird auch durch § 100 c Abs. 2 Satz 1 StPO klargestellt, in dem es heißt, dass sich Maßnahmen nach Absatz 1 nur gegen den Beschuldigten richten dürfen. Eine Ausnahme hiervon, wie dies für Maßnahmen nach § 100 c Abs. 1 Nr. 1 und 2 StPO vorgesehen ist, gibt es nicht (vgl. BTDrucks 13/8651, S. 13). Die Einschränkung auf den Beschuldigten gilt deshalb auch für die Überwachung der Wohnung anderer Personen nach § 100 c Abs. 2 Satz 5 StPO.

264

Allein mit der aktuellen Anwesenheit des Beschuldigten in der Wohnung eines unverdächtigen Dritten wird die Angemessenheit der Maßnahme in Wohnungen Dritter aber noch nicht erreicht. Neben der von § 100 c Abs. 2 Satz 5 StPO vorgeschriebenen Subsidiarität einer Überwachung von Wohnungen Nichtbeschuldigter muss eine hinreichende Wahrscheinlichkeit bestehen, verfahrensrelevante Informationen zu gewinnen. Das verlangt nach tatsächlichen Anhaltspunkten dafür, dass der Beschuldigte in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird. Bloße Vermutungen und eine Überwachung "ins Blaue hinein", alBVerfGE 109, 279 (356)BVerfGE 109, 279 (357)lein getragen von der Hoffnung auf Erkenntnisse, genügen nicht.

265

(g) Wegen der besonderen Intensität des Grundrechtseingriffs für unverdächtige Dritte betreffen die zur Wahrung der Angemessenheit gebotenen Einschränkungen nicht nur die Wohnungen Dritter. Sie gelten auch für den Regelfall der Überwachung der Wohnung des Beschuldigten nach § 100 c Abs. 2 Satz 4 StPO, soweit sich in der Wohnung des Beschuldigten unverdächtige Dritte dauerhaft oder vorübergehend aufhalten.

266

(d) Der Gesetzgeber hat eine die Angemessenheit der gesetzlichen Ermächtigung wahrende Einschränkung ferner durch § 100 c Abs. 3 StPO vorgenommen. Zwar heißt es dort nur, dass Maßnahmen auch durchgeführt werden dürfen, wenn Dritte unvermeidbar betroffen sind. Im Umkehrschluss folgt daraus jedoch ebenfalls, dass die akustische Wohnraumüberwachung unzulässig ist, wenn diese zu einer vermeidbaren Beeinträchtigung führt.

267

Dritte im Sinne des § 100 c Abs. 2, 3 StPO sind all diejenigen Personen, die nicht Zielperson der Maßnahme sind. Da Zielpersonen einer akustischen Wohnraumüberwachung nach der ausdrücklichen Regelung des § 100 c Abs. 1 Nr. 3, Abs. 2 Satz 1 StPO ausschließlich Beschuldigte sind, gehören zu den Dritten im Sinne des § 100 c Abs. 3 StPO sämtliche anderen Betroffenen ungeachtet dessen, ob diese sich in der Wohnung des Beschuldigten oder in der überwachten Wohnung eines Dritten aufhalten. Unter § 100 c Abs. 3 StPO fallen damit ebenso Familienangehörige des Beschuldigten wie zufällig in der Wohnung anwesende Personen. Die Anforderungen, die an die Unvermeidbarkeit der Betroffenheit Dritter zu stellen sind, hängen maßgeblich von den tatsächlichen Gegebenheiten und Möglichkeiten des Ausschlusses Dritter im Einzelfall ab.

VII.

Die Regelungen in § 100 d Abs. 5 Satz 2 und § 100 f Abs. 1 StPO über die Verwendung personenbezogener Informationen in anderen Verfahren sind mit Art. 13 Abs. 1, Art. 2 Abs. 1 und Art. 1 Abs. 1 GG insoweit nicht vereinbar, als keine Pflicht zur Kennzeichnung der weitergegebenen Informationen begründet worden ist.

328

1. Die Vorschriften über die Weitergabe der aus Wohnraumüberwachungen zu Strafverfolgungszwecken gewonnenen Informationen nach § 100 d Abs. 5 und § 100 f Abs. 1 StPO sind von den Beschwerdeführern zu 2 allerdings nicht fristgerecht angegriffen worden. Nicht zulässigerweise angegriffene Vorschriften können aber bei bestehendem Regelungszusammenhang von Amts wegen auf ihre Verfassungsmäßigkeit überprüft werden, wenn ihre Verfassungswidrigkeit auf zulässigerweise angegriffene Vorschriften ausstrahlen würde (vgl. BVerfGE 30, 1 [29]) oder wenn sie notwendiger Bestandteil einer Gesamtregelung sind (vgl. MVVerfG, LKV 2000, S. 345 [347]). So liegt es hier. Die Tragweite der heimlichen akustischen Wohnraumüberwachung erschließt sich erst, wenn die Vorschriften für die Verwendung der Informationen unter Einschluss von Zufallsfunden (§ 100 d Abs. 5 StPO) in die Betrachtung einbezogen werden.

329

Die Schutzwirkungen des Art. 13 Abs. 1 und des Art. 2 Abs. 1 sowie Art. 1 Abs. 1 GG beziehen sich nicht nur auf die Erhebung, sondern ebenso auf die Weitergabe der Daten und Informationen, die durch einen Eingriff in die räumliche Privatsphäre gewonnen worden sind (vgl. BVerfGE 100, 313 [360] zu Art. 10 GG). Denn die verfassungsrechtliche Beurteilung der Informationserhebung hängt auch davon ab, in welchen Verwendungszusammenhängen die gewonnenen Informationen genutzt werden können und welcheBVerfGE 109, 279 (374) BVerfGE 109, 279 (375)Schutzvorkehrungen, insbesondere welche datenschutzrechtlichen Regelungen, getroffen worden sind. Wäre eine weitere Verwendung der Daten ohne verfassungsrechtlich hinreichende Sicherungen möglich, wäre auch die Datenerhebung verfassungswidrig. Solche Wirkungen sind durch die Einbeziehung der Verwendungsvorschriften in die verfassungsrechtliche Prüfung auszuschließen.

330

Nicht Gegenstand der Prüfung ist jedoch die Vorschrift des § 100 f Abs. 2 StPO. Sie regelt mit Blick auf das Strafverfahren die Verwendung personenbezogener Informationen, die aus präventiv-polizeilichen Maßnahmen der akustischen Wohnraumüberwachung gewonnen worden sind. Die im vorliegenden Verfahren zu überprüfenden Regelungen zur Durchführung der akustischen Wohraumüberwachung zum Zwecke der Strafverfolgung hätten auch dann Bestand, wenn sich die Verwendung von präventiv-polizeilich gewonnenen Daten im Strafverfahren als verfassungswidrig erwiese. § 100 f Abs. 2 StPO ist auch kein notwendiger Bestandteil der gesetzlichen Normen zur Durchführung der durch Art. 13 Abs. 3 GG ermöglichten Wohnraumüberwachung.

331

2. § 100 d Abs. 5 Satz 2 und § 100 f Abs. 1 StPO sind für sich genommen verfassungsrechtlich nicht zu beanstanden. Insbesondere begegnet die in den Vorschriften zugelassene Zweckänderung der durch akustische Wohnraumüberwachung gewonnenen personenbezogenen Informationen keinen verfassungsrechtlichen Bedenken.

332

a) Die Speicherung und Verwendung der mit der Wohnraumüberwachung gewonnenen personenbezogenen Informationen und Daten sind grundsätzlich an den Zweck und auch an das Ermittlungsverfahren gebunden, für die sie erhoben worden sind (vgl. BVerfGE 100, 313 [360] zu Art. 10 GG). Sollen die gewonnenen Informationen zu einem anderen Zweck als dem ursprünglich verfolgten verwendet werden, so stellt dies grundsätzlich einen eigenständigen Grundrechtseingriff dar, da sich der Schutz des Art. 13 Abs. 1 GG nicht nur auf die Phase der Datenerhebung in und aus Wohnungen beschränkt, sondern auch die Weitergabe einbezieht (vgl. BVerfGE 100, 313 [360] zu Art. 10 GG).

333

Zwar schließt der Grundsatz der Zweckbindung eine Zweckänderung nicht generell aus. Sie bedarf jedoch ihrerseits einer gesetzliBVerfGE 109, 279 (375)BVerfGE 109, 279 (376)chen Grundlage, die formell und materiell verfassungsmäßig ist. Dazu gehört, dass die Zweckänderung durch Allgemeinbelange gerechtfertigt ist, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden, und hinreichend normenklar geregelt sein. Schließlich dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht miteinander unvereinbar sein (vgl. BVerfGE 65, 1 [51, 62]; 100, 313 [360]).

334

b) Diesen Anforderungen werden die angegriffenen Regelungen für sich gesehen gerecht.

335

Nach § 100 d Abs. 5 Satz 2 StPO dürfen personenbezogene Informationen, die durch eine Maßnahme nach § 100 c Abs. 1 Nr. 3 StPO erlangt worden sind, in anderen Strafverfahren zu Beweiszwecken nur verwendet werden, soweit sich bei Gelegenheit der Auswertung Erkenntnisse ergeben, die zur Aufklärung einer in § 100 c Abs. 1 Nr. 3 StPO bezeichneten Straftat benötigt werden. Ferner dürfen die Informationen nach § 100 f Abs. 1 StPO zur Abwehr einer im Einzelfall bestehenden Gefahr für Leben, Leib oder Freiheit einer Person oder für erhebliche Sach- oder Vermögenswerte verwendet werden. Mit diesen Regelungen hat der Gesetzgeber spezialgesetzliche Verwendungseinschränkungen getroffen. Sie bleiben durch die allgemeine Vorschrift des § 477 Abs. 2 StPO unberührt (vgl. Franke, in: Karlsruher Kommentar zur Strafprozessordnung, a.a.O., § 477 Rn. 3 m.w.N.).

336

aa) Der Zweck der Regelungen ist verfassungsrechtlich gerechtfertigt. Die Daten und Informationen sollen zur Aufklärung anderer Katalogtaten und zur Abwehr von im Einzelfall bestehenden Gefahren für hochrangige Rechtsgüter nutzbar gemacht werden. Der Gesetzgeber ist auch der Anforderung nachgekommen, die Zwecke, zu denen die personenbezogenen Daten verwendet werden dürfen, bereichsspezifisch und präzise festzulegen (vgl. BVerfGE 100, 313 [389]). Die Norm knüpft an die Aufgaben der Daten empfangenden Behörden zur Strafverfolgung und Gefahrenabwehr an und grenzt die Verwendungszwecke auf die Verfolgung der in dem Katalog genannten Straftaten und die Abwehr besonderer Gefahren ein.BVerfGE 109, 279 (376)

337

BVerfGE 109, 279 (377)bb) Die Zwecke sind darüber hinaus mit dem ursprünglichen Zweck, der die Durchführung der akustischen Wohnraumüberwachung rechtfertigt, vereinbar. Eine Unvereinbarkeit läge vor, wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen (vgl. BVerfGE 100, 313 [389 f.]). Das ist mit Blick auf die angegriffenen Vorschriften jedoch nicht der Fall.

338

(1) Der Gesetzgeber hat die Verwendung von Informationen auch in anderen Strafverfahren gemäß § 100 d Abs. 5 Satz 2 StPO nur zur Aufklärung einer in § 100 c Abs. 1 Nr. 3 StPO aufgezählten Straftat zugelassen. Die durch eine akustische Wohnraumüberwachung erhobenen Daten dürfen nur verwendet werden, wenn die Straftaten aus diesem Katalog abstrakt und im konkreten Fall besonders schwer sind (siehe zur besonders schweren Straftat oben C II 3 b dd [1]). Diese Beschränkung gilt nicht nur für die Verwendung zu Beweiszwecken im engeren Sinne, sondern ist darüber hinaus auch bei der Verwendung von Spurenansätzen für die Aufklärung von Straftaten zu beachten. Anderenfalls könnten in einem Folgeverfahren Informationen aus einer akustischen Wohnraumüberwachung verwendet werden, ohne dass in diesem Verfahren jemals der Verdacht einer Katalogtat bestanden hat. Die für die Erhebung der Informationen bestehenden strengen Voraussetzungen sind in gleicher Weise bei der Verwendung in anderen Verfahren zu beachten.

339

Eine Verwertung aus der Wohnraumüberwachung gewonnener Erkenntnisse setzt voraus, dass die Erkenntnisse eine konkretisierte Verdachtslage begründen. Eine Verwendung von Daten in anderen Zusammenhängen ist nicht zu rechtfertigen, wenn die gewonnenen Erkenntnisse nicht den Grad an Tatverdacht stützen, der ansonsten als Grundlage der Durchführung einer akustischen Wohnraumüberwachung zu verlangen ist (vgl. BVerfGE 100, 313 [394]). Auch die Subsidiaritätsklausel des § 100 c Abs. 1 Nr. 3 StPO ist im Rahmen der Verwertung nach § 100 d Abs. 5 Satz 2 StPO entsprechend zu beachten. Eine Verwertung ist nur dann möglich, wenn die Aufklärung des Sachverhalts in dem anderen Strafverfahren ohne denBVerfGE 109, 279 (377) BVerfGE 109, 279 (378)Fund unmöglich oder unverhältnismäßig erschwert wäre. Hierbei stellt die Verhältnismäßigkeit an die Erschwernis aber geringere Anforderungen, weil die belastende Information als sicher feststeht, die Unsicherheit der Prognose damit entfällt und eine alternative Beweiserhebung ebenfalls in die Grundrechte des Betroffenen eingreifen würde.

340

Dürfen die erhobenen Erkenntnisse bereits im Anlassverfahren nicht verwertet werden, gilt dies erst recht für die Verwertung in anderen Verfahren, da § 100 d Abs. 5 Satz 2 StPO als reine Verwertungsvorschrift eine ordnungsgemäße Erhebung der Informationen voraussetzt. Gesetzliche und verfassungsunmittelbare Verwertungsverbote sind bei der Weiterverwendung oder bei der Verwertung von Zufallsfunden ebenso zu beachten wie im Anlassverfahren selbst (vgl. Rudolphi/Wolter, a.a.O., § 100 f Rn. 6 und 7, Stand: Oktober 2000).

341

(2) Auch bei einer Übermittlung von strafprozessual gewonnenen Informationen an Polizeibehörden zur Gefahrenabwehr nach § 100 f Abs. 1 2. Alt. StPO haben sich die Voraussetzungen für die Zweckänderung an entsprechenden Grundsätzen zu orientieren. Da die Daten durch einen schwerwiegenden Grundrechtseingriff erlangt worden sind, wäre es verfassungsrechtlich nicht zu rechtfertigen, die Übermittlungsschwelle unter diejenige abzusenken, die im Rahmen der Gefahrenabwehr für entsprechende Eingriffe in das Grundrecht der Unverletzlichkeit der Wohnung gilt (vgl. BVerfGE 100, 313 [394]). Eine gesetzliche Regelung für die Übermittlung nach § 100 c Abs. 1 Nr. 3 StPO erhobener Daten an Behörden zu präventiv-polizeilichen Zwecken hat daher die ver-

fassungsrechtlichen Wertungen zu berücksichtigen, die in Art. 13 Abs. 4 GG für den Primäreingriff getroffen worden sind.

342

Nach dieser Maßgabe ist § 100 f Abs. 1 2. Alt. StPO verfassungsrechtlich nicht zu beanstanden. Die Vorschrift stellt hinsichtlich der Gefahrenintensität und des Ranges der Schutzgüter Anforderungen, die den nach Art. 13 Abs. 4 GG bestehenden Voraussetzungen für eine präventiv-polizeiliche Wohnraumüberwachung vergleichbar sind.

343

Mit den Tatbestandsmerkmalen "Abwehr" und "im Einzelfall"BVerfGE 109, 279 (378) BVerfGE 109, 279 (379)stellt § 100 f Abs. 1 StPO klar, dass eine Übermittlung nur bei konkreten Gefahren im polizeirechtlichen Sinne in Betracht kommt. Im Unterschied zu Art. 13 Abs. 4 GG verlangt § 100 f Abs. 1 StPO für die Übermittlung der Information zwar ausdrücklich keine dringende Gefahr. Dass die Gefahr gleichwohl dringend sein muss, folgt aber in verfassungskonformer Auslegung des § 100 f Abs. 1 StPO aus Art. 13 Abs. 4 GG.

344

§ 100 f Abs. 1 StPO setzt im Übrigen durch den Verweis auf die Tatbestandsmerkmale Leben, Leib oder Freiheit einer Person Gefahren für Rechtsgüter voraus, die hinreichend gewichtig sind, um den Einsatz technischer Mittel zur Überwachung von Wohnungen nach Art. 13 Abs. 4 GG zu rechtfertigen. Eine einfache Körperverletzung (§ 223 StGB) erfüllt diese Voraussetzungen nicht. Soweit § 100 f Abs. 1 StPO für die polizeiliche Verwendung der Erkenntnisse eine Gefahr für erhebliche Sach- und Vermögenswerte genügen lässt, ist unter Berücksichtigung der Vorgaben des Art. 13 Abs. 4 GG Voraussetzung, dass das für eine gemeine Gefahr typische Gefahrenpotential gegeben ist. Nur dann hat die Gefährdung von Sach- und Vermögenswerten ein Gewicht, das der vom verfassungsändernden Gesetzgeber angestrebten Wertigkeit der bedrohten Rechtsgüter in Art. 13 Abs. 4 GG entspricht.

345

3. Die Vorschriften über die weitere Verwendung der erhobenen Daten sind jedoch insoweit nicht mit Art. 13 Abs. 1 sowie Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu vereinbaren, als es der Gesetzgeber versäumt hat, eine Pflicht zur Kennzeichnung der aus der akustischen Wohnraumüberwachung stammenden Daten vorzusehen.

346

Die Zweckbindung lässt sich nur gewährleisten, wenn auch nach der Informationserhebung erkennbar bleibt, dass es sich um Daten handelt, die durch eine Maßnahme der akustischen Wohnraumüberwachung gewonnen worden sind. Eine entsprechende Kennzeichnung der Daten ist daher von Verfassungs wegen geboten (vgl. BVerfGE 100, 313 [360 f.] zu Art. 10 GG). Der Gesetzgeber hat sowohl den datenerhebenden als auch den datenempfangenden Behörden zur Sicherung der Zweckbindung eine Kennzeichnungspflicht aufzuerlegen. Sonst könnten die aus der akustischen WohnBVerfGE 109, 279 (379)BVerfGE 109, 279 (380)raumüberwachung stammenden Daten in einer Weise gespeichert und mit anderen Daten vermischt werden, die ihre Herkunft nicht mehr erkennen lässt (vgl. BVerfGE 100, 313 [396 f.]). Die in § 100 f Abs. 1 StPO vorgesehenen Verwendungsbeschränkungen wären damit unterlaufen.

347

VIII.

Die Vorschriften über die Datenvernichtung in § 100 d Abs. 4 Satz 3, § 100 b Abs. 6 StPO, die ebenso wie die Vorschriften zur Weitergabe von Daten in einem verfassungsrechtlich erheblichen Regelungszusammenhang zu den Vorschriften über die Datenerhebung stehen, verstoßen gegen Art. 19 Abs. 4 GG. Die Regelungen zur Datenvernichtung sind ungeachtet der Versäumung der Rügefrist aus den gleichen Gründen in die verfassungsrechtliche Prüfung einzubeziehen wie die zur Datenverwendung (siehe oben C VII).

348

Der sich auch auf die weiteren Phasen der Datenverarbeitung erstreckende Schutz des Art. 13 Abs. 1 GG verlangt zwar, dass die rechtmäßig erlangten Daten grundsätzlich vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr benötigt werden (vgl. BVerfGE 100, 313 [362] zu Art. 10 GG). Die Regelungen über die Datenvernichtung müssen aber zugleich dem Gebot des effektiven Rechtsschutzes genügen. Insofern kann eine spezifische Konfliktlage dadurch entstehen, dass es einerseits dem Datenschutz entspricht, nicht mehr benötigte Daten zu löschen, und dass andererseits durch die Löschung ein effektiver Rechtsschutz erschwert, wenn nicht gar vereitelt wird, weil eine Nachprüfung des Vorgangs nach Vernichtung der Unterlagen nur noch eingeschränkt möglich ist (vgl. MVVerfG, LKV 2000, S. 345 [354]). Vor diesem Hintergrund muss die Vernichtungspflicht für die Fälle, in denen der Betroffene die gerichtliche Kontrolle staatlicher Informations- und Datenverarbeitungsmaßnahmen anstrebt, mit der Rechtsschutzgarantie so abgestimmt werden, dass der Rechtsschutz nicht unterlaufen oder vereitelt wird (vgl. BVerfGE 100, 313 [364, 400]).

349

Dies kann in der Weise geschehen, dass in Fällen, in denen der Betroffene ein ernsthaftes -- grundsätzlich zu vermutendes -- InteresBVerfGE 109, 279 (380)BVerfGE 109, 279 (381)se an Rechtsschutz oder an der Geltendmachung seines Datenschutzrechts gegenüber der zuständigen Stelle haben kann, die Daten einstweilen nicht gelöscht, wohl aber gesperrt werden und zu keinem anderen Zweck als dem zur Information des Betroffe-

nen und zur gerichtlichen Kontrolle verwendet werden dürfen. Eine Vernichtung kommt erst dann in Betracht, wenn sichergestellt ist, dass die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme nicht oder nicht mehr benötigt werden (vgl. BVerfGE 100, 313 [400]).

350

Solche Vorkehrungen treffen § 100 d Abs. 4 Satz 3 und § 100 b Abs. 6 StPO nicht. § 100 d Abs. 4 Satz 3 StPO verweist auf § 100 b Abs. 6 StPO, der die Datenvernichtung nach erfolgten Telefonüberwachungen regelt. Danach sind die durch die Maßnahme erlangten Unterlagen unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich sind. § 100 d Abs. 4 Satz 3 und § 100 b Abs. 6 StPO lassen eine die Rechtsschutzmöglichkeit sichernde Auslegung nicht zu. Die Vorschriften ordnen vielmehr ohne Einschränkung die Vernichtung der Unterlagen an, sobald diese für die Strafverfolgung nicht mehr erforderlich sind. […]

### 3) BVerfGE 120, 274 – Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme

*a) Sachverhalt*

Gegenstand der Verfassungsbeschwerden sind Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen (im Folgenden: NWVerfSchG), die zum einen Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen insbesondere aus informationstechnischen Systemen, zum anderen den Umgang mit den erhobenen Daten regeln. Die angegriffenen Vorschriften wurden überwiegend durch das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. 12. 2006 (NWGVBl, S. 620) eingefügt oder geändert.

Die Bf. zu 1a (1 BvR 370/07) ist Journalistin und schreibt vor allem für eine Online-Publikation. Im Rahmen ihrer beruflichen Tätigkeit besucht sie auch Internet-Präsenzen, die von verfassungsfeindlichen Personen und Organisationen betrieben werden. Sie engagiert sich darüber hinaus in datenschutzrechtlichen Angelegenheiten und betreibt zusammen mit anderen die Homepage www.stop1984.com. Im Zusammenhang mit dieser Homepage besteht die Möglichkeit, an so genannten Chats teilzunehmen. Diese Möglichkeit wird auch von Rechtsextremisten genutzt. Informationen über diese Personen speichert die Bf. zu 1a auf der Festplatte ihres privat wie beruflich genutzten Computers.

Der Bf. zu 1b (1 BvR 370/07) ist aktives Mitglied des Landesverbandes Nordrhein-Westfalen der Partei DIE LINKE, die vom nordrhein-westfälischen Verfassungsschutz beobachtet wird. Für seine politische Tätigkeit nutzt er auch seinen an das Internet angeschlossenen Computer. Wie die Bf. zu 1a greift er daneben auf das Internet zur privaten Kommunikation sowie zur Abwicklung von Zahlungsvorgängen über sein Girokonto zu.

Die Bf. zu 2a und 2b (1 BvR 595/07) sind Sozien einer Rechtsanwaltskanzlei. Der Bf. zu 2a betreut als Rechtsanwalt unter anderem Asylbewerber. Unter ihnen befand sich ein führendes Mitglied der kurdischen Arbeiterpartei PKK, die unter der Beobachtung der nordrhein-westfälischen Verfassungsschutzbehörde steht. Er nutzt sowohl in seiner Wohnung als auch in den Kanzleiräumen Computernetzwerke, die mit dem Internet verbunden sind. Das Kanzleinetzwerk wird auch von dem Bf. zu 2b sowie von dem Bf. zu 2c, der in der Kanzlei als freier Mitarbeiter beschäftigt ist, genutzt.

Beide Verfassungsbeschwerden rügen die Verfassungswidrigkeit von § 5 II Nr. 11 NWVerfSchG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde zu zwei Arten von Ermittlungsmaßnahmen: zum einen zum heimlichen Beobachten und sonstigen Aufklären des Internet (Alt. 1), zum anderen zum heimlichen Zugriff auf informationstechnische Systeme (Alt. 2). Nur die Bf. zu 2 wenden sich im Zusammenhang mit Maßnahmen nach § 5 II 2 Nr. 11 NWVerfSchG auch gegen § 17 NWVerfSchG, der die Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörde regelt. Beide Verfassungsbeschwerden richten sich weiter gegen § 5 III NWVerfSchG. Diese Vorschrift hat die Benachrichtigung des Betroffenen nach einem Einsatz der in § 5 II NWVerfSchG geregelten nachrichtendienstlichen Mittel zum Gegenstand. Sie enthält in Satz 1 eine grundsätzliche Pflicht zur Benachrichtigung, von der Satz 2 mehrere Ausnahmen vorsieht. Nur die Bf. zu 1 wenden sich gegen § 5a I NWVerfSchG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde dazu, bei Kreditinstituten Auskünfte über Beteiligte am Zahlungsverkehr und über Geldbewegungen und Geldanlagen einzuholen. Voraussetzung ist, dass tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die Schutzgüter des Verfassungsschutzes bestehen. Ebenfalls nur die Bf. zu 1 rügen die Verfassungswidrigkeit von § 13 NWVerfSchG. Diese Norm ermächtigt die Verfassungsschutzbehörde, ihre Erkenntnisse in gemeinsamen Dateien mit anderen Sicherheitsbehörden zu verarbeiten. Wegen Anlass, Umfang und weiteren Anforderungen an die Dateiführung verweist die Norm auf sonstiges Bundes- oder Landesrecht. Dieses sonstige Recht haben die Bf. zu 1 allerdings nicht zum Gegenstand ihrer Verfassungsbeschwerde gemacht. Ausschließlich die Bf. zu 2 wenden sich gegen § 7 II NWVerfSchG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde zur akustischen und optischen Überwachung von Wohnungen. Sie stammt aus dem Jahr 1994 und wurde im Rahmen der Novellierung des Verfassungsschutzgesetzes nicht verändert. Eine Überarbeitung oder Streichung der Norm wurde zwar erwogen, letztlich aber zurückgestellt (vgl. LT-Dr 14/2211, S. 16). Schließlich greifen wiederum nur die Bf. zu 2 die in § 8 IV 2 i.V. mit §§ 10, 11 NWVerfSchG enthaltenen Regelungen über die Führung so genannter elektronischer Sachakten an. Diese Vorschriften sehen in ihrer Zusammenschau vor, dass personenbezogene Daten, die in sol-

chen Sachakten enthalten sind, auch dann gespeichert bleiben dürfen, wenn an der betroffenen Person selbst kein Ermittlungsinteresse der Verfassungsschutzbehörde mehr besteht. Damit soll die für eine elektronische Dokumentenverwaltung erforderliche Vollständigkeit der elektronisch geführten Sachakte gesichert werden. Die Belange des Datenschutzes werden dadurch berücksichtigt, dass die betroffenen personenbezogenen Daten nicht mehr recherchierbar sein und auch nicht uneingeschränkt verwendet werden dürfen.
(Zusammenfassung nach NJW 2008, 822, beck-online)

*b) Leitsätze*

**1.** Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.
**2.** Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.
**3.** Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.
**4.** Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.
**5.** Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist.
**6.** Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.
(Bearbeitung, zuletzt am 13. Sep. 2017, durch: Dominika Blonski, http://www.servat.unibe.ch/dfr/bv120274.html )

*c) Begründung*

Die Verfassungsbeschwerden sind, soweit zulässig, weitgehend begründet. § 5 Abs. 2 Nr. 11 VSG ist in der zweiten dort aufgeführten Alternative verfassungswidrig und nichtig (I). Gleiches gilt für die erste Alternative dieser Norm (II). In der Folge der Nichtigkeit erledigen sich die gegen § 5 Abs. 3 und § 17 VSG gerichteten Rügen (III). Gegen § 5a Abs. 1 VSG bestehen hingegen keine verfassungsrechtlichen Bedenken (IV). […]
I.
§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

166

Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (1). Vorliegend sind die Eingriffe verfassungsrechtlich nicht gerechtfertigt: § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt nicht dem Gebot der Normenklarheit (2 a), die Anforderungen des Verhältnismäßigkeitsgrundsatzes sind nicht gewahrt (2 b) und die Norm enthält keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (2 c). Die angegriffene Norm ist nichtig (2 d).BVerfGE 120, 274 (302) BVerfGE 120, 274 (303)Einer zusätzlichen Prüfung anhand anderer Grundrechte bedarf es nicht (2 e).

167

1. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; sie tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.

168

a) Das allgemeine Persönlichkeitsrecht gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen (vgl. BVerfGE 99, 185 [193]; 114, 339 [346]). Einer solchen lückenschließen-

den Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann (vgl. BVerfGE 54, 148 [153]; 65, 1 [41]; 118, 168 [183]). Die Zuordnung eines konkreten Rechtsschutzbegehrens zu den verschiedenen Aspekten des Persönlichkeitsrechts richtet sich vor allem nach der Art der Persönlichkeitsgefährdung (vgl. BVerfGE 101, 361 [380]; 106, 28 [39]).

169

b) Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.

170

aa) Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.

171

Dies gilt zunächst für Personalcomputer, über die mittlerweile eine deutliche Mehrheit der Haushalte in der Bundesrepublik verfügt (vgl. Statistisches Bundesamt, Statistisches Jahrbuch 2007, S. 113). Die Leistungsfähigkeit derartiger Rechner ist ebenso geBVerfGE 120, 274 (303)BVerfGE 120, 274 (304)stiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen.

172

Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind.

173

bb) Der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Dies wird insbesondere aufgrund der gestiegenen Nutzung des Internet durch große Kreise der Bevölkerung mehr und mehr zum Normalfall.

174

Eine Vernetzung informationstechnischer Systeme ermöglicht allgemein, Aufgaben auf diese Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen. So können etwa die von einzelnen der vernetzten Systeme gelieferten Daten ausgewertet und die Systeme zu bestimmten Reaktionen veranlasst werden. Auf diese Weise kann zugleich der Funktionsumfang des einzelnen Systems erweitert werden.

175

Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Rechners nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er aktiv soziale Verbindungen aufbauen und pflegen kann. Zudem führen techBVerfGE 120, 274 (304)BVerfGE 120, 274 (305)nische Konvergenzeffekte dazu, dass auch herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können (vgl. etwa zur Sprachtelefonie Katko, CR 2005, S. 189).

176

cc) Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.

177

(1) Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (vgl. zu den aus solchen Folgerungen entstehenden Persönlichkeitsgefährdungen BVerfGE 65, 1 [42]).

178

(2) Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der

Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten derBVerfGE 120, 274 (305) BVerfGE 120, 274 (306)Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.

179

Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten -- etwa die Verschlüsselung oder die Verschleierung sensibler Daten -- werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.

180

c) Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.

181

aa) Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche ÜbermittlungBVerfGE 120, 274 (306) BVerfGE 120, 274 (307)von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 [172]; 106, 28 [35 f.]), nicht aber auch die Vertraulichkeit und Integrität von informationstechnischen Systemen.

182

(1) Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden (vgl. BVerfGE 106, 28 [36]; 115, 166 [182]). Der Schutzbereich des Telekommunikationsgeheimnisses erstreckt sich danach auch auf die Kommunikationsdienste des Internet (vgl. zu E-Mails BVerfGE 113, 348 [383]). Zudem sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 [172]; 85, 386 [396]; 100, 313 [358]; 107, 299 [312 f.]). Das Telekommunikationsgeheimnis begegnet in diesem Rahmen alten sowie neuen Persönlichkeitsgefährdungen, die sich aus der gestiegenen Bedeutung der Informationstechnik für die Entfaltung des Einzelnen ergeben.

183

Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt (vgl. BVerfGE 106, 28 [37 f.]; 115, 166 [186 f.]). Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt.

184

(2) Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich allerdings nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines KommunikationsteilnehBVerfGE 120, 274 (307)BVerfGE 120, 274 (308)mers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort (vgl. BVerfGE 115, 166 [183 ff.]).

185

(3) Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem

Online-Zugriff auf gespeicherte Daten der Fall ist (vgl. Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 497; Rux, JZ 2007, S. 285 [292]).

186

(4) Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist.

187

Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert ("Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbeBVerfGE 120, 274 (308)BVerfGE 120, 274 (309)sondere auch der Inhalt angelegter Dateien oder -- soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert -- das Verhalten in der eigenen Wohnung.

188

Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen -- anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung -- stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden.

189

Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.

190

bb) Auch die durch Art. 13 Abs. 1 GG gewährleistete Garantie der Unverletzlichkeit der Wohnung verbürgt dem Einzelnen mit Blick auf seine Menschenwürde sowie im Interesse der Entfaltung seiner Persönlichkeit einen elementaren Lebensraum, in den nur unter den besonderen Voraussetzungen von Art. 13 Abs. 2 bis 7 GG eingegriffen werden darf, belässt aber Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme.

191

Das Schutzgut dieses Grundrechts ist die räumliche Sphäre, in der sich das Privatleben entfaltet (vgl. BVerfGE 89, 1 [12]; 103, 142 [150 f.]). Neben Privatwohnungen fallen auch Betriebs- und Geschäftsräume in den Schutzbereich des Art. 13 GG (vgl. BVerfGE 32, 54 [69 ff.]; 44, 353 [371]; 76, 83 [88]; 96, 44 [51]). Dabei erschöpft sich der Grundrechtsschutz nicht in der Abwehr eines körperlichen Eindringens in die Wohnung. Als Eingriff in Art. 13 GG sind auch Maßnahmen anzusehen, durch die staatlicheBVerfGE 120, 274 (309) BVerfGE 120, 274 (310)Stellen sich mit besonderen Hilfsmitteln einen Einblick in Vorgänge innerhalb der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind. Dazu gehören nicht nur die akustische oder optische Wohnraumüberwachung (vgl. BVerfGE 109, 279 [309, 327]), sondern ebenfalls etwa die Messung elektromagnetischer Abstrahlungen, mit der die Nutzung eines informationstechnischen Systems in der Wohnung überwacht werden kann. Das kann auch ein System betreffen, das offline arbeitet.

192

Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden.

193

Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet (vgl. etwa Beulke/Meininghaus, StV 2007, S. 63 [64]; Gercke, CR 2007, S. 245 [250]; Schlegel, GA 2007, S. 648 [654 ff.]; a. A. etwa Buermeyer, HRRS 2007, S. 392 [395 ff.]; Rux, JZ 2007, S. 285 [292 ff.]; Schaar/Landwehr, K&R 2007, S. 202 [204]). Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechni-

schen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. DerBVerfGE 120, 274 (310) BVerfGE 120, 274 (311)Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone.

194

Art. 13 Abs. 1 GG schützt zudem nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht (vgl. zum gleichläufigen Verhältnis von Wohnungsdurchsuchung und Beschlagnahme BVerfGE 113, 29 [45]).

195

cc) Auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistungen des Schutzes der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, genügen dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht in ausreichendem Maße.

196

(1) In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll (vgl. BVerfGE 27, 344 [350 ff.]; 44, 353 [372 f.]; 90, 255 [260]; 101, 361 [382 f.]). Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.

197

(2) Das Recht auf informationelle Selbstbestimmung geht überBVerfGE 120, 274 (311) BVerfGE 120, 274 (312)den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1 [43]; 84, 192 [194]). Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann. Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommenen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben (vgl. BVerfGE 118, 168 [184 f.]).

198

Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Oktober 2006 -- 1 BvR 2027/02 --, JZ 2007, S. 576) zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können (vgl. BVerfGE 65, 1 [42]; 113, 29 [45 f.]; 115, 320 [342]; 118, 168 [184 f.]).

199

Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner persönlichBVerfGE 120, 274 (312)BVerfGE 120, 274 (313)keitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.

200

d) Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist,

trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

201

aa) Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält -- zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik --, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle SelbstbeBVerfGE 120, 274 (313)BVerfGE 120, 274 (314)stimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren.

202

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

203

bb) Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

204

(1) Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der GrundrechtsBVerfGE 120, 274 (314)BVerfGE 120, 274 (315)schutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur.

205

(2) Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.

206

2. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Hinsichtlich der vorliegend zu überprüfenden Ermächtigung der Verfassungsschutzbehörde, präventive Maßnahmen vorzunehmen, fehlt es daran.

207

a) Die angegriffene Norm wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht.

208

aa) Das Bestimmtheitsgebot findet auch im Hinblick auf das allgemeine Persönlichkeitsrecht in seinen verschiedenen Ausprägungen seine Grundlage im Rechtsstaatsprinzip (Art. 20, Art. 28BVerfGE 120, 274 (315) BVerfGE 120, 274 (316)Abs. 1 GG; vgl. BVerfGE 110, 33 [53, 57, 70]; 112, 284 [301]; 113, 348 [375]; 115, 320 [365]). Es soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann (vgl. BVerfGE 110, 33 [52 ff.]; 113, 348 [375 ff.]). Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 100, 313 [359 f., 372]; 110, 33 [53]; 113, 348 [375]; 118, 168 [186 ff.]).

209

Je nach der zu erfüllenden Aufgabe findet der Gesetzgeber unterschiedliche Möglichkeiten zur Regelung der Eingriffsvoraussetzungen vor. Die Anforderungen des Bestimmtheitsgrundsatzes richten sich auch nach diesen Regelungsmöglichkeiten (vgl. BVerfGE 110, 33 [55 f.]; 118, 168, [188]). Bedient sich der Gesetzgeber unbestimmter Rechtsbegriffe, dürfen verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justitiabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind (vgl. BVerfGE 21, 73 [79 f.]; 31, 255 [264]; 83, 130 [145]; 102, 254 [337]; 110, 33 [56 f.]; 118, 168 [188]).

210

bb) Nach diesen Maßstäben genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG dem Gebot der Normenklarheit und Normenbestimmtheit insoweit nicht, als sich die tatbestandlichen Voraussetzungen der geregelten Maßnahmen dem Gesetz nicht hinreichend entnehmen lassen.

211

(1) Die Voraussetzungen für Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG können über zwei Normverweisungen zu bestimmen sein. Zum einen verweist § 5 Abs. 2 VSG allgemein auf § 7 Abs. 1 VSG, der seinerseits § 3 Abs. 1 VSG in Bezug nimmt. Danach ist ein Einsatz nachrichtendienstlicher Mittel zulässig, wenn auf diese Weise verfassungsschutzrelevante ErkenntnisseBVerfGE 120, 274 (316) BVerfGE 120, 274 (317)gewonnen werden können. Zum anderen verweist § 5 Abs. 2 Nr. 11 Satz 2 VSG für den Fall, dass eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG in das Brief-, Post- oder Fernmeldegeheimnis eingreift oder einem solchen Eingriff nach Art und Schwere gleichkommt, auf die strengeren Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz.

212

(2) Mit dem Gebot der Normenklarheit und Normenbestimmtheit ist nicht vereinbar, dass § 5 Abs. 2 Nr. 11 Satz 2 VSG für die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz darauf abstellt, ob eine Maßnahme in Art. 10 GG eingreift. Die Antwort auf die Frage, in welche Grundrechte Ermittlungsmaßnahmen der Verfassungsschutzbehörde eingreifen, kann komplexe Abschätzungen und Bewertungen erfordern. Zu ihnen ist zunächst und vorrangig der Gesetzgeber berufen. Seiner Aufgabe, die einschlägigen Grundrechte durch entsprechende gesetzliche Vorkehrungen zu konkretisieren, kann er sich nicht entziehen, indem er durch eine bloße tatbestandliche Bezugnahme auf ein möglicherweise einschlägiges Grundrecht die Entscheidung darüber, wie dieses Grundrecht auszufüllen und umzusetzen ist, an die normvollziehende Verwaltung weiterreicht. Eine derartige "salvatorische" Regelungstechnik genügt dem Bestimmtheitsgebot nicht bei einer Norm wie § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, die neuartige Ermittlungsmaßnahmen vorsieht, welche auf neuere technologische Entwicklungen reagieren sollen.

213

Der Verstoß gegen das Gebot der Normenklarheit wird noch vertieft durch den in § 5 Abs. 2 Nr. 11 Satz 2 VSG enthaltenen Zusatz, die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz greife auch dann, wenn eine Ermittlungsmaßnahme einem Eingriff in Art. 10 GG "in Art und Schwere" gleichkommt. Damit werden die tatbestandlichen Voraussetzungen des geregelten Zugriffs von einem wertenden Vergleich zwischen diesem Zugriff und einer Maßnahme, die als Eingriff in ein bestimmtes Grundrecht anzusehen wäre, abhängig gemacht. Für diesen Vergleich enthält § 5 Abs. 2 Nr. 11 Satz 2 VSG keinerlei Maßstäbe. Wenn schon durch die bloße Verweisung auf ein bestimmtes Grundrecht die Tatbestandsvoraussetzungen nicht hinreichend bestimmt geBVerfGE 120, 274 (317)BVerfGE 120, 274 (318)regelt werden können, so gilt dies erst recht für eine Norm, die einen derartigen, normativ nicht weiter angeleiteten Vergleich der geregelten Maßnahme mit einem Eingriff in ein bestimmtes Grundrecht vorsieht.

214

(3) Die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz in § 5 Abs. 2 Nr. 11 Satz 2 VSG genügt dem Gebot der Normenklarheit und Normenbestimmtheit auch insoweit nicht, als die Reichweite der Verweisung nicht hinreichend bestimmt geregelt ist.

215

§ 5 Abs. 2 Nr. 11 Satz 2 VSG verweist auf die "Voraussetzungen" des Gesetzes zu Artikel 10 Grundgesetz. Die Norm lässt damit weitgehend im Unklaren, auf welche Teile des Gesetzes zu Artikel 10 Grundgesetz verwiesen

werden soll. Ihr lässt sich nicht entnehmen, ob unter den Voraussetzungen dieses Gesetzes nur die in § 3 G 10 geregelte materielle Eingriffsschwelle zu verstehen ist oder ob auch weitere Vorschriften in Bezug genommen werden sollen. So könnten auch die Verfahrensregelungen der §§ 9 ff. G 10 zu den Voraussetzungen eines Eingriffs nach diesem Gesetz gezählt werden. Zumindest denkbar wäre sogar, die Verweisung noch weitergehend auf sowohl die materiellen Eingriffsschwellen als auch sämtliche Verfahrensvorkehrungen des Gesetzes zu Artikel 10 Grundgesetz zu beziehen, wie dies die nordrhein-westfälische Landesregierung vorschlägt. Danach wären auch die in § 4 G 10 enthaltenen Regelungen über den Umgang mit erhobenen Daten und die Normen der §§ 14 ff. G 10 über die parlamentarische Kontrolle erfasst, obwohl diese Normen Regelungen enthalten, die erst nach einem Eingriff zu beachten sind und daher sprachlich kaum zu den Eingriffsvoraussetzungen gezählt werden können.

216

Es ist nicht ersichtlich, dass die unbestimmte Fassung des Gesetzes besonderen Regelungsschwierigkeiten geschuldet wäre. Dem Gesetzgeber wäre ohne weiteres möglich gewesen, in der Verweisungsnorm einzelne Vorschriften des Gesetzes zu Artikel 10 Grundgesetz aufzuzählen, auf die verwiesen werden soll.

217

b) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt auch nicht den Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als MittelBVerfGE 120, 274 (318) BVerfGE 120, 274 (319)zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl. BVerfGE 109, 279 [335 ff.]; 115, 320 [345]; 118, 168 [193]).

218

aa) Die in der angegriffenen Norm vorgesehenen Datenerhebungen dienen der Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben nach § 3 Abs. 1 VSG und damit der im Vorfeld konkreter Gefahren einsetzenden Sicherung der freiheitlichen demokratischen Grundordnung, des Bestandes von Bund und Ländern sowie bestimmter auf das Verhältnis zum Ausland gerichteter Interessen der Bundesrepublik. Dabei wurde mit der Novellierung des Verfassungsschutzgesetzes nach der Gesetzesbegründung insbesondere auch das Ziel verfolgt, eine effektive Terrorismusbekämpfung durch die Verfassungsschutzbehörde angesichts neuer, insbesondere mit der Internetkommunikation verbundener, Gefährdungen sicherzustellen (vgl. LTDrucks 14/2211, S. 1). Allerdings ist der Anwendungsbereich der Neuregelung weder ausdrücklich noch als Folge des systematischen Zusammenhangs auf die Terrorismusbekämpfung begrenzt. Die Norm bedarf einer Rechtfertigung für ihr gesamtes Anwendungsfeld.

219

Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen (vgl. BVerfGE 49, 24 [56 f.]; 115, 320 [346]). Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG (vgl. BVerfGE 115, 118 [152]). Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erBVerfGE 120, 274 (319)BVerfGE 120, 274 (320)schließen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen (vgl. zur Strafverfolgung BVerfGE 115, 166 [193]).

220

bb) Der heimliche Zugriff auf informationstechnische Systeme ist geeignet, diesen Zielen zu dienen. Mit ihm werden die Möglichkeiten der Verfassungsschutzbehörde zur Aufklärung von Bedrohungslagen erweitert. Bei der Beurteilung der Eignung ist dem Gesetzgeber ein beträchtlicher Einschätzungsspielraum eingeräumt (vgl. BVerfGE 77, 84 [106]; 90, 145 [173]; 109, 279 [336]). Es ist nicht ersichtlich, dass dieser Spielraum hier überschritten wurde.

221

Die in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG enthaltene Befugnis verliert nicht dadurch ihre Eignung, dass der Betroffene nach einer in der Literatur vertretenen (vgl. etwa Buermeyer, HRRS 2007, S. 154 [165 f.]; Gercke, CR 2007, S. 245 [253]; Hornung, DuD 2007, S. 575 [579]) und von den in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen geteilten Einschätzung technische Selbstschutzmöglichkeiten hat, um jedenfalls einen Zugriff wirkungsvoll zu verhindern, bei dem die Infiltration des Zielsystems mit Hilfe einer Zugriffssoftware durchgeführt wird. Im Rahmen der Eignungsprüfung ist nicht zu fordern, dass Maßnahmen, welche die angegriffene Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen. Die gesetzgeberische Prognose, dass Zugriffe der geregelten Art im Einzelfall Erfolg haben können, ist zumindest nicht offensichtlich fehlsam. Es kann nicht als selbstverständlich unterstellt werden, dass jede mögliche Zielperson eines Zugriffs bestehende Schutzmöglichkeiten dagegen nutzt und tatsächlich fehlerfrei implementiert. Im Übrigen erscheint

denkbar, dass sich im Zuge der weiteren informationstechnischen Entwicklung für die Verfassungsschutzbehörde Zugriffsmöglichkeiten auftun, die sich technisch nicht mehr oder doch nur mit unverhältnismäßigem Aufwand unterbinden lassen.

222

Weiter ist die Eignung der geregelten Befugnis auch nicht deshalb zu verneinen, weil möglicherweise der Beweiswert der ErBVerfGE 120, 274 (320)BVerfGE 120, 274 (321)kenntnisse, die mittels des Zugriffs gewonnen werden, begrenzt ist. Insoweit wird vorgebracht, eine technische Echtheitsbestätigung der erhobenen Daten setze grundsätzlich eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus (vgl. Hansen/Pfitzmann, DRiZ 2007, S. 225 [228]). Jedoch bewirken diese Schwierigkeiten der Beweissicherung nicht, dass den erhobenen Daten kein Informationswert zukommt. Zudem dient der Online-Zugriff nach der angegriffenen Norm nicht unmittelbar der Gewinnung revisionsfester Beweise für ein Strafverfahren, sondern soll der Verfassungsschutzbehörde Kenntnisse verschaffen, an deren Zuverlässigkeit wegen der andersartigen Aufgabenstellung des Verfassungsschutzes zur Prävention im Vorfeld konkreter Gefahren geringere Anforderungen zu stellen sind als in einem Strafverfahren.

223

cc) Der heimliche Zugriff auf informationstechnische Systeme verletzt auch den Grundsatz der Erforderlichkeit nicht. Im Rahmen seiner Einschätzungsprärogative durfte der Gesetzgeber annehmen, dass kein ebenso wirksamer, aber den Betroffenen weniger belastender Weg gegeben ist, die auf solchen Systemen vorhandenen Daten zu erheben.

224

Grundsätzlich ist zwar eine -- im Verfassungsschutzgesetz nicht vorgesehene -- offene Durchsuchung des Zielsystems gegenüber dem heimlichen Zugriff als milderes Mittel anzusehen (vgl. Hornung, DuD 2007, S. 575 [580]). Hat die Verfassungsschutzbehörde jedoch im Rahmen ihrer Aufgabenstellung einen hinreichenden Grund, die auf den Speichermedien eines informationstechnischen Systems abgelegten Dateien umfassend -- unter Einschluss verschlüsselter Daten -- zu sichten, über einen längeren Zeitraum Änderungen zu verfolgen oder die Nutzung des Systems umfassend zu überwachen, so sind mildere Mittel, diese Erkenntnisziele zu erreichen, nicht ersichtlich. Gleiches gilt für den Zugriff auf verschlüsselte Inhalte der Internetkommunikation, soweit ein Zugriff auf der Übertragungsstrecke nicht erfolgversprechend ist.

225

dd) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt jedoch nicht das Gebot der Verhältnismäßigkeit im engeren Sinne.

226

Dieses Gebot verlangt, dass die Schwere des Eingriffs bei einerBVerfGE 120, 274 (321) BVerfGE 120, 274 (322)Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (vgl. BVerfGE 90, 145 [173]; 109, 279 [349 ff.]; 113, 348 [382]; stRspr). Der Gesetzgeber hat das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann dazu führen, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange (vgl. BVerfGE 115, 320 [345 f.]; 118, 168 [195]).

227

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt dem nicht. Die in dieser Norm vorgesehenen Maßnahmen bewirken derart intensive Grundrechtseingriffe, dass sie zu dem öffentlichen Ermittlungsinteresse, das sich aus dem geregelten Eingriffsanlass ergibt, außer Verhältnis stehen. Zudem bedarf es ergänzender verfahrensrechtlicher Vorgaben, um den grundrechtlich geschützten Interessen des Betroffenen Rechnung zu tragen; auch an ihnen fehlt es.

228

(1) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Grundrechtseingriffen von hoher Intensität.

229

(a) Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von Speichermedien solcher Systeme (vgl. zu solchen Fallgestaltungen etwa BVerfGE 113, 29; 115, 166; 117, 244).

230

(aa) Ein solcher heimlicher Zugriff auf ein informationstechnisches System öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Dies liegt an der Vielzahl unterschiedlicher Nutzungsmöglichkeiten, die komplexe informationstechnische Systeme bieten und die mit der Erzeugung, Verarbeitung und Speicherung von personenbezogenen Daten verbunden sind. Insbesondere werden solBVerfGE 120, 274 (322)BVerfGE 120, 274 (323)che Geräte nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebens-

führung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen.

231

Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.

232

(bb) Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die -- auch im Allgemeinwohl liegende -- Möglichkeit der Bürger beschränkt wird, an einer unbeobachteten Fernkommunikation teilzunehmen (vgl. zur Erhebung von Verbindungsdaten BVerfGE 115, 166 [187 ff.]). Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann. Zudem weisen solche Datenerhebungen insoweit eine beträchtliche, das Gewicht des Eingriffs erhöhende Streubreite auf, als mit den Kommunikationspartnern der Zielperson notwendigerweise Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 [382 f.]; ferner BVerfGE 34, 238 [247]; 107, 299 [321]).

233

(b) Das Gewicht des Grundrechtseingriffs ist von besonderer Schwere, wenn -- wie dies die angegriffene Norm vorsieht -- eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.BVerfGE 120, 274 (323)

234

BVerfGE 120, 274 (324)(aa) Umfang und Vielfältigkeit des Datenbestands, der durch einen derartigen Zugriff erlangt werden kann, sind noch erheblich größer als bei einer einmaligen und punktuellen Datenerhebung. Der Zugriff macht auch lediglich im Arbeitsspeicher gehaltene flüchtige oder nur temporär auf den Speichermedien des Zielsystems abgelegte Daten für die Ermittlungsbehörde verfügbar. Er ermöglicht zudem, die gesamte Internetkommunikation des Betroffenen über einen längeren Zeitraum mitzuverfolgen. Im Übrigen kann sich die Streubreite der Ermittlungsmaßnahme erhöhen, wenn das Zielsystem in ein (lokales) Netzwerk eingebunden ist, auf das der Zugriff erstreckt wird.

235

Flüchtige oder nur temporär gespeicherte Daten können eine besondere Relevanz für die Persönlichkeit des Betroffenen aufweisen oder einen Zugriff auf weitere, besonders sensible Daten ermöglichen. Dies gilt etwa für Cache-Speicher, die von Dienstprogrammen wie etwa Web-Browsern angelegt werden und deren Auswertung Schlüsse über die Nutzung solcher Programme und damit mittelbar über Vorlieben oder Kommunikationsgewohnheiten des Betroffenen ermöglichen kann, oder für Passwörter, mit denen der Betroffene Zugang zu technisch gesicherten Inhalten auf seinem System oder im Netz erlangt. Zudem ist eine längerfristige Überwachung der Internetkommunikation, wie sie die angegriffene Norm ermöglicht, gegenüber einer einmaligen Erhebung von Kommunikationsinhalten und Kommunikationsumständen gleichfalls ein erheblich intensiverer Eingriff. Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs.

236

Auch das Risiko einer Bildung von Verhaltens- und Kommunikationsprofilen erhöht sich durch die Möglichkeit, über einen längeren Zeitraum die Nutzung des Zielsystems umfassend zu überwachen. Die Behörde kann auf diese Weise die persönlichenBVerfGE 120, 274 (324) BVerfGE 120, 274 (325)Verhältnisse und das Kommunikationsverhalten des Betroffenen weitgehend ausforschen. Eine solche umfassende Erhebung persönlicher Daten ist als Grundrechtseingriff von besonders hoher Intensität anzusehen.

237

(bb) Die Eingriffsintensität des geregelten Zugriffs wird weiter durch dessen Heimlichkeit bestimmt. In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung (vgl. BVerfGE 118, 168 [197]). Erfährt der Betroffene von einer ihn belastenden staatlichen Maßnahme vor ihrer Durchführung, kann er von vornherein seine Interessen wahrnehmen. Er kann zum einen rechtlich gegen sie vorgehen, etwa gerichtlichen Rechtsschutz in Anspruch nehmen. Zum anderen hat er bei einer offen durchgeführten Datenerhebung faktisch die Möglichkeit, durch sein Verhalten auf den Gang der Ermittlung einzuwirken. Der Ausschluss dieser Einflusschance verstärkt das Gewicht des Grundrechtseingriffs (vgl. zu rechtlichen Abwehrmöglichkeiten BVerfGE 113, 348 [383 f.]; 115, 320 [353]).

238

(cc) Das Gewicht des Eingriffs wird schließlich dadurch geprägt, dass infolge des Zugriffs Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch Dritter begründet werden.

239

Die in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen haben ausgeführt, es könne nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht. So könnten Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen (vgl. auch Hansen/Pfitzmann, DRiZ 2007, S. 225 [228]). Zudem ist zu beachten, dass es einen rein lesenden Zugriff infolge der Infiltration nicht gibt. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können aufgrund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen. Dies kann den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen.

240

Je nach der eingesetzten Infiltrationstechnik kann die InfiltraBVerfGE 120, 274 (325)BVerfGE 120, 274 (326)tion auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.

241

(2) Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.

242

(a) In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte gehört es zur Aufgabe des Gesetzgebers, in abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen (vgl. BVerfGE 109, 279 [350]). Dies kann dazu führen, dass bestimmte intensive Grundrechtseingriffe nur zum Schutz bestimmter Rechtsgüter und erst von bestimmten Verdachts- oder Gefahrenstufen an vorBVerfGE 120, 274 (326)BVerfGE 120, 274 (327)gesehen werden dürfen. In dem Verbot unangemessener Grundrechtseingriffe finden auch die Pflichten des Staates zum Schutz anderer Rechtsgüter ihre Grenze (vgl. BVerfGE 115, 320 [358]). Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten (vgl. BVerfGE 100, 313 [383 f.]; 109, 279 [350 ff.]; 115, 320 [346]).

243

(b) Ein Grundrechtseingriff von hoher Intensität kann bereits als solcher unverhältnismäßig sein, wenn der gesetzlich geregelte Eingriffsanlass kein hinreichendes Gewicht aufweist. Soweit das einschlägige Gesetz der Abwehr bestimmter Gefahren dient, wie sich dies für das Verfassungsschutzgesetz aus § 1 VSG ergibt, kommt es für das Gewicht des Eingriffsanlasses maßgeblich auf den Rang und die Art der Gefährdung der Schutzgüter an, die in der jeweiligen Regelung in Bezug genommen werden (vgl. BVerfGE 115, 320 [360 f.]).

244

Wiegen die Schutzgüter einer Eingriffsermächtigung als solche hinreichend schwer, um Grundrechtseingriffe der geregelten Art zu rechtfertigen, begründet der Verhältnismäßigkeitsgrundsatz verfassungsrechtliche Anforderungen an die tatsächlichen Voraussetzungen des Eingriffs. Der Gesetzgeber hat insoweit die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits zu wahren (vgl. BVerfGE 100, 313 [392 ff.]). Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose müssen in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutsbeeinträchtigung kann auf das Erfordernis einer hinreichenden Eintrittswahrscheinlichkeit nicht verzichtet werden. Auch muss als Voraussetzung eines schweren Grundrechtseingriffs gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen besitzen (vgl. BVerfGE 113, 348 [386]; 115, 320 [360 f.]).

245

(c) Der Verhältnismäßigkeitsgrundsatz setzt einer gesetzlichen Regelung, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, zunächst insoweit Grenzen, als besondereBVerfGE 120, 274 (327) BVerfGE 120, 274 (328)Anforderungen an den Eingriffsanlass bestehen. Dieser besteht hier in der Gefahrenprävention im Rahmen der Aufgaben der Verfassungsschutzbehörde gemäß § 1 VSG.

246

(aa) Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.

247

Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die -- wie hier -- die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.

248

(bb) Die gesetzliche Ermächtigungsgrundlage muss weiter als Voraussetzung des heimlichen Zugriffs vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter der Norm bestehen.

249

α) Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen (vgl. BVerfGE 110, 33 [61]; 113, 348 [378]).

250

Diese Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein. Dies ist eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird. Die konkreteBVerfGE 120, 274 (328) BVerfGE 120, 274 (329)Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. Der hier zu beurteilende Zugriff auf das informationstechnische System kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

251

Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.

252

Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur ein durch relativ diffuse Anhaltspunkte für mögliche Gefahren gekennzeichnetes Geschehen bekannt ist. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. zur Straftatenverhütung BVerfGE 110, 33 [59]).

253

β) Die verfassungsrechtlichen Anforderungen an die Regelung des tatsächlichen Eingriffsanlasses sind im Fall des heimlichen Zugriffs auf ein informationstechnisches System für alle Eingriffsermächtigungen mit präventiver Zielsetzung zu beachten. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die Gleiche ist, besteht hinsichtlich seiner AnfordeBVerfGE 120, 274 (329)BVerfGE 120, 274 (330)rungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang.

254

Zwar können Differenzierungen zwischen den Ermächtigungen der verschiedenen Behörden mit präventiven Aufgaben vor der Verfassung Bestand haben. So rechtfertigen die besonderen Zwecke im Bereich der strategischen Telekommunikationsüberwachung durch den Bundesnachrichtendienst, dass die Eingriffsvoraussetzungen anders bestimmt werden als im Polizei- oder Strafprozessrecht (vgl. BVerfGE 100, 313 [383]). Auch können die Einschreitvoraussetzungen für Ermittlungsmaßnahmen unterschiedlich gestaltet werden, je nachdem welche Behörde mit welcher Zielsetzung handelt. Auf diese Weise kann etwa der besonderen Aufgabenstellung der

Verfassungsschutzbehörden zur Aufklärung verfassungsfeindlicher Bestrebungen im Vorfeld konkreter Gefahren Rechnung getragen werden (vgl. allgemein zum Problem adäquater Ermittlungsregelungen im Vorfeldbereich Möstl, DVBl 2007, S. 581; Volkmann, JZ 2006, S. 918). So ist es grundsätzlich verfassungsrechtlich nicht zu beanstanden, dass die Verfassungsschutzbehörden nachrichtendienstliche Mittel auch einsetzen dürfen, um Erkenntnisse über Gruppierungen zu erlangen, die die Schutzgüter des Verfassungsschutzgesetzes -- zumindest noch -- auf dem Boden der Legalität bekämpfen. Auch ist für den Einsatz solcher Mittel nicht generell zu fordern, dass über die stets erforderlichen tatsächlichen Anhaltspunkte für derartige Bestrebungen (vgl. etwa § 7 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 VSG) hinaus konkrete Verdachtsmomente bestehen.

255

Jedoch ist der Gesetzgeber auch bei der Regelung der einzelnen Befugnisse von Sicherheitsbehörden, deren Aufgabe in der Vorfeldaufklärung besteht, an die verfassungsrechtlichen Vorgaben gebunden, die sich aus dem Verhältnismäßigkeitsgrundsatz ergeBVerfGE 120, 274 (330)BVerfGE 120, 274 (331)ben. Dies kann dazu führen, dass auch solche Behörden zu bestimmten intensiven Grundrechtseingriffen nur dann ermächtigt werden dürfen, wenn erhöhte Anforderungen an die Regelung des Eingriffsanlasses gewahrt sind. So liegt es insbesondere bei dem heimlichen Zugriff auf ein informationstechnisches System, der unabhängig von der handelnden Behörde das Risiko birgt, dass der Betroffene für eine weitgehende staatliche Ausspähung seiner Persönlichkeit verfügbar gemacht wird. Auch wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern.

256

(d) Weiter muss eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden, um die Interessen des Betroffenen verfahrensrechtlich abzusichern. Sieht eine Norm heimliche Ermittlungstätigkeiten des Staates vor, die -- wie hier -- besonders geschützte Zonen der Privatheit berühren oder eine besonders hohe Eingriffsintensität aufweisen, ist dem Gewicht des Grundrechtseingriffs durch geeignete Verfahrensvorkehrungen Rechnung zu tragen (vgl. BVerfGE 118, 168 [202], m.w.N.). Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.

257

(aa) Ein solcher Vorbehalt ermöglicht die vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz. Eine derartige Kontrolle kann bedeutsames Element eines effektiven Grundrechtsschutzes sein. Sie ist zwar nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden (vgl. BVerfGE 110, 33 [67 f.]). Sie kann aberBVerfGE 120, 274 (331) BVerfGE 120, 274 (332)gewährleisten, dass die Entscheidung über eine heimliche Ermittlungsmaßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn der Betroffene selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann. Die Kontrolle dient insoweit der "kompensatorischen Repräsentation" der Interessen des Betroffenen im Verwaltungsverfahren (vgl. SächsVerfGH, Urteil vom 14. Mai 1996 -- Vf.44-II-94 --, JZ 1996, S. 957 [964]).

258

(bb) Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, grundsätzlich ein Regelungsspielraum eingeräumt. Bei einem Grundrechtseingriff von besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren (vgl. BVerfGE 103, 142 [151]; 107, 299 [325]). Vorausgesetzt ist allerdings, dass sie die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten (zu den Anforderungen an die Anordnung einer akustischen Wohnraumüberwachung vgl. BVerfGE 109, 279 [358 ff.]; zur Kritik an der Praxis der Ausübung des Richtervorbehalts bei Wohnungsdurchsuchungen vgl. BVerfGE 103, 142 [152], m.w.N.).

259

Der Gesetzgeber darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter. Auch von ihr muss eine Begründung zur Rechtmäßigkeit gegeben werden.

260

Von dem Erfordernis einer vorherigen Kontrolle der Maßnahme durch eine dafür geeignete neutrale Stelle darf eine Ausnahme fürBVerfGE 120, 274 (332) BVerfGE 120, 274 (333)Eilfälle, etwa bei Gefahr im Verzug, vorgesehen werden, wenn für eine anschließende Überprüfung durch die neutrale Stelle gesorgt ist. Für die tatsächli-

chen und rechtlichen Voraussetzungen der Annahme eines Eilfalls bestehen dabei indes wiederum verfassungsrechtliche Vorgaben (vgl. BVerfGE 103, 142 [153 ff.] zu Art. 13 Abs. 2 GG).

261

(3) Nach diesen Maßstäben genügt die angegriffene Norm nicht den verfassungsrechtlichen Anforderungen.

262

(a) Nach § 5 Abs. 2 in Verbindung mit § 7 Abs. 1 Nr. 1 und § 3 Abs. 1 VSG sind Voraussetzung für den Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörde lediglich tatsächliche Anhaltspunkte für die Annahme, dass auf diese Weise Erkenntnisse über verfassungsfeindliche Bestrebungen gewonnen werden können. Dies ist sowohl hinsichtlich der tatsächlichen Voraussetzungen für den Eingriff als auch des Gewichts der zu schützenden Rechtsgüter keine hinreichende materielle Eingriffsschwelle. Auch ist eine vorherige Prüfung durch eine unabhängige Stelle nicht vorgesehen, so dass die verfassungsrechtlich geforderte verfahrensrechtliche Sicherung fehlt.

263

(b) Diese Mängel entfallen nicht, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG auf die näheren Voraussetzungen nach dem Gesetz zu Artikel 10 Grundgesetz trotz ihrer Unbestimmtheit in die Prüfung einbezogen und in der weiten Interpretation der nordrhein-westfälischen Landesregierung so verstanden wird, dass sie sich auf sämtliche formellen und materiellen Vorkehrungen dieses Gesetzes bezieht. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG beschränkt den heimlichen Zugriff auf ein informationstechnisches System nicht auf eine Telekommunikationsüberwachung, deren Voraussetzungen § 3 Abs. 1 G 10 regelt, sondern ermöglicht derartige Zugriffe grundsätzlich zur Gewinnung aller verfügbaren Daten.

264

Weder die Regelung der Eingriffsschwelle noch die verfahrensrechtlichen Vorgaben in den in § 3 Abs. 1 G 10 vorgesehenen Eingriffstatbeständen genügen den verfassungsrechtlichen Anforderungen.

265

(aa) Nach § 3 Abs. 1 Satz 1 G 10 ist eine ÜberwachungsmaßBVerfGE 120, 274 (333)BVerfGE 120, 274 (334)nahme zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat aus einem in der Norm geregelten Katalog plant, begeht oder begangen hat. Der Straftatenkatalog lässt zum einen kein Konzept erkennen, nach dem es gerechtfertigt sein könnte, sämtliche dort aufgeführten Straftaten zum Anlass von Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG zu nehmen. So ist nicht bei allen in Bezug genommenen Normen gesichert, dass der Zugriff im konkreten Fall der Abwehr eines der oben (C I 2 b, dd [2] [c] [aa]) aufgeführten überragend wichtigen Rechtsgüter dient. Zum andern stellt die Verweisung auf § 3 Abs. 1 Satz 1 G 10 nicht in jedem Fall sicher, dass der heimliche Zugriff auf ein informationstechnisches System nur erfolgt, wenn solche Rechtsgüter im Einzelfall mit hinreichender Wahrscheinlichkeit (C I 2 b, dd [2] [c] [bb]) in näherer Zukunft gefährdet sind.

266

Gemäß § 3 Abs. 1 Satz 2 G 10 kann eine Überwachungsmaßnahme auch angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die sich gegen die Schutzgüter des Verfassungsschutzes richten. Die Straftaten werden allerdings nur allgemein umschrieben, so dass das Risiko einer ausweitenden Auslegung naheliegt, die einen Eingriff auch zum Schutz von Rechtsgütern ermöglichen würde, die nicht überragend wichtig sind. Zudem müssten nach dieser Vorschrift nicht in jedem Fall, in dem der Eingriffstatbestand des § 3 Abs. 1 Satz 2 G 10 verwirklicht ist, hinreichende tatsächliche Anhaltspunkte für eine im Einzelfall von dieser Person oder der Vereinigung drohende Gefahr für ein überragend wichtiges Rechtsgut vorliegen.

267

(bb) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt weiter selbst dann, wenn die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz einbezogen wird, nicht den verfassungsrechtlichen Anforderungen an die vorbeugende Kontrolle eines heimlichen Zugriffs auf ein informationstechnisches System.

268

§ 10 G 10 sieht eine vorherige Anordnung der Überwachungsmaßnahme vor, die auf Antrag der Verfassungsschutzbehörde vonBVerfGE 120, 274 (334) BVerfGE 120, 274 (335)der zuständigen obersten Landesbehörde erteilt wird. Dieses Verfahren reicht nicht aus, um die von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geforderte vorbeugende Kontrolle sicherzustellen. Das Gesetz regelt weder einen Richtervorbehalt noch -- da die in § 3 Abs. 6 AG G 10 NRW enthaltene Regelung einer vorbeugenden Kontrolle durch die G 10-Kommission nicht von dem Verweis erfasst ist -- einen gleichwertigen Kontrollmechanismus. Die zuständige oberste Landesbehörde kann, anders als ein Gericht, aufgrund ihres Ressortzuschnitts ein eigenes Interesse an der Durchführung nachrichtendienstlicher Maßnahmen des Verfassungsschutzes haben. Sie bietet keine vergleichbare Gewähr für die Unabhängigkeit und Neutralität einer Kontrolle wie ein Gericht.

269

c) Schließlich fehlt es an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung durch Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG zu vermeiden.

270

aa) Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt (vgl. BVerfGE 6, 32 [41]; 27, 1 [6]; 32, 373 [378 f.]; 34, 238 [245]; 80, 367 [373]; 109, 279 [313]; 113, 348 [390]). Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen (vgl. BVerfGE 34, 238 [245]; 109, 279 [313]). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen (vgl. BVerfGE 109, 279 [314]).

271

Im Rahmen eines heimlichen Zugriffs auf ein informationstechnisches System besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind. So kann der Betroffene das System dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente, anzulegen und zu speiBVerfGE 120, 274 (335)BVerfGE 120, 274 (336)chern. Derartige Dateien können ebenso wie etwa schriftliche Verkörperungen des höchstpersönlichen Erlebens (dazu vgl. BVerfGE 80, 367 [373 ff.]; 109, 279 [319]) einen absoluten Schutz genießen. Zum anderen kann das System, soweit es telekommunikativen Zwecken dient, zur Übermittlung von Inhalten genutzt werden, die gleichfalls dem Kernbereich unterfallen können. Dies gilt nicht nur für Sprachtelefonate, sondern auch etwa für die Fernkommunikation mittels E-Mails oder anderer Kommunikationsdienste des Internet (vgl. BVerfGE 113, 348 [390]). Die absolut geschützten Daten können bei unterschiedlichen Arten von Zugriffen erhoben werden, etwa bei der Durchsicht von Speichermedien ebenso wie bei der Überwachung der laufenden Internetkommunikation oder gar einer Vollüberwachung der Nutzung des Zielsystems.

272

bb) Soll heimlich auf das informationstechnische System des Betroffenen zugegriffen werden, bedarf es besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen.

273

Die Bürger nutzen zur Verwaltung ihrer persönlichen Angelegenheiten und zur Telekommunikation auch mit engen Bezugspersonen zunehmend komplexe informationstechnische Systeme, die ihnen Entfaltungsmöglichkeiten im höchstpersönlichen Bereich bieten. Angesichts dessen schafft eine Ermittlungsmaßnahme wie der Zugriff auf ein informationstechnisches System, mittels dessen die auf dem Zielsystem vorhandenen Daten umfassend erhoben werden können, gegenüber anderen Überwachungsmaßnahmen -- etwa der Nutzung des Global Positioning Systems als Instrument technischer Observation (vgl. dazu BVerfGE 112, 304 [318]) -- die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden.

274

Wegen der Heimlichkeit des Zugriffs hat der Betroffene keine Möglichkeit, selbst vor oder während der Ermittlungsmaßnahme darauf hinzuwirken, dass die ermittelnde staatliche Stelle den Kernbereich seiner privaten Lebensgestaltung achtet. Diesem vollständigen Kontrollverlust ist durch besondere Regelungen zuBVerfGE 120, 274 (336) BVerfGE 120, 274 (337)begegnen, welche die Gefahr einer Kernbereichsverletzung durch geeignete Verfahrensvorkehrungen abschirmen.

275

cc) Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes können je nach der Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein.

276

Eine gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, hat so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Ist es -- wie bei dem heimlichen Zugriff auf ein informationstechnisches System -- praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden (vgl. BVerfGE 109, 279 [318]; 113, 348 [391 f.]).

277

(1) Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhebung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.

278

Selbst wenn der Datenzugriff unmittelbar durch Personen ohne vorherige technische Aufzeichnung erfolgt, etwa bei einer persönlichen Überwachung der über das Internet geführten Sprachtelefonie, stößt ein Kernbereichsschutz schon bei der Datenerhebung auf praktische Schwierigkeiten. Bei der Durchführung einer derartigen Maßnahme ist in der Regel nicht sicher vorhersehbar, welchen Inhalt die erhobenen Daten haben werden (vgl.

zur TelekomBVerfGE 120, 274 (337)BVerfGE 120, 274 (338)munikationsüberwachung BVerfGE 113, 348 [392]). Auch kann es Schwierigkeiten geben, die Daten inhaltlich während der Erhebung zu analysieren. So liegt es etwa bei fremdsprachlichen Textdokumenten oder Gesprächen. Auch in derartigen Fällen kann die Kernbereichsrelevanz der überwachten Vorgänge nicht stets vor oder bei der Datenerhebung abgeschätzt werden. In solchen Fällen ist es verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen, da Grundlage des Zugriffs auf das informationstechnische System tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Schutzgut sind.

279

(2) Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten.

280

(a) Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 [391 f.]; zur akustischen Wohnraumüberwachung BVerfGE 109, 279 [318, 324]). Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben. Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.

281

(b) In vielen Fällen wird sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären lassen. Der Gesetzgeber hat durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben.BVerfGE 120, 274 (338)

282

BVerfGE 120, 274 (339)Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt. Ergibt die Durchsicht, dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen (vgl. BVerfGE 109, 279 [324]; 113, 348 [392]).

283

dd) Das Verfassungsschutzgesetz enthält die erforderlichen kernbereichsschützenden Vorschriften nicht. Nichts anderes ergibt sich, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG auf das Gesetz zu Artikel 10 Grundgesetz trotz ihrer Unbestimmtheit einbezogen wird. Dieses Gesetz enthält gleichfalls keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

284

Entgegen der Auffassung der nordrhein-westfälischen Landesregierung kann insoweit selbst dann nicht § 4 Abs. 1 G 10 herangezogen werden, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG in weiter Interpretation so verstanden wird, dass sie sich auf diese Vorschrift erstreckt. § 4 Abs. 1 G 10 regelt lediglich, dass erhobene Daten, die nicht oder nicht mehr benötigt werden, zu löschen sind, und normiert damit das allgemeine Gebot der Erforderlichkeit. Die Vorschrift enthält demgegenüber keinerlei besondere Maßgaben für die Erhebung, Durchsicht und Löschung von Daten, die einen Kernbereichsbezug aufweisen können. Das Gebot der Erforderlichkeit kann mit der verfassungsrechtlich gebotenen Achtung des Kernbereichs privater Lebensgestaltung nicht gleichgesetzt werden. Der Kernbereich ist vielmehr einer Relativierung durch gegenläufige Ermittlungsinteressen, wie sie durch eine Anwendung des Erforderlichkeitsgebots implizit eingeführt würde, gerade nicht zugänglich (vgl. BVerfGE 109, 279 [314]).

285

d) Der Verstoß gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) führt zur Nichtigkeit von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG.BVerfGE 120, 274 (339)

286

BVerfGE 120, 274 (340)e) Angesichts dessen bedarf es keiner Prüfung mehr, wie weit Maßnahmen, zu denen die Norm ermächtigt, auch gegen andere Grundrechte oder das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG verstoßen.

287

II.

Die Ermächtigung zum heimlichen Aufklären des Internet in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG verletzt das durch Art. 10 Abs. 1 GG gewährleistete Telekommunikationsgeheimnis. Maßnahmen nach dieser Norm können sich in bestimmten Fällen als Eingriff in dieses Grundrecht darstellen, der verfassungsrechtlich nicht gerechtfertigt ist (1); auch ist Art. 19 Abs. 1 Satz 2 GG verletzt (2). Die Verfassungswidrigkeit führt zur Nichtigkeit der

Norm (3). Die Verfassungsschutzbehörde darf allerdings weiterhin Maßnahmen der Internetaufklärung treffen, soweit diese nicht als Grundrechtseingriffe anzusehen sind (4).

288

1. Das in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG geregelte heimliche Aufklären des Internet umfasst Maßnahmen, mit der die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt, also zum Beispiel durch Aufruf einer Webseite im World Wide Web mittels eines Web-Browsers (s. o. A I 1 a). Dies kann in bestimmten Fällen in das Telekommunikationsgeheimnis eingreifen. Ein solcher Eingriff wird durch die angegriffene Norm verfassungsrechtlich nicht gerechtfertigt.

289

a) Der Schutzbereich von Art. 10 Abs. 1 GG umfasst die mit einem an das Internet angeschlossenen informationstechnischen System geführte laufende Fernkommunikation (vgl. oben I 1 c, aa [1]). Allerdings schützt dieses Grundrecht lediglich das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird. Dagegen ist das Vertrauen der Kommunikationspartner zueinander nicht Gegenstand des Grundrechtsschutzes. Steht im Vordergrund einer staatlichen Ermittlungsmaßnahme nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den KommunikationsBVerfGE 120, 274 (340)BVerfGE 120, 274 (341)partner, so liegt darin kein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 106, 28 [37 f.]). Die staatliche Wahrnehmung von Inhalten der Telekommunikation ist daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein. Das Grundrecht schützt dagegen nicht davor, dass eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt.

290

Erlangt eine staatliche Stelle Kenntnis von den Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle hierzu nicht durch Kommunikationsbeteiligte autorisiert ist. Da das Telekommunikationsgeheimnis das personengebundene Vertrauen der Kommunikationsbeteiligten zueinander nicht schützt, erfasst die staatliche Stelle die Kommunikationsinhalte bereits dann autorisiert, wenn nur einer von mehreren Beteiligten ihr diesen Zugriff freiwillig ermöglicht hat.

291

Das heimliche Aufklären des Internet greift danach dann in Art. 10 Abs. 1 GG ein, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. So liegt es etwa, wenn ein mittels Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen.

292

Dagegen ist ein Eingriff in Art. 10 Abs. 1 GG zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt. Erst recht scheidet ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht.

293

b) Die von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG ermöglichtenBVerfGE 120, 274 (341) BVerfGE 120, 274 (342)Eingriffe in Art. 10 Abs. 1 GG sind verfassungsrechtlich nicht gerechtfertigt. Die angegriffene Norm genügt nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu solchen Eingriffen.

294

aa) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht, da aufgrund der Unbestimmtheit von Satz 2 dieser Vorschrift die Eingriffsvoraussetzungen nicht hinreichend präzise geregelt sind (vgl. oben C I 2 a, bb).

295

bb) Die angegriffene Norm steht weiter, soweit sie an Art. 10 Abs. 1 GG zu messen ist, mit dem Gebot der Verhältnismäßigkeit im engeren Sinne nicht in Einklang.

296

Der Eingriff in das Telekommunikationsgeheimnis wiegt schwer. Auf der Grundlage der angegriffenen Norm kann die Verfassungsschutzbehörde auf Kommunikationsinhalte zugreifen, die sensibler Art sein und Einblicke in die persönlichen Angelegenheiten und Gewohnheiten des Betroffenen zulassen können. Betroffen ist nicht nur derjenige, der den Anlass für die Überwachungsmaßnahme gegeben hat. Der Eingriff kann vielmehr eine gewisse Streubreite aufweisen, wenn Erkenntnisse nicht nur über das Kommunikationsverhalten desjenigen, gegen den sich die Maßnahme richtet, sondern auch über seine Kommunikationspartner gewonnen werden. Die Heimlichkeit des Zugriffs erhöht die Eingriffsintensität. Zudem können wegen der weiten Fassung der Eingriffsvoraussetzungen in § 7 Abs. 1 Nr. 1 in Verbindung mit § 3 Abs. 1 VSG auch Personen überwacht werden, die für den Eingriffsanlass nicht verantwortlich sind.

297

Ein derart schwerwiegender Grundrechtseingriff setzt auch unter Berücksichtigung des Gewichts der Ziele des Verfassungsschutzes grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus (vgl. zu strafrechtlichen Ermittlungen BVerfGE 107, 299 [321]). Daran fehlt es hier. Vielmehr lässt § 7 Abs. 1 Nr. 1 in Verbindung mit § 3 Abs. 1 VSG nachrichtendienstliche Maßnahmen in weitem Umfang im Vorfeld konkreter Gefährdungen zu, ohne Rücksicht auf das Gewicht der möglichen Rechtsgutsverletzung und auch gegenüber Dritten. EiBVerfGE 120, 274 (342)BVerfGE 120, 274 (343)ne derart weitreichende Eingriffsermächtigung ist mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar.

298

cc) Das Verfassungsschutzgesetz enthält im Zusammenhang mit Eingriffen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Solche Regelungen sind jedoch erforderlich, soweit eine staatliche Stelle zur Erhebung von Inhalten der Telekommunikation unter Eingriff in Art. 10 Abs. 1 GG ermächtigt wird (vgl. BVerfGE 113, 348 [390 ff.]).

299

2. Schließlich genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG, soweit die Norm zu Eingriffen in Art. 10 Abs. 1 GG ermächtigt, nicht dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG.

300

Nach Art. 19 Abs. 1 Satz 2 GG muss ein Gesetz dasjenige Grundrecht unter Angabe seines Artikels benennen, das durch dieses Gesetz oder aufgrund dieses Gesetzes eingeschränkt wird. Das Zitiergebot erfüllt eine Warn- und Besinnungsfunktion (vgl. BVerfGE 64, 72 [79 f.]). Durch die Benennung des Eingriffs im Gesetzeswortlaut soll gesichert werden, dass der Gesetzgeber nur Eingriffe vorsieht, die ihm als solche bewusst sind und über deren Auswirkungen auf die betroffenen Grundrechte er sich Rechenschaft ablegt (vgl. BVerfGE 5, 13 [16]; 85, 386 [404]). Die ausdrückliche Benennung erleichtert es auch, die Notwendigkeit und das Ausmaß des beabsichtigten Grundrechtseingriffs in öffentlicher Debatte zu klären. Nicht ausreichend ist hingegen, dass der Gesetzgeber sich des Grundrechtseingriffs bewusst war, wenn sich dies im Gesetzestext nicht niedergeschlagen hat (vgl. BVerfGE 113, 348 [366 f.]).

301

Die angegriffene Norm wahrt das Zitiergebot im Hinblick auf Art. 10 Abs. 1 GG nicht. Entgegen der Ansicht der nordrhein-westfälischen Landesregierung genügt die angegriffene Norm den Anforderungen nicht schon deshalb, weil § 5 Abs. 2 Nr. 11 Satz 2 VSG durch die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz darauf hindeuten mag, dass der Gesetzgeber einen Eingriff in das Telekommunikationsgeheimnis für möglich gehalten hat. Dem Zitiergebot ist nur Rechnung getragen, wenn das Grundrecht im Gesetzestext ausdrücklich als eingeschränkt benannt wird. ImBVerfGE 120, 274 (343) BVerfGE 120, 274 (344)Übrigen ergibt sich angesichts des Umstands, dass § 5 Abs. 2 Nr. 11 VSG zwei unterschiedliche Eingriffsermächtigungen enthält, aus dem Gesetz keineswegs mit hinreichender Deutlichkeit, für welche von ihnen der Gesetzgeber zumindest mit der Möglichkeit eines Eingriffs in Art. 10 GG gerechnet hat.

302

3. Der Verstoß von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG gegen Art. 10 Abs. 1 und Art. 19 Abs. 1 Satz 2 GG bewirkt die Nichtigkeit der Vorschrift.

303

4. Die Nichtigkeit der Ermächtigung führt allerdings nicht dazu, dass der Behörde Maßnahmen der Internetaufklärung grundsätzlich verwehrt sind, soweit diese nicht in Grundrechte eingreifen.

304

Das heimliche Aufklären des Internet greift, soweit es nicht unter Art. 10 Abs. 1 GG fällt, insbesondere nicht stets in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht ein.

305

a) Die von dem allgemeinen Persönlichkeitsrecht gewährleistete Vertraulichkeit und Integrität informationstechnischer Systeme wird durch Maßnahmen der Internetaufklärung nicht berührt, da Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG sich darauf beschränken, Daten, die der Inhaber des Systems -- beispielsweise der Betreiber eines Webservers -- für die Internetkommunikation vorgesehen hat, auf dem technisch dafür vorgesehenen Weg zu erheben. Für solche Datenerhebungen hat der Betroffene selbst sein System technisch geöffnet. Er kann nicht darauf vertrauen, dass es nicht zu ihnen kommt.

306

b) Zumindest in der Regel ist auch ein Eingriff in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in der Ausprägung als Recht auf informationelle Selbstbestimmung zu verneinen.

307

aa) Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können (vgl. etwa T. Böckenförde, Die Ermittlung im Netz, 2003, S. 196 f.; Zöller, GA 2000, S. 563 [569]). Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest anBVerfGE 120, 274 (344) BVerfGE 120, 274 (345)einen nicht weiter abgegrenzten Personenkreis richten. So liegt es etwa, wenn die Behörde eine allge-

mein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offen stehende Mailingliste abonniert oder einen offenen Chat beobachtet.

308

Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann allerdings gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Hierfür bedarf es einer Ermächtigungsgrundlage.

309

bb) Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde (vgl. zu Ermittlungen durch verdeckte Ermittler BVerwG, Urteil vom 29. April 1997 -- 1 C 2/95 --, NJW 1997, S. 2534; Di Fabio, in: Maunz/Dürig, GG, Art. 2 Abs. 1 Rn. 176; Duttge, JZ 1996, S. 556 [562 f.]; Murswiek, in: Sachs, GG, 4. Aufl., 2007, Art. 2 Rn. 88 b; Warntjen, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 2007, S. 163; speziell zu Ermittlungen im Netz Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.).

310

Danach wird die reine Internetaufklärung in aller Regel keinen Grundrechtseingriff bewirken. Die Kommunikationsdienste des Internet ermöglichen in weitem Umfang den Aufbau von Kommunikationsbeziehungen, in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen bereitstehen. Dies gilt selbst dann, wenn bestimmte Personen -- etwa im Rahmen eines Diskussionsforums -- über einen längeren Zeitraum an der KommunikaBVerfGE 120, 274 (345)BVerfGE 120, 274 (346)tion teilnehmen und sich auf diese Weise eine Art "elektronische Gemeinschaft" gebildet hat. Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig.

311

III.

Da § 5 Abs. 2 Nr. 11 VSG insgesamt nichtig ist, erledigen sich die gegen § 5 Abs. 3 und § 17 VSG vorgebrachten Rügen. Soweit die Rügen der Beschwerdeführer zulässig sind, ist die Verfassungswidrigkeit der angegriffenen Normen lediglich in Bezug auf Maßnahmen nach der nichtigen Vorschrift geltend gemacht.

312

IV.

§ 5a Abs. 1 VSG steht mit dem Grundgesetz in Einklang, soweit sein Anwendungsbereich auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG ausgedehnt wurde. Insbesondere verletzt diese Vorschrift nicht Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

313

1. Die in § 5a Abs. 1 VSG vorgesehene Erhebung von Kontoinhalten und Kontobewegungen greift in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein.

314

Derartige Kontoinformationen können für den Persönlichkeitsschutz des Betroffenen bedeutsam sein und werden vom Grundrecht geschützt. Nach den gegenwärtigen Gepflogenheiten werden die meisten Zahlungsvorgänge, die über Bargeschäfte des täglichen Lebens hinausgehen, über Konten abgewickelt. Werden Informationen über die Inhalte der Konten einer bestimmten Person gezielt zusammengetragen, ermöglicht dies einen Einblick in die Vermögensverhältnisse und die sozialen Kontakte des Betroffenen, soweit diese -- etwa durch Mitgliedsbeiträge oder Unterhaltsleistungen -- eine finanzielle Dimension aufweisen. Manche Konteninhaltsdaten, etwa die Höhe von Zahlungen im Rahmen verbrauchsabhängiger Dauerschuldverhältnisse, können auchBVerfGE 120, 274 (346) BVerfGE 120, 274 (347)weitere Rückschlüsse auf das Verhalten des Betroffenen ermöglichen (vgl. BVerfGE 118, 168 [185 f.]).

315

Die in § 5a Abs. 1 VSG vorgesehenen Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein. Dabei kommt es nicht darauf an, ob sich der Regelungsgehalt der angegriffenen Norm in einer Befugnis der Verfassungsschutzbehörde erschöpft, ein Auskunftsersuchen an ein Kreditinstitut zu richten, oder ob sie implizit eine Auskunftspflicht des jeweiligen Kreditinstituts enthält. In jedem Fall ermächtigt die Vorschrift die Behörde zu Datenerhebungen, die bereits als solche einen Grundrechtseingriff bewirken.

316

2. Die in § 5a Abs. 1 VSG vorgesehenen Grundrechtseingriffe sind jedoch zur Ermittlung im Hinblick auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG verfassungsrechtlich gerechtfertigt. Insbesondere genügt die angegriffene Norm insoweit dem Verhältnismäßigkeitsgrundsatz.

317

a) Die in § 5a Abs. 1 VSG geregelten Maßnahmen dienen aufgrund der Erweiterung des Anwendungsbereichs der Norm auch zur Aufklärung der Finanzierungswege und der finanziellen Verhältnisse und Verflechtungen im Zusammenhang mit Bestrebungen im Sinne von § 3 Abs. 1 Nr. 1 VSG. Dies ist ein legitimes Ziel des Verfassungsschutzes.

318

Die Norm ist in ihrer erweiterten Fassung geeignet, dieses Ziel zu erreichen. Sie ist hierzu auch erforderlich. Ein den Betroffenen weniger belastendes, aber ebenso wirksames Mittel zur Aufklärung von Bankgeschäften mit Blick auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG ist nicht ersichtlich.

319

b) § 5a Abs. 1 VSG wahrt auch das Gebot der Verhältnismäßigkeit im engeren Sinne.

320

aa) Allerdings ermächtigt die Norm die Verfassungsschutzbehörde zu Grundrechtseingriffen.

321

Bei Informationen über Kontoinhalte und Kontobewegungen kann es sich um sensible Daten handeln, deren Kenntnisnahme die grundrechtlich geschützten Interessen des Betroffenen erheblich beeinträchtigt. Die Erhebung solcher Informationen hat daher in der Regel ein erhöhtes grundrechtliches Gewicht (vgl. BVerfGEBVerfGE 120, 274 (347) BVerfGE 120, 274 (348)118, 168 [198 f.]). Die Intensität des Eingriffs wird zudem durch seine Heimlichkeit verstärkt. Nach § 5a Abs. 3 Satz 11 VSG darf auch das auskunftgebende Kreditinstitut dem Betroffenen das Auskunftsersuchen und die übermittelten Daten nicht mitteilen. Schließlich können dem Betroffenen Nachteile daraus entstehen, dass das kontoführende Kreditinstitut selbst zwangsläufig von der Datenerhebung erfährt und daraus ungünstige Schlüsse über den Betroffenen ziehen kann (vgl. BVerfGE 118, 168 [195]).

322

bb) Die mit § 5a Abs. 1 VSG verfolgten öffentlichen Interessen weisen jedoch solches Gewicht auf, dass sie zu den in der Norm geregelten Grundrechtseingriffen nicht außer Verhältnis stehen.

323

(1) Das Gesetz knüpft die Kenntnisnahme der Kontoinhalte und Kontobewegungen an tatbestandliche Voraussetzungen, die der Bedeutung des Grundrechtseingriffs für den Betroffenen hinreichend Rechnung tragen.

324

§ 5a Abs. 1 VSG macht die Erhebung von einem sowohl hinsichtlich der betroffenen Rechtsgüter als auch hinsichtlich der tatsächlichen Grundlage des Eingriffs qualifizierten Gefährdungstatbestand abhängig. Es müssen tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 3 Abs. 1 VSG genannten Schutzgüter vorliegen. Der Begriff der schwerwiegenden Gefahr verweist -- ebenso wie in dem insoweit gleichlautenden § 8a Abs. 2 BVerfSchG (vgl. dazu BTDrucks 16/2921, S. 14) -- auf eine erhöhte Intensität der Rechtsgutsbedrohung. Durch das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr wird zudem die tatsächliche Grundlage des Eingriffs qualifiziert. Es reicht nicht aus, dass die geregelte Datenerhebung allgemein für die Aufgabenerfüllung der Verfassungsschutzbehörde nützlich ist. Vielmehr müssen Anhaltspunkte für einen Zustand bestehen, in dem das Schutzgut konkret bedroht ist.

325

Diese in zweifacher Hinsicht qualifizierte Eingriffsschwelle genügt den Anforderungen des allgemeinen Persönlichkeitsrechts. Weitere Eingrenzungen der tatbestandlichen Voraussetzungen des Eingriffs sind von Verfassungs wegen nicht zu fordern.

326

Zurückzuweisen ist insbesondere die Auffassung des Beschwerdeführers zu 1b, die materielle Eingriffsschwelle müsse hinsichtBVerfGE 120, 274 (348)BVerfGE 120, 274 (349)lich der in § 3 Abs. 1 Nr. 1 VSG genannten Bestrebungen so heraufgesetzt werden, dass § 5a Abs. 1 VSG nur militante und volksverhetzende Bestrebungen erfasst. Durch das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr ist hinreichend sichergestellt, dass nicht jeder vage Verdacht, bestimmte Gruppierungen könnten sich gegen die freiheitliche demokratische Grundordnung richten, zu einer Erhebung von Kontoinhalten und Kontobewegungen ausreicht. Der damit verbundene Eingriff wiegt andererseits nicht so schwer, dass er lediglich zur Bekämpfung gewalttätiger oder solcher Gruppierungen verhältnismäßig sein könnte, die volksverhetzend tätig werden.

327

Keine durchgreifenden verfassungsrechtlichen Bedenken ergeben sich auch daraus, dass § 5a Abs. 1 VSG keine besonderen Anforderungen an die Auswahl des von einer Datenerhebung Betroffenen regelt. Aufgrund dessen kann es zwar geschehen, dass Kontoinhaltsdaten einer Person erhoben werden, die nicht im Verdacht steht, für die Gefahr rechtlich verantwortlich zu sein. In Betracht kommt insbesondere, dass jemand als undoloses Werkzeug in Vermögenstransaktionen der betroffenen Bestrebung eingeschaltet worden ist. Jedoch ist es verfassungsrechtlich zulässig, eine Maßnahme nach § 5a Abs. 1 VSG auch gegen eine solche Person zu treffen, wenn sich Finanzierungsmechanismen ansonsten nicht aufklären lassen. Die Auswahl zwischen mehreren denkbaren Betroffenen kann durch den auch im Rahmen von § 5a Abs. 1 VSG geltenden Verhältnismäßigkeitsgrundsatz hinreichend angeleitet werden. Dagegen werden Auskünfte über die Kontoinhalte von Personen, die nicht im

Verdacht stehen, an den Vermögenstransaktionen der betroffenen Bestrebung bewusst oder unbewusst beteiligt zu sein, kaum je dem gesetzlichen Ziel dienen können, einer schwerwiegenden Gefahr durch die Aufklärung von Finanzierungsmechanismen zu begegnen.

328

(2) Die angegriffene Norm trägt dem Gewicht des geregelten Grundrechtseingriffs zudem durch geeignete Verfahrensvorkehrungen Rechnung.

329

So bedarf die Datenerhebung nach § 5a Abs. 3 Satz 3 VSG einerBVerfGE 120, 274 (349) BVerfGE 120, 274 (350)Anordnung des Innenministers, die vom Leiter der Verfassungsschutzabteilung oder seinem Vertreter zu beantragen ist. Der in der Erhebung von Kontoinhalten und Kontobewegungen liegende Grundrechtseingriff wiegt zwar nicht so schwer, dass eine ex-ante-Kontrolle durch eine neutrale Stelle verfassungsrechtlich schlechthin geboten wäre. Die vorgesehene behördeninterne Kontrolle dient jedoch der Sicherung der Interessen des Betroffenen bereits im Vorfeld der Datenerhebung und trägt so zur Verhältnismäßigkeit des Eingriffs bei. Zudem ist eine zusätzliche ex-post-Kontrolle durch die G 10-Kommission gemäß § 5a Abs. 3 Satz 4 bis 8 VSG vorgesehen, die gleichfalls dem Schutz der grundrechtlich geschützten Interessen des Betroffenen dient.

330

Für die Verarbeitung und Übermittlung der erhobenen Daten enthält § 5a Abs. 3 Satz 9 VSG in Verbindung mit § 4 AG G 10 NRW Maßgaben, die insbesondere den Geboten der Erforderlichkeit und der Zweckbindung genügen.

331

§ 5a Abs. 3 Satz 11 VSG in Verbindung mit § 5 AG G 10 NRW sieht schließlich eine Benachrichtigung des Betroffenen vor, sobald eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Auf diese Weise wird dem Betroffenen weitgehend ermöglicht, seine Interessen zumindest im Nachhinein zu verfolgen. […]

**4) BVerfGE 115, 320 – Rasterfahndung II**

*a) Sachverhalt*

Die Verfassungsbeschwerde richtete sich gegen gerichtliche Entscheidungen über die Anordnung einer präventiven polizeilichen Rasterfahndung. Die Rasterfahndung ist eine besondere polizeiliche Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Polizeibehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich (Rasterung) mit anderen Daten vorzunehmen. Durch den Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte und für die weiteren Ermittlungen als bedeutsam angesehene Merkmale zutreffen. Nach den terroristischen Anschlägen vom 11. September 2001 führten die Landespolizeibehörden unter Mitwirkung des Bundeskriminalamts eine bundesweit koordinierte Rasterfahndung nach islamistischen Terroristen durch, nachdem bekannt geworden war, dass einige der Attentäter zuvor in Deutschland gelebt hatten (vgl. zur Frage der Vorbereitung der Anschläge von Deutschland aus BGHSt 49, 112 [112ff., 116ff.] = NJW 2004, 112; BGH, NJW 2005, 2322 [2324f.]). Ziel war insbesondere die Erfassung so genannter Schläfer, also solcher Personen, die zu terroristischen Handlungen bereit sind, sich jedoch lange Zeit hindurch sorgfältig um ein gesetzeskonformes und möglichst unauffälliges Verhalten bemühen, um ihr kriminelles Vorhaben dann im entscheidenden Zeitpunkt überraschend und damit besonders wirkungsvoll verwirklichen zu können. Am 18. 9. 2001 setzte der Arbeitskreis „Innere Sicherheit" der Ständigen Konferenz der Innenminister und -senatoren der Länder eine „Koordinierungsgruppe Internationaler Terrorismus" unter Vorsitz des Bundeskriminalamts ein, in welcher unter anderem der Bundesgrenzschutz, das Bundesamt für Verfassungsschutz und der Bundesnachrichtendienst vertreten waren (vgl. BT-Dr 14/7206, S. 1f.). Von dieser Koordinierungsgruppe wurden nach Angaben des Bundesbeauftragten für den Datenschutz bundesweit abgestimmte Rasterkriterien zur Entdeckung potenzieller islamistischer Terroristen in Deutschland entwickelt. Die Landeskriminalämter erhoben anschließend Daten unter anderem bei Universitäten, Einwohnermeldeämtern und dem Ausländerzentralregister und rasterten die Datenbestände nach den folgenden Kriterien: männlich, Alter 18 bis 40 Jahre, Student oder ehemaliger Student, islamische Religionszugehörigkeit, Geburtsland oder Nationalität bestimmter, im Einzelnen benannter Länder mit überwiegend islamischer Bevölkerung (vgl. zu den Kriterien auch AG Wiesbaden, DuD 2001, 752 [753f.]). Die durch Datenabgleich nach diesen Kriterien auf Landesebene gewonnenen Daten wurden anschließend an das Bundeskriminalamt übermittelt. Dort wurden sie in die bundesweite Verbunddatei „Schläfer" eingestellt. Nach Angaben des Bundeskriminalamts übermittelten die Länder insgesamt 31988 Datensätze. Diese wurden anschließend mit weiteren, durch das Bundeskriminalamt erhobenen Datenbeständen abgeglichen. Unter den Abgleichsdateien befanden sich nach Angaben des Polizeipräsidiums Düsseldorf gegenüber der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen etwa Dateien über Inhaber von Fluglizenzen oder Personen, die gem. § 12b AtG einer Zuverlässigkeitsprüfung bedürfen. Nach Einschätzung des Bundesbeauftragten für den Datenschutz waren in diesen Abgleichsdateien zwischenzeitlich die Daten von 200000 bis 300000 Personen gespeichert. Als „Treffer" sei es beim Abgleich angesehen worden, wenn ein Datensatz aus der Datei

„Schläfer" mit einem Abgleichsdatensatz in jeweils zwei Bestandteilen eine Übereinstimmung ergeben habe, etwa Name und Geburtsdatum oder Name und Geburtsland. Das Ergebnis des Abgleichs sei in einer Ergebnisdatei zusammengefasst und den jeweiligen Landeskriminalämtern zur Verfügung gestellt worden. Sowohl die Daten der Verbunddatei „Schläfer" als auch die Abgleichsdateien waren nach Angaben des Bundesbeauftragten für den Datenschutz bis 2003 beim Bundeskriminalamt gespeichert. Die Löschung der Verbunddatei erfolgte danach am 30. 6. 2003, die der Abgleichsdateien am 21. 7. 2003. Die Rasterfahndung führte, soweit ersichtlich, in keinem Fall dazu, dass „Schläfer" aufgedeckt worden wären oder gar auf Grund der gewonnenen Erkenntnisse eine Anklage - etwa wegen Mitgliedschaft in einer terroristischen Vereinigung oder wegen Unterstützung einer solchen (vgl. §§ 129a, 129b StGB) - gegen eine der davon erfassten Personen erhoben worden wäre.
An der bundesweit koordinierten Rasterfahndung beteiligte sich auch das Land Nordrhein-Westfalen. Am 2. 10. 2001 ordnete das AG auf Antrag des Polizeipräsidiums Düsseldorf die Rasterfahndung durch den mit der Verfassungsbeschwerde angegriffenen Beschluss an. Alle Einwohnermeldeämter des Landes Nordrhein-Westfalen, das Ausländerzentralregister in Köln und die Universitäten, Hochschulen und Fachhochschulen in Nordrhein-Westfalen wurden verpflichtet, Daten von zwischen dem 1. 10. 1960 und dem 1. 10. 1983 geborenen Männern zu übermitteln. Die Anordnung stützte sich auf § 31 NWPolG in der Fassung der Bekanntmachung vom 24. 2. 1990 (GVBl S. 70, im Folgenden: NWPolG 1990). Die Vorschrift lautete:

**§ 31. Rasterfahndung**. (1) Die Polizei kann von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung).

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie andere für den Einzelfall benötigte Daten zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen von der Polizei nicht genutzt werden.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf den Datenträgern zu löschen und die Akten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, zu vernichten. Über die getroffene Maßnahme ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten oder der Vernichtung der Akten nach Satz 1 folgt, zu vernichten.

(4) Die Maßnahme darf nur auf Antrag des Behördenleiters durch den Richter angeordnet werden. Zuständig ist das AG, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(5) Personen, gegen die nach Abschluss der Rasterfahndung weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der weiteren Datennutzung erfolgen kann. Die Unterrichtung durch die Polizei unterbleibt, wenn wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden ist.

Die Vorschrift ist 2003 geändert worden. § 31 in der Fassung der Bekanntmachung vom 25. 7. 2003 (GVBl S. 441, im Folgenden: NWPolG 2003) verzichtet in Absatz 1 auf das Merkmal der Gegenwärtigkeit der Gefahr. Dieser lautet nunmehr wie folgt: Die Polizei kann von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs die Übermittlung von personenbezogenen Daten einer unbestimmten Anzahl von Personen, die bestimmte, auf Verursacher einer Gefahr i.S. des § 4 vermutlich zutreffende Prüfungsmerkmale erfüllen, zum Zwecke des maschinellen Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung). Der Datenabgleich soll den Ausschluss von Personen bezwecken; er kann auch der Ermittlung eines Verdachts gegen Personen als mögliche Verursacher einer Gefahr sowie der Feststellung gefahrenverstärkender Eigenschaften dieser Personen dienen. Die Polizei kann zur Ergänzung unvollständig übermittelter Daten die erforderlichen Datenerhebungen auch bei anderen Stellen durchführen und die übermittelten Datenträger zur Ermöglichung des maschinellen Abgleichs technisch aufbereiten.
Zur Begründung seiner Anordnung vom 2. 10. 2001 führte das AG unter anderem aus: Es bestehe eine gegenwärtige Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person in Form von terroristischen Gewaltakten extremistischer islamistischer Gruppierungen. Diese seien nach den polizeilichen Erkenntnissen für die Terroranschläge in den Vereinigten Staaten von Ameri-

ka vom 11. September 2001 verantwortlich. Es könne als gesichert gelten, dass diese extremistischen Gruppierungen international agierten. Ihre Mitglieder und Anhänger seien militärisch und ideologisch geschult und jederzeit zu den gravierendsten Terroranschlägen bereit. Diese Gefahr bestehe gegenwärtig. Zwar lasse sich derzeit ein unmittelbar bevorstehender Anschlag nicht sicher prognostizieren. Auf Grund der bereits begangenen Taten und der sich zuspitzenden Lage im Mittleren Osten, wo ein Militärschlag der Vereinigten Staaten und ihrer Verbündeten in Kürze zu erwarten sei, müsse aber jederzeit mit einem terroristischen Vergeltungsschlag gerechnet werden. Die Anordnung der Rasterfahndung sei verhältnismäßig.
Der 1978 geborene Bf. ist marokkanischer Staatsangehöriger islamischen Glaubens. Im Zeitpunkt der hier angegriffenen Anordnung war er Student der Universität Duisburg. Er legte gegen den Beschluss des AG Beschwerde ein. Die Voraussetzungen des § 31 I NWPolG 1990 für die Anordnung einer Rasterfahndung seien nicht gegeben. Insbesondere fehle es am Vorliegen einer gegenwärtigen Gefahr. Das LG wies die Beschwerde mit dem ebenfalls angegriffenen Beschluss als unbegründet zurück. Das Gericht folge den zutreffenden Ausführungen des AG im angefochtenen Beschluss. Der Bf. erhob gegen den Beschluss des LG weitere Beschwerde, welche durch das OLG mit dem ebenfalls angegriffenen Beschluss zurückgewiesen wurde.
Mit seiner Verfassungsbeschwerde machte der Bf. eine Verletzung seines Grundrechts auf informationelle Selbstbestimmung aus Art. 2 I i.V. mit Art. 1 I GG geltend. Das BVerfG stellte fest: Der Beschluss des OLG Düsseldorf vom 8. 2. 2002 (3 Wx 356/01), der Beschluss des LG Düsseldorf vom 29. 10. 2001 (25 T 873/01) und der Beschluss des AG Düsseldorf vom 2. 10. 2001 (151 Gs 4092/01) verletzen den Bf. in seinem Grundrecht aus Art. 2 I i.V. mit Art. 1 I GG. Die Beschlüsse des OLG und des LG werden aufgehoben. Das Verfahren wird an das LG zurückverwiesen.
(Zusammenfassung nach NJW 2006, 1939, beck-online)

*b) Leitsätze*

**1.** Eine präventive polizeiliche Rasterfahndung der in § 31 PolG NW 1990 geregelten Art ist mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) nur vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus.
**2.** Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen reichen für die Anordnung der Rasterfahndung nicht aus. Vorausgesetzt ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergibt.
(Bearbeitung, zuletzt am 12. Juli 2016, durch: Engin Kunter; Dominika Blonski, http://www.servat.unibe.ch/dfr/bv115320.html )

*c) Begründung*

Die zulässige Verfassungsbeschwerde ist begründet.
Die angegriffenen Entscheidungen verletzen den Beschwerdeführer in seinem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Sie sind auf eine verfassungsgemäße Eingriffsgrundlage gestützt, geben dieser jedoch im Wege der Auslegung einen Inhalt, den auch der Gesetzgeber nicht ohne Verstoß gegen dieses Grundrecht hätte bestimmen dürfen. Die Anwendung der Vorschrift im konkreten Fall beruht auf dieser Auslegung. […]
I.
§ 31 Abs. 1 PolG NW 1990, auf den die Anordnung der Rasterfahndung gestützt ist, entspricht der Verfassung in formeller und materieller Hinsicht.
67
1. § 31 Abs. 1 PolG NW 1990 ermächtigt zu Eingriffen in den Schutzbereich des durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgten Grundrechts auf informationelle Selbstbestimmung.
68
a) Dieses Recht gewährleistet die aus dem Grundsatz der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. BVerfGE 65, 1 [43]; 78, 77 [84]; 84, 192 [194]; 96, 171 [181]; 103, 21 [32 f.]; 113, 29 [46]). Es sichert seinen Trägern insbesondere Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten (vgl. BVerfGE 65, 1 [43]; 67, 100 [143]; 84, 239 [279]; 103, 21 [33]; BVerfG, NJW 2006, S. 976 [979]). Denn individuelle Selbstbestimmung setzt -- auch unter den Bedingungen moderner Informationsverarbeitung -- voraus, dass dem Einzelnen EntscheidungsfreiheitBVerfGE 115, 320 (341) BVerfGE 115, 320 (342)über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunika-

tionspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden (vgl. BVerfGE 65, 1 [42 f.]).

69

Die beobachtende oder observierende Tätigkeit der Polizei kann den grundrechtlichen Schutzbereich berühren und die rechtliche Qualität von Grundrechtseingriffen gewinnen (vgl. BVerfGE 110, 33 [56]). Das gilt namentlich, wenn personenbezogene Informationen zum Zwecke der elektronischen Datenverarbeitung erhoben und gespeichert werden. In der Folge sind diese Daten nicht nur jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar, sie können darüber hinaus -- vor allem beim Aufbau integrierter Informationssysteme -- mit anderen Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen (vgl. BVerfGE 65, 1 [42]). Der mit solchen technischen Möglichkeiten unter den modernen Bedingungen der Datenverarbeitung einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz (vgl. BVerfGE 65, 1 [42]; 113, 29 [45 f.]).

70

b) Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist durch die Ermächtigung des § 31 PolG NW 1990 berührt.

71

Die gesetzliche Befugnis betrifft Informationen mit unterschiedlich intensivem Bezug zu dem Persönlichkeitsrecht. Es kann dahinstehen, ob das Recht auf informationelle Selbstbestimmung vor der Erhebung jedes einzelnen Datums, das von der Erhebung erfasst wird, schützt, da die Kenntnis jedes der Daten im Zusammenhang mit anderen einen eigenständigen Einblick in den Persönlichkeitsbereich ermöglicht. Die Kombination der ausdrücklich in § 31 Abs. 2 PolG NW 1990 benannten Daten -- Name, Anschrift, Tag und Ort der Geburt -- mit anderen, etwa, wie im vorliegenden Fall, derBVerfGE 115, 320 (342) BVerfGE 115, 320 (343)Staatsangehörigkeit, der Religionszugehörigkeit oder der Studienfachrichtung, kann und soll Aufschluss über Verhaltensweisen und damit Verdachtsmomente und insbesondere -- wie es in § 31 Abs. 1 PolG NRW 2003 nunmehr ausdrücklich heißt -- über "gefahrenverstärkende Eigenschaften dieser Personen" ermöglichen. Vor einer Datenerhebung und Datenverarbeitung mit dieser Zielrichtung schützt das Grundrecht auf informationelle Selbstbestimmung.

72

c) Die Regelung des § 31 Abs. 1 PolG NW 1990 ermächtigt zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung derjenigen, auf welche sich die übermittelten Daten beziehen.

73

aa) Die Übermittlungsanordnung stellt einen Eingriff dar, da sie die Grundlage für die Erfassung und Speicherung der Daten sowie für ihren Abgleich mit weiteren Daten schafft. Die Eingriffsqualität der Anordnung zeigt sich an ihrer Auswirkung auf das Recht auf personelle Selbstbestimmung der Betroffenen. Die Anordnung macht die Daten für die Behörden verfügbar und bildet die Basis für einen nachfolgenden Abgleich mit Suchbegriffen. An der Eingriffsqualität fehlt es lediglich, sofern Daten ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden (vgl. BVerfGE 100, 313 [366]; 107, 299 [328]). Auch dann, wenn die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge bildet, kann in der Datenerhebung bereits ein Eingriff liegen (vgl. BVerfGE 100, 313 [366 mit 337, 380]). Maßgeblich ist, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist.

74

Bei einer Rasterfahndung gemäß § 31 Abs. 1 PolG NW 1990 ist dies jedenfalls hinsichtlich solcher Personen der Fall, deren Daten nach einem ersten Datenabgleich noch Gegenstand weiterer, nachfolgender Maßnahmen, insbesondere weitergehender Datenabgleiche, werden sollen. Die Übermittlungsanordnung stellt eine BeeinBVerfGE 115, 320 (343)BVerfGE 115, 320 (344)trächtigung des informationellen Selbstbestimmungsrechts dieser Personen dar. Das Verlangen der Datenübermittlung richtet sich zwar nicht unmittelbar an diese Personen, es zielt aber auf die Erfassung ihrer Daten und nimmt sie damit in das Visier staatlicher Überwachungstätigkeit.

75

So ist etwa im vorliegenden Fall ein Grundrechtseingriff durch die Übermittlung jedenfalls bei denjenigen zunächst etwa 11.000 Personen zu bejahen, die von den Landesbehörden im Wege des Abgleichs nach den bundesweit abgesprochenen Kriterien aus der Gesamtmenge der übermittelten Datensätze ausgefiltert wurden. Diese Datensätze sollten Gegenstand weiterer Verarbeitungsmaßnahmen werden. Dafür wurden sie an das Bundeskriminalamt weitergeleitet, um dort in die bundesweite Datei "Schläfer" eingestellt und mit weiteren Dateien abgeglichen zu werden. Darüber hinaus stand der Großteil der Datensätze den Landesbehörden auch nach der Übermittlung an das Bundeskriminalamt zur Verfügung.

76

Ein eigenständiges behördliches Ermittlungsinteresse besteht in solchen Fällen nicht nur hinsichtlich der nach Vollzug aller Teilschritte verbleibenden Restmenge an Daten, sondern bereits bei den ersten, für die weiteren Maßnahmen erforderlichen Teilschritten, durch welche die übermittelte Gesamtdatenmenge nach und nach reduziert wird.

77

bb) Auch die -- sei es auch nur vorläufige -- Speicherung der übermittelten Daten bei der Stelle, an welche sie übermittelt und bei der sie aufbewahrt und für den Datenabgleich bereitgehalten werden, greift in das informationelle Selbstbestimmungsrecht derjenigen Personen ein, deren Daten nach einem solchen Datenabgleich Gegenstand weiterer Maßnahmen werden (vgl. BVerfGE 100, 313 [366]).

78

cc) Eingriffscharakter kommt in Bezug auf diese Personen schließlich auch dem Datenabgleich selbst als Akt der Auswahl für eine weitere Auswertung zu (vgl. BVerfGE 100, 313 [366]).

79

2. Die in § 31 Abs. 1 PolG NW 1990 enthaltene Ermächtigung zu Grundrechtseingriffen genügt verfassungsrechtlichen Anforderungen.

80

a) Das Grundrecht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der Einzelne muss vielmehr solBVerfGE 115, 320 (344)BVerfGE 115, 320 (345)che Beschränkungen seines Rechts hinnehmen, die durch überwiegende Allgemeininteressen gerechtfertigt sind (vgl. BVerfGE 65, 1 [43 f.]). Diese Beschränkungen bedürfen jedoch einer verfassungsmäßigen gesetzlichen Grundlage, die insbesondere dem Grundsatz der Verhältnismäßigkeit und dem Gebot der Normenklarheit entsprechen muss (vgl. BVerfGE 65, 1 [44]).

81

b) Die das Grundrecht beschränkende Regelung des § 31 Abs. 1 PolG NW 1990 wahrt den Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass der Staat mit dem Grundrechtseingriff einen legitimen Zweck mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt (vgl. BVerfGE 109, 279 [335 ff.]).

82

aa) Mit der Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person verfolgt die Regelung einen legitimen Zweck.

83

bb) Das Mittel der Rasterfahndung ist zur Verfolgung dieses Zweckes auch geeignet.

84

Ein Gesetz ist zur Zweckerreichung geeignet, wenn mit seiner Hilfe der erstrebte Erfolg gefördert werden kann (vgl. BVerfGE 67, 157 [173, 175]; 90, 145 [172]; 100, 313 [373]; 109, 279 [336]). Das ist vorliegend der Fall. Die Eignung scheitert nicht etwa an der großen Streubreite der Erfassungsmethode, die nur in vergleichsweise wenigen Fällen Erkenntnisse verspricht (vgl. BVerfGE 100, 313 [373]).

85

cc) Der Eingriff ist auch erforderlich zur Verfolgung des gesetzgeberischen Zweckes. Dieser lässt sich nicht durch mildere Mittel ebenso wirksam erreichen.

86

dd) Die gesetzliche Ermächtigung wahrt auch noch die Grenzen der Verhältnismäßigkeit im engeren Sinn.

87

Das Gebot der Verhältnismäßigkeit im engeren Sinn verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (stRspr; vgl. BVerfGE 90, 145 [173]; 92, 277 [327]; 109, 279 [349 ff.]). Die Prüfung an diesem Maßstab kann dazu führen, dass ein an sich geeignetes und erforderliches Mittel des Rechtsgüterschutzes nicht angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen den Zuwachs an RechtsgüterBVerfGE 115, 320 (345)BVerfGE 115, 320 (346)schutz überwiegen, so dass der Einsatz des Schutzmittels als unangemessen erscheint (vgl. BVerfGE 90, 145 [173]). In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte ist es dabei zunächst Aufgabe des Gesetzgebers, in abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen (vgl. BVerfGE 109, 279 [350]). Dies kann dazu führen, dass bestimmte intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen. Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten (vgl. BVerfGE 100, 313 [383 f.]; 109, 279 [350 ff.]; BayVerfGH, Entscheidung vom 7. Februar 2006 -- Vf. 69-VI-04 --).

88

Diese Voraussetzungen sind bei der Rasterfahndung gewahrt, wenn der Gesetzgeber den Grundrechtseingriff an das Vorliegen einer konkreten Gefahr für die bedrohten Rechtsgüter knüpft. Das ist bei der hier maßgeblichen Regelung des § 31 Abs. 1 PolG NW 1990 der Fall.

89

(1) Der Eingriff, zu dem § 31 PolG NW 1990 ermächtigt, dient dem Schutz hochrangiger Verfassungsgüter.

90

Mit dem Bestand und der Sicherheit des Bundes und eines Landes sowie Leib, Leben und Freiheit einer Person, die vor Gefahren geschützt werden sollen, sind Schutzgüter von hohem verfassungsrechtlichem Gewicht bezeichnet. Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm -- unter Achtung von Würde und Eigenwert des Einzelnen -- zu gewährleistende Sicherheit der Bevölkerung sind Verfassungswerte, die mit anderen hochwertigen im gleichen Rang stehen (vgl. BVerfGE 49, 24 [56 f.]).

91
Art. 2 Abs. 2 Satz 1 GG verpflichtet in Verbindung mit Art. 1 Abs. 1 Satz 2 GG den Staat dazu, das Leben und die körperliche Unversehrtheit des Einzelnen zu schützen, das heißt vor allem, auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren (stRspr; vgl. BVerfGE 90, 145 [195]; BVerfG, NJW 2006, S. 751 [757]). Dieser Schutzpflicht des Staates kommt ein hohes verfasBVerfGE 115, 320 (346)BVerfGE 115, 320 (347)sungsrechtliches Gewicht zu. Gleiches gilt für das Rechtsgut der Freiheit einer Person im Sinne des Art. 2 Abs. 2 Satz 2 GG.

92
(2) Zum Schutz dieser Rechtsgüter ermächtigt § 31 PolG NW 1990 zu Eingriffen in das Recht auf informationelle Selbstbestimmung von erheblichem Gewicht.

93
(a) Für die rechtliche Beurteilung der Art des durch die Ermächtigung ermöglichten Eingriffs ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben (vgl. BVerfGE 100, 313 [376]; 107, 299 [318 ff.]; 109, 279 [353]). Maßgebend sind also die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen (vgl. BVerfGE 100, 313 [376]). Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden (vgl. BVerfGE 100, 313 [376]; 109, 279 [353]).

94
Das Bundesverfassungsgericht hat diese Kriterien für die Bemessung der Eingriffsintensität informationsbezogener Grundrechtseingriffe bislang vor allem in Entscheidungen zum Fernmeldegeheimnis aus Art. 10 Abs. 1 GG und zum Grundrecht der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG entwickelt. Da diese Grundrechte spezielle Ausprägungen des Grundrechts auf informationelle Selbstbestimmung darstellen (vgl. BVerfGE 51, 97 [105]; 100, 313 [358]; 109, 279 [325 f.]), sind diese Maßstäbe auch auf das allgemeinere Grundrecht anwendbar, soweit sie nicht durch die für die speziellen Gewährleistungen geltenden Besonderheiten geprägt sind.

95
(b) Auch wenn die von der Rasterfahndung betroffenen Informationen für sich genommen im Regelfall eine geringere Persönlichkeitsrelevanz haben werden, als sie regelmäßig bei Eingriffen in den Schutzbereich der Grundrechte aus Art. 10 Abs. 1 und Art. 13 Abs. 1 GG gegeben ist, kommt den mit der Rasterfahndung verbundenen Eingriffen angesichts der inhaltlichen Weite der Befugnis sowie der mit ihr eröffneten Möglichkeit der Verknüpfung von DatenBVerfGE 115, 320 (347) BVerfGE 115, 320 (348)auch im Hinblick auf das allgemeine Grundrecht auf informationelle Selbstbestimmung ein erhebliches Gewicht zu.

96
(aa) Das Gewicht eines Eingriffs in das Recht auf informationelle Selbstbestimmung hängt unter anderem davon ab, welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen, und auf welchem Wege diese Inhalte erlangt werden (vgl. BVerfGE 100, 313 [376]; 107, 299 [319 f.]; 109, 279 [353]).

97
So ist die Eingriffsintensität hoch, wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG (vgl. BVerfGE 109, 279 [313 f., 325, 327 f.]; 113, 348 [364 f., 383, 391]).

98
Sämtliche durch die Rasterfahndung betroffenen Informationen haben einen Personenbezug und erlauben durch ihre Verknüpfung mit anderen Informationen persönlichkeitsbezogene Einblicke. Eine besondere Persönlichkeitsrelevanz kommt vor allem Informationen zu, die sich auf anderweitig, etwa in Art. 3 Abs. 3 GG oder in Art. 140 GG in Verbindung mit Art. 136 Abs. 3 WRV verfassungsrechtlich geschützte Bereiche beziehen. Dies findet auf einfachgesetzlicher Ebene etwa in der Kategorie der "besonderen Arten personenbezogener Daten" gemäß § 3 Abs. 9 BDSG Ausdruck, wozu nach dieser Vorschrift Angaben über die rassische und ethnische Herkunft, über politische Meinungen, religiöse oder philosophische Überzeugungen, über eine Gewerkschaftszugehörigkeit und über die Gesundheit oder das Sexualleben zu zählen sind.

99
(bb) Dem durch die Ermächtigung zur Rasterfahndung ermöglichten Grundrechtseingriff kommt grundsätzlich ein erhebliches Gewicht mit Blick auf den Inhalt sowohl der übermittelten Daten als auch derjenigen Daten zu, mit denen die übermittelten abgeglichen werden sollen. Gleiches gilt für diejenigen weiterreichenden Informationen, die aus der Zusammenführung und dem Abgleich der verschiedenen Datenbestände gewonnen werden können.BVerfGE 115, 320 (348)

100

BVerfGE 115, 320 (349)Bereits die zu übermittelnden Daten können eine hohe Persönlichkeitsrelevanz haben. Die gesondert genannten Identifizierungsdaten, also Name, Anschrift, Tag und Ort der Geburt, stehen zwar entstehungsgeschichtlich betrachtet im Vordergrund der Rasterfahndung. Hierauf beschränkt sich aber die gesetzliche Befugnis nicht. Vielmehr können auch alle anderen "für den Einzelfall benötigte(n) Daten" in die Fahndung einbezogen werden (§ 31 Abs. 2 Satz 1, 1. Halbsatz PolG NW 1990). Das Übermittlungsersuchen darf sich lediglich auf diejenigen personenbezogenen Daten nicht erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (§ 31 Abs. 2 Satz 1, 2. Halbsatz PolG NW 1990). Im Übrigen sind die von der Befugnis erfassten Daten nach Art und Inhalt nicht eingegrenzt. Dementsprechend kann -- wie vorliegend geschehen -- das Ersuchen auf weitere Angaben zur Religionszugehörigkeit, Staatsangehörigkeit, zum Familienstand und zur Studienfachrichtung erstreckt werden. Die gesetzliche Befugnis umfasst demnach auch solche persönlichkeitsbezogenen Daten, an deren Privatheit der Einzelne ein hohes Interesse besitzen kann und auf deren Vertraulichkeit er baut, wie etwa seine Glaubensüberzeugung. Dies kann auch auf die "anderen Datenbestände" zutreffen, mit denen die übermittelten Daten abgeglichen werden. Hinzu kommt, dass sich aus der Zusammenführung und Kombination der übermittelten und der sonstigen Datenbestände und ihrem wechselseitigen Abgleich vielfältige neue Informationen gewinnen lassen. Sie können nach Art und Inhalt eine besonders starke Persönlichkeitsrelevanz besitzen.

101

(c) Erfasst eine Übermittlungsbefugnis, wie diejenige nach § 31 Abs. 1 PolG NW 1990, nahezu sämtliche personenbezogenen Daten, die bei irgendeiner öffentlichen oder nichtöffentlichen Stelle vorhanden sind, wird damit aufgrund der Vielfältigkeit und des Umfangs der erfassten Daten dazu ermächtigt, einen Eingriff von hoher Intensität vorzunehmen.

102

Das nordrhein-westfälische Polizeigesetz sieht außer dem allgemein zu beachtenden Verhältnismäßigkeitsgrundsatz (vgl. § 2 PolG NW 1990) keine Begrenzung des Umfangs der erfassten Daten vor. Eine solche ergibt sich auch mittelbar weder aus einer BegrenzungBVerfGE 115, 320 (349) BVerfGE 115, 320 (350)der Art der erfassten Daten noch aus einer Begrenzung des Adressatenkreises. Denn die Übermittlung kann nach dem Wortlaut von § 31 Abs. 1 PolG NW 1990 von allen öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereichs verlangt werden. Soweit nicht in den für diese Stellen geltenden bereichsspezifischen Regelungen abschließende Übermittlungsverbote vorgesehen sind, sind daher sämtliche Stellen erfasst, bei denen personenbezogene Daten vorhanden sind. Diese Weite der Zugriffsbefugnis entspricht auch der Zielsetzung der Rasterfahndung. Da Ansätze zur Rasterfahndung in jeder möglichen Richtung gefunden werden können, kann grundsätzlich fast jeder Datenbestand relevant werden.

103

Die Befugnis ermöglicht es daher vorbehaltlich der Einschränkung des § 31 Abs. 2 PolG NW 1990 und der allgemeinen Grenze der Verhältnismäßigkeit, alle bei irgendwelchen öffentlichen oder privaten Stellen über irgendeine Person vorhandenen Daten bei Bedarf bei einer Stelle zusammenzuführen und gegeneinander abzugleichen. Die der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten, durch welche auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen kann (vgl. BVerfGE 65, 1 [45]), werden dadurch ausgeschöpft.

104

Dadurch entsteht ein Risiko, dass das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat (vgl. BVerfGE 65, 1 [47]) umgangen wird. Denn eine solche Befugnis zur Zweckänderung kann im Ergebnis alle zu einem bestimmten Zeitpunkt bei öffentlichen oder privaten Stellen vorhandenen Daten zu einem für die Zwecke des § 31 PolG NW 1990 bereitstehenden Gesamtdatenbestand umfunktionieren. Dies vermag eine eigene Vorratsspeicherung all jener Daten im Ergebnis zu ersetzen, die ohnehin bei irgendeiner anderen Stelle vorhanden sind.

105

Auch nähert sich die Zugriffsbefugnis des § 31 PolG NW 1990 angesichts der Menge und Vielfalt der personenbezogenen Daten, die heute -- bei allen öffentlichen oder privaten Stellen zusammengenommen -- über nahezu jede Person vorhanden sind, der von der Verfassung nicht zugelassenen Möglichkeit zumindest an, dass Daten mit anderen Datensammlungen zu einem teilweise oder weitgeBVerfGE 115, 320 (350)BVerfGE 115, 320 (351)hend vollständigen Persönlichkeitsbild zusammengefügt werden (vgl. BVerfGE 65, 1 [42]). Insbesondere sind auch sämtliche Datenbestände privater Stellen ("Stellen außerhalb des öffentlichen Bereichs") betroffen, in denen sich ein ganz wesentlicher Anteil aller gespeicherten personenbezogenen Daten befindet. So führen etwa die Kundenkartensysteme, die in vielen Kaufhäusern eingeführt sind, dazu, dass detaillierte Informationen über das private Einkaufsverhalten der Inhaber solcher Karten -- aber auch über ihren Aufenthaltsort und anderes -- bei nichtöffentlichen Stellen gespeichert sind. Auch wenn die Zugriffsbefugnis des § 31 PolG NW 1990 aus verfassungsrechtlichen Gründen so auszulegen ist, dass sie keine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger erlaubt -- dies wäre selbst in der Anonymität statistischer Erhebungen unzulässig (vgl. BVerfGE 65, 1 [53]) --, können die Erhebung und Verknüpfung entsprechender Daten der Erstellung eines Persönlichkeitsprofils nahe kommen und dadurch einen besonders intensiven Grundrechtseingriff ermöglichen.

106
(d) Auf die Intensität des Eingriffs wirken sich ferner etwaige aus der Rasterfahndung resultierende weitere Folgen für die Betroffenen aus.

107
Das Gewicht informationsbezogener Grundrechtseingriffe richtet sich auch danach, welche Nachteile den Betroffenen aufgrund der Eingriffe drohen oder von ihnen nicht ohne Grund befürchtet werden (vgl. BVerfGE 100, 313 [376]; 107, 299 [320]). So kann die Übermittlung und Verwendung von Daten für die davon Betroffenen das Risiko begründen, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden (vgl. BVerfGE 107, 299 [321]). Auch können informationsbezogene Ermittlungsmaßnahmen im Falle ihres Bekanntwerdens eine stigmatisierende Wirkung für die Betroffenen haben und so mittelbar das Risiko erhöhen, im Alltag oder im Berufsleben diskriminiert zu werden.

108
Beides trifft auf die mit der Rasterfahndung verbundenen Grundrechtseingriffe zu.BVerfGE 115, 320 (351)

109
BVerfGE 115, 320 (352)(aa) Die Rasterfahndung begründet für die Personen, in deren Grundrechte sie eingreift, ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Dies hat etwa der Verlauf der nach dem 11. September 2001 durchgeführten Rasterfahndung gezeigt. So sind nach einem Pressebericht aufgrund der Ergebnisse dieser Rasterfahndung in Hamburg 140 ausländische Studenten von der Polizei zu "Gesprächen" vorgeladen worden (vgl. Frankfurter Rundschau vom 22. Januar 2002). Ein Sprecher der Hamburger Polizei habe bestätigt, dass sich das Vorgehen -- welches nicht bedeute, dass die Personen beschuldigt oder verdächtigt seien -- gegen männliche, in Hamburg studierende Personen bestimmter Herkunft und Altersgruppen richte. Die Vorgeladenen seien aufgefordert worden, zu den Gesprächen im Polizeipräsidium unter anderem Ausweisdokumente, Studienbescheinigungen aller besuchten Hochschulen, Mietverträge, Arbeitsbescheinigungen und Praktikumsunterlagen, Dokumente über Reisen, Bankkonto-Unterlagen und Bescheinigungen über Vereinsmitgliedschaften mitzubringen. Die Betroffenen hätten der Vorladung zwar nicht folgen müssen. Doch seien sie in solchen Fällen auf andere Weise überprüft worden (vgl. a.a.O.; siehe auch Hamburgischer Datenschutzbeauftragter [Hrsg.], 19. Tätigkeitsbericht 2002/2003, 2004, S. 63, wonach das Landeskriminalamt die dreistellige Zahl der "Trefferfälle" der Rasterfahndung mit den üblichen Ermittlungsmethoden -- zum Beispiel Befragung von Betroffenen, Umfelderkundungen -- abgearbeitet hat).

110
(bb) Ferner kann die Tatsache einer nach bestimmten Kriterien durchgeführten polizeilichen Rasterfahndung als solche -- wenn sie bekannt wird -- eine stigmatisierende Wirkung für diejenigen haben, die diese Kriterien erfüllen. Das kann insbesondere dann der Fall sein, wenn die Rasterfahndung -- wie nach § 31 Abs. 1 PolG NW 1990 grundsätzlich möglich -- an die besonderen persönlichkeitsbezogenen Merkmale des Art. 3 Abs. 3 GG oder des Art. 140 GG in Verbindung mit Art. 136 Abs. 3 WRV anknüpft. Auch dort, wo keine Diskriminierung wegen der in Art. 3 Abs. 3 GG aufgeführten Merkmale vorliegt, ist nicht nur die verfassungsrechtliche Bindung an den Gleichheitssatz umso enger (stRspr; vgl. nur BVerfGE 92, 26 [51]), sondern auch die Intensität eines mit der UngleichbehandBVerfGE 115, 320 (352)BVerfGE 115, 320 (353)lung verbundenen Grundrechtseingriffs -- hier in das Grundrecht auf informationelle Selbstbestimmung -- umso höher, je mehr sich die Merkmale, nach denen staatliche Maßnahmen differenzieren, den in Art. 3 Abs. 3 GG genannten annähern.

111
So fällt etwa für die Rasterfahndungen, die nach dem 11. September 2001 durchgeführt wurden, im Hinblick auf deren Eingriffsintensität ins Gewicht, dass sie sich gegen Ausländer bestimmter Herkunft und muslimischen Glaubens richten, womit stets auch das Risiko verbunden ist, Vorurteile zu reproduzieren und diese Bevölkerungsgruppen in der öffentlichen Wahrnehmung zu stigmatisieren (vgl. Limbach, Ist die kollektive Sicherheit Feind der individuellen Freiheit?, 2002, S. 10). Insbesondere die kaum vermeidbaren Nebeneffekte einer nach der Zugehörigkeit zu einer Religion differenzierenden und alle Angehörigen dieser Religion pauschal erfassenden Rasterfahndung erhöhen das Gewicht der mit ihr verbundenen Grundrechtseingriffe und damit die von Verfassungs wegen an ihre Rechtfertigung zu stellenden Anforderungen. Das wirkt sich auf die Eingriffsintensität der gesetzlichen Ermächtigung des § 31 Abs. 1 PolG NW 1990 aus, die eine nach derartigen Kriterien differenzierende Rasterfahndung ermöglicht.

112
(e) Die Intensität des Eingriffs wird ferner davon beeinflusst, dass die gesetzliche Regelung nur für einen Teil der Betroffenen eine individuelle Benachrichtigung und dies erst nach Abschluss der Rasterfahndung vorsieht. Die Heimlichkeit einer staatlichen Eingriffsmaßnahme führt zur Erhöhung ihrer Intensität (vgl. BVerfGE 107, 299 [321]; BVerfG, NJW 2006, S. 976 [981]). Eine individuelle Benachrichtigung der Betroffenen nach Abschluss der Rasterfahndung schreibt § 31 Abs. 5 Satz 1 PolG NW 1990 nur für diejenigen Personen vor, gegen die weitere Maßnahmen durchgeführt werden, und auch für diese nur dann, wenn dies ohne Gefährdung des Zwecks der weiteren Datennutzung erfolgen kann. Die Unterrichtung unterbleibt nach § 31 Abs. 5 Satz 2 PolG NW 1990, wenn wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden ist.BVerfGE 115, 320 (353)

113
BVerfGE 115, 320 (354)Die in § 31 Abs. 4 Satz 1 PolG NW 1990 vorgesehene richterliche Anordnung reduziert zwar die Heimlichkeit der Maßnahme, sofern es -- wie im vorliegenden Fall (vgl. AG Düsseldorf, DuD 2001, S. 754) -- zu einer Veröffentlichung kommt. Dadurch können potentielle Betroffene erkennen, dass sie zu dem von der Rasterfahndung erfassten Personenkreis gehören und gegebenenfalls -- wie der Beschwerdeführer im vorliegenden Fall -- Rechtsschutz beanspruchen. Jedoch ist eine derartige Veröffentlichung gesetzlich nicht vorgeschrieben. Kommt es anders als hier nicht zur Veröffentlichung, bleibt die Maßnahme ohne eine individuelle Benachrichtigung dem Einzelnen verborgen.

114
(f) Ins Gewicht fällt auch, dass die von der Rasterfahndung Betroffenen nicht durchgängig anonym bleiben (vgl. BVerfGE 100, 313 [381]; 107, 299 [320 f.]). Anonymität besteht jedenfalls für diejenigen Personen nicht, deren Daten nach Abschluss der Gesamtmaßnahme weiterhin in der Ergebnisdatenmenge enthalten sind. Der Personenbezug der Daten wird bei diesen Personen durchgehend gerade zu dem Zweck erhalten, weitere Ermittlungsmaßnahmen gegen sie zu ermöglichen.

115
(g) Von Bedeutung ist schließlich auch, dass § 31 Abs. 1 PolG NW 1990 verdachtslose Grundrechtseingriffe mit großer Streubreite vorsieht.

116
(aa) Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind -- bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben -- weisen grundsätzlich eine hohe Eingriffsintensität auf (vgl. BVerfGE 100, 313 [376, 392]; 107, 299 [320 f.]; 109, 279 [353]; 113, 29 [53]; 113, 348 [383]). Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können (vgl. BVerfGE 65, 1 [42]; 113, 29 [46]). Ein von der Grundrechtsausübung abschreckender Effekt muss nicht nur zum SchutzeBVerfGE 115, 320 (354) BVerfGE 115, 320 (355)der subjektiven Rechte der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird dadurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist (vgl. BVerfGE 113, 29 [46]). Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen (vgl. BVerfGE 107, 299 [328]).

117
(bb) Bei der Rasterfahndung gemäß § 31 Abs. 1 PolG NW 1990 handelt es sich um einen verdachtslosen Eingriff. Die Vorschrift begründet Eingriffsbefugnisse gegen so genannte Nichtstörer, setzt also nicht voraus, dass der Adressat der Eingriffsmaßnahme für die Gefahr verantwortlich ist. Es können nach der Gesetzesfassung alle Personen einbezogen werden, welche die Auswahlkriterien erfüllen, ohne dass es Anforderungen an die Nähe dieser Personen zur Gefahr oder zu verdächtigen Personen gibt. Auch die nach der Rasterung anhand weiterer Kriterien verbleibenden Personen muss dabei noch kein konkreter Störerverdacht treffen. Ob die betroffenen Personen Tatverdächtige oder Störer sind oder nicht, soll in diesen Fällen vielmehr gerade herausgefunden werden, sei es bereits durch die Rasterung anhand weiterer Kriterien, sei es erst durch die sich anschließenden konventionellen personenbezogenen Ermittlungsmaßnahmen.

118
Die Rasterfahndung ist "Verdachts-" oder "Verdächtigengewinnungseingriff" (vgl. Gusy, KritVj 2002, S. 474 [483]; Brugger, Freiheit und Sicherheit, 2004, S. 98 f.) insbesondere dann, wenn sie -- wie im vorliegenden Fall -- zur Aufdeckung von so genannten terroristischen Schläfern führen soll. Da solche "Schläfer" sich gerade durch ihr völlig angepasstes und damit unauffälliges Vorgehen auszeichnen sollen, fehlt es bei ihnen definitionsgemäß an konkreten Anhaltspunkten für ein Verhalten, das auf eine potentielle Störereigenschaft hindeuten könnte. Für eine Rasterfahndung, durch die solche Personen aufgefunden werden sollen, müssen daher relativ unspezifische Annahmen über Täterprofile entwickelt und entsprechend unspezifische Suchkriterien eingesetzt werden, mit der Folge, dass die Suche in Abkehr von traditionellen polizeirechtlichenBVerfGE 115, 320 (355) BVerfGE 115, 320 (356)Strukturen weit in das Vorfeld eines konkreten Störerverdachts verlagert wird. Die Situation unterscheidet sich insofern grundlegend von einer Fahndung nach einem prinzipiell bekannten Täterkreis mit bestimmten, vom Üblichen abweichenden Verhaltensmerkmalen, wie zum Beispiel der Barzahlung von Stromrechnungen, auf die bei der Fahndung nach gesuchten RAF-Terroristen unter anderem abgestellt worden war (vgl. zur damals eingesetzten Rasterfahndung Herold, RuP 1985, S. 84 [91, 93]).

119
Gegenüber den für die frühere Rasterfahndung typischen Konstellationen wird die Verdachtslosigkeit der Maßnahme noch erhöht, wenn gerade die Unauffälligkeit und Angepasstheit des Verhaltens zu einem maßgeblichen Kriterium der Suche erhoben wird. Das wird an der im vorliegenden Fall vorgenommenen bundesweit koordinierten Rasterfahndung deutlich. Weder für die etwa 5,2 Mio. Personen, deren Datensätze an das Polizeipräsidi-

um Düsseldorf übermittelt wurden, noch für die etwa 32.000 Personen, deren Daten nach Angaben des Bundesbeauftragten für den Datenschutz insgesamt in die bundesweite Datei "Schläfer" aufgenommen wurden, gab es auch nur ansatzweise konkrete Anhaltspunkte dafür, dass es sich gerade bei ihnen um so genannte Schläfer handeln könnte oder sie mit solchen in Kontakt stehen würden. Auch die nach dem vorgesehenen Abgleich durch das Bundeskriminalamt verbliebenen Personen, deren Daten sich zugleich in den Abgleichsdateien fanden, traf allein aufgrund dessen noch kein konkreter Störerverdacht. Vielmehr diente die Rasterfahndung auch in Bezug auf sie lediglich dazu, den Kreis derer einzuengen, bei denen möglicherweise weitere Ermittlungen erst zur Begründung eines derartigen Verdachtes führen sollten.

120

(cc) Die Rasterfahndung kann, wie die Anzahl der im vorliegenden Fall erfassten Personen zeigt, auch durch eine außerordentlich hohe Streubreite geprägt sein.

121

(α) Als Fahndungsmethode weist die Rasterfahndung die Vorteile auf, die automatisierte, rechnergestützte Operationen generell mit sich bringen, ermöglicht also die Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit. Ein herkömmliches Verfahren, die nach dem Modell abgestufter ErBVerfGE 115, 320 (356)BVerfGE 115, 320 (357)kenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer bislang unbekannten Durchschlagskraft versehen (vgl. Rogall, in: Duttge u.a. [Hrsg.], Gedächtnisschrift Schlüchter, 2002, S. 611 [617]; Welp, in: Erichsen u.a. [Hrsg.], Recht der Persönlichkeit, 1996, S. 389 f.). In grundrechtlicher Hinsicht führt die neue Qualität der polizeilichen Ermittlungsmaßnahme zu einer erhöhten Eingriffsintensität.

122

(β) Für die Beurteilung der Angemessenheit ist die Zahl nicht nur derjenigen Personen relevant, die von der Rasterfahndung in einer einen Grundrechtseingriff auslösenden Weise betroffen sind, sondern es ist -- aufgrund der objektiven Bedeutung des Grundrechts -- auch die Gesamtzahl der erfassten Personen zu berücksichtigen (vgl. BVerfGE 107, 299 [328]).

123

Werden Daten nach relativ unspezifischen Kriterien zusammengestellt, kann von der Rasterfahndung eine sehr große Ausgangsmenge von Personen betroffen sein, die aus ex ante-Sicht Unverdächtige oder Nichtstörer sind. Auch die nach einem ersten Abgleich verbleibende Gruppe von Trägern der gesuchten Merkmale kann -- wie im vorliegenden Fall -- sehr viele Personen umfassen und wird jedenfalls in der ganz überwiegenden Mehrzahl selbst aus der ex post-Sicht aus Nichtstörern bestehen.

124

(3) Der insofern mit der Rasterfahndung verbundene Eingriff ist angesichts der hochrangigen Verfassungsgüter, deren Schutz § 31 Abs. 1 PolG NW 1990 dient, zwar noch nicht als solcher unverhältnismäßig. Er ist jedoch nur dann angemessen, wenn der Gesetzgeber rechtsstaatliche Anforderungen dadurch wahrt, dass er den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für die bedrohten Rechtsgüter an vorsieht.

125

(a) Der Staat darf und muss terroristischen Bestrebungen -- etwa solchen, die die Zerstörung der freiheitlichen demokratischen Grundordnung zum Ziel haben und die planmäßige Vernichtung von Menschenleben als Mittel zur Verwirklichung dieses Vorhabens einsetzen -- mit den erforderlichen rechtsstaatlichen Mitteln wirksam entgegentreten (vgl. BVerfGE 49, 24 [56]). Auf die rechtsstaatlichen Mittel hat sich der Staat unter dem Grundgesetz jedoch auch zu beschränken.BVerfGE 115, 320 (357)

126

BVerfGE 115, 320 (358)Das Grundgesetz enthält einen Auftrag zur Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Ordnung unter Einhaltung der Regeln des Rechtsstaats (vgl. BVerfGE 111, 147 [158]; BVerfGK 2, 1 [5]). Daran, dass er auch den Umgang mit seinen Gegnern den allgemein geltenden Grundsätzen unterwirft, zeigt sich gerade die Kraft dieses Rechtsstaats (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 1. Mai 2001 -- 1 BvQ 22/01 --, NJW 2001, S. 2076 [2077]).

127

Das gilt auch für die Verfolgung der fundamentalen Staatszwecke der Sicherheit und des Schutzes der Bevölkerung. Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Das schließt nicht nur die Verfolgung des Zieles absoluter Sicherheit aus, welche ohnehin faktisch kaum, jedenfalls aber nur um den Preis einer Aufhebung der Freiheit zu erreichen wäre. Das Grundgesetz unterwirft auch die Verfolgung des Zieles, die nach den tatsächlichen Umständen größtmögliche Sicherheit herzustellen, rechtsstaatlichen Bindungen, zu denen insbesondere das Verbot unangemessener Eingriffe in die Grundrechte als Rechte staatlicher Eingriffsabwehr zählt.

128

In diesem Verbot finden auch die Schutzpflichten des Staates ihre Grenze. Die Grundrechte sind dazu bestimmt, die Freiheitssphäre des Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern; sie sind Abwehrrechte des Bürgers gegen den Staat (vgl. BVerfGE 7, 198 [204 f.]). Die Funktion der Grundrechte als objektive Prinzipien und der sich daraus ergebenden Schutzpflichten (vgl. BVerfGE 96, 56 [64]) besteht in der prinzipiellen Verstärkung ihrer Geltungskraft, hat jedoch ihre Wurzel in dieser primären Bedeutung (vgl. BVerfGE 50, 290 [337]).

129
Bei der Wahl der Mittel zur Erfüllung einer Schutzpflicht ist der Staat daher auf diejenigen Mittel beschränkt, deren Einsatz mit der Verfassung in Einklang steht (vgl. BVerfG, NJW 2006, S. 751 [760]). Der staatliche Eingriff in den absolut geschützten Achtungsanspruch des Einzelnen auf Wahrung seiner Würde (vgl. BVerfGE 109, 279 [313]) ist ungeachtet des Gewichts der betroffenen VerfasBVerfGE 115, 320 (358)BVerfGE 115, 320 (359)sungsgüter stets verboten (vgl. BVerfG, NJW 2006, S. 751 [757 ff.]). Aber auch im Rahmen der Abwägung nach Maßgabe des Grundsatzes der Verhältnismäßigkeit im engeren Sinne dürfen staatliche Schutzpflichten nicht dazu führen, dass das Verbot unangemessener Grundrechtseingriffe unter Berufung auf grundrechtliche Schutzpflichten leer läuft, so dass in der Folge allenfalls ungeeignete oder unnötige Eingriffe abgewehrt werden könnten.

130
(b) Aus dem Gebot der Verhältnismäßigkeit im engeren Sinne kann unter bestimmten Voraussetzungen sogar die vollständige Unzulässigkeit der Vornahme bestimmter Grundrechtseingriffe zu Zwecken persönlichkeitsbezogener Ermittlungen im Bereich der inneren Sicherheit folgen. So ist der Einsatz der Befugnisse des Bundesnachrichtendienstes, zur so genannten strategischen Kontrolle verdachtslos Fernmeldeverkehre zu überwachen und sie durch Abgleich mit Suchbegriffen auszuwerten, für Zwecke der personenbezogenen Risikoabwehr im Bereich der inneren Sicherheit in jedem Falle unverhältnismäßig und damit verfassungswidrig (vgl. BVerfGE 67, 157 [157, 180 f.]; 100, 313 [389]). Lediglich eine Verwertung von Zufallsfunden im Rahmen einer nachträglichen Zweckänderung kann unter engsten Voraussetzungen an die Verhältnismäßigkeit vorgesehen werden (vgl. BVerfGE 100, 313 [389 ff.]).

131
(c) Für die Rasterfahndung gemäß § 31 Abs. 1 PolG NW 1990 folgt aus dem Verhältnismäßigkeitsgrundsatz kein Verbot, das Grundrechtseingriffe zu persönlichkeitsbezogenen Ermittlungszwecken ausnahmslos ausschlösse. Allerdings gleicht die Befugnis zur Rasterfahndung den zu Zwecken der strategischen Kontrolle vorgenommenen Eingriffen in das Fernmeldegeheimnis insofern, als auch sie vollständig verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vorsieht. Auch handelt es sich bei ihr nicht lediglich um eine Ermächtigung zur nachträglich zweckändernden Verwertung von Zufallsfunden. Bei ihr sollen die Erkenntnisse vielmehr von vornherein gerade zu dem Zweck zusammengeführt und ausgewertet werden, einen Kreis von potentiellen Verdächtigen zu bestimmen, gegen den dann weitere personenbezogene ErmittlungsBVerfGE 115, 320 (359)BVerfGE 115, 320 (360)maßnahmen gerichtet werden können. Übermittlung, Zusammenführung und Abgleich solcher Daten stellen eigenständige Eingriffe dar, die -- anders als im Falle der strategischen Überwachung -- von vornherein zu personenbezogenen Ermittlungszwecken erfolgen.

132
(d) Das Gewicht der mit der Durchführung einer Rasterfahndung einhergehenden Grundrechtseingriffe, deren Voraussetzungen zudem gesetzlich nicht eng umschrieben worden sind, ist so hoch, dass der Gesetzgeber die Maßnahme zum Schutz der hochrangigen Rechtsgüter des § 31 Abs. 1 PolG NW 1990 nur bei Vorliegen einer konkreten Gefahr vorsehen darf.

133
Der Gesetzgeber ist bei der Gestaltung von Eingriffsbefugnissen nicht zwingend an die mit dem überkommenen Gefahrenbegriff verbundenen polizeirechtlichen Eingriffsgrenzen gebunden. Er darf sie bei Eingriffen der hier vorliegenden Intensität jedoch nur bei Wahrung besonderer Anforderungen an die Verhältnismäßigkeit unterschreiten. Diese sind im Falle eines vollständig verdachtslosen Grundrechtseingriffs von der Art der Rasterfahndung nicht erfüllt. Die Rasterfahndung darf daher von Verfassungs wegen erst bei Vorliegen einer konkreten Gefahr eingesetzt werden.

134
(aa) Die Verfassung hindert den Gesetzgeber nicht grundsätzlich daran, die traditionellen rechtsstaatlichen Bindungen im Bereich des Polizeirechts auf der Grundlage einer seiner Prärogative unterliegenden Feststellung neuartiger oder veränderter Gefährdungs- und Bedrohungssituationen fortzuentwickeln. Die Balance zwischen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch von ihm nicht grundlegend verschoben werden.

135
Im Hinblick auf den Verhältnismäßigkeitsgrundsatz im engeren Sinne hat der Gesetzgeber die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits, wie der Einschreitschwelle, der geforderten Tatsachenbasis und dem Gewicht der geschützten Rechtsgüter, zu wahren (vgl. BVerfGE 100, 313 [392 ff.]). Je gewichtiger die drohende oder erfolgte Rechtsgutbeeinträchtigung und je weniger gewichtig der Grundrechtseingriff ist, um den es sich handelt, desto geringer darf dieBVerfGE 115, 320 (360) BVerfGE 115, 320 (361)Wahrscheinlichkeit sein, mit der auf eine drohende oder erfolgte Verletzung des Rechtsguts geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die dem Verdacht zugrunde liegen (vgl. BVerfGE 100, 313 [392]; 110, 33 [60]; 113, 348 [386]). Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose dürfen allerdings nicht beliebig herabgesenkt werden, sondern müssen auch in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung und zur Aussicht auf den Erfolg des beabsich-

tigten Rechtsgüterschutzes stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden. Auch muss als Voraussetzung eines schweren Grundrechtseingriffs gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen besitzen (vgl. BVerfGE 113, 348 [386]). Insbesondere lässt die Verfassung grundrechtseingreifende Ermittlungen "ins Blaue hinein" nicht zu (vgl. BVerfGE 112, 284 [297]; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 6. April 1989 -- 1 BvR 33/87 --, NJW 1990, S. 701 [702]).

136

Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf (vgl. BVerfGE 100, 313 [383 f.]; 109, 279 [350 ff.]). So ist eine gesetzliche Befugnis zum Verbot oder zur Auflösung von Versammlungen nur dann verhältnismäßig, wenn eine unmittelbare, aus erkennbaren Umständen herleitbare Gefährdung der geschützten Rechtsgüter gegeben ist (vgl. BVerfGE 69, 315 [353 f.]). Ob ein Grundrechtseingriff zur Abwehr künftig drohender Rechtsgutbeeinträchtigungen auch im Vorfeld konkreter Gefahren verhältnismäßig sein kann, hängt nicht nur davon ab, ob eine hinreichende Aussicht darauf besteht, dass der Eingriff Erfolg verspricht (zum Erfordernis der Erfolgseignung BVerfGE 42, 212 [220]; 96, 44 [51]; BVerfG, NJW 2006, S. 976 [982]), sondern auch davon, welche Anforderungen die EingriffsBVerfGE 115, 320 (361)BVerfGE 115, 320 (362)norm hinsichtlich der Nähe der betroffenen Personen zur fraglichen Rechtsgutbedrohung vorsieht (vgl. BVerfGE 100, 313 [395]; 107, 299 [322 f., 329]; 110, 33 [60 f.]; 113, 348 [385 ff., 389]). Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.

137

(bb) Nach diesen Maßstäben darf eine Rasterfahndung nicht schon im Vorfeld einer konkreten Gefahr ermöglicht werden, denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können.

138

Die Rasterfahndung nach dem nordrhein-westfälischen Polizeirecht zeichnet sich gegenüber anderen personenbezogenen Ermittlungsmaßnahmen im Vorfeld konkreter Gefahren, die das Bundesverfassungsgericht nicht von vornherein als unzulässig angesehen hat, dadurch aus, dass sie keinerlei tatsachengestützte Verbindung zu einer konkret für die Bedrohungssituation verantwortlichen Person voraussetzt, gegen welche die Ermittlungen gerichtet werden könnten. Die zur "Verdächtigengewinnung" eingesetzte Maßnahme dient weder der weiteren Ermittlung gegen konkrete Beschuldigte (vgl. dazu BVerfGE 107, 299 [314 ff., 326 ff.]) noch der weiteren Verdichtung eines bereits in sonstiger Weise auf bestimmte Personen fokussierten Risikoverdachts (vgl. dazu BVerfGE 100, 313 [395]; 110, 33 [58 ff., 61]; 113, 348 [375 ff., 378 ff., 383]).

139

Die vom Bundesverfassungsgericht hervorgehobene rechtsstaatliche Maßgabe, nach welcher auch bei fehlendem polizeirechtlichem Störer- oder strafprozessrechtlichem Straftatverdacht eine durch eine hinreichende Tatsachenbasis belegte Nähebeziehung zu künftigen Rechtsgutverletzungen bestehen muss, läuft bei der Rasterfahndung vielmehr ins Leere. Denn eine Tatsachenkette zu einem in irgendeiner Hinsicht konkretisierten personenbezogenen Verdacht besteht bei ihr nicht. Das rechtsstaatliche Defizit, das mit dem für die Rasterfahndung typischen Verzicht auf eine Nähebeziehung zwischen dem gefährdeten Rechtsgut und den von dem GrundBVerfGE 115, 320 (362)BVerfGE 115, 320 (363)rechtseingriff Betroffenen verbunden ist, muss auf andere Weise kompensiert werden, um die Uferlosigkeit der Ermächtigung auszuschließen. Vorliegend hat der Gesetzgeber nicht den Weg gewählt, die zum Rechtsgüterschutz einsetzbare Maßnahme so zu umschreiben, dass die möglichen Eingriffe keine nennenswerte Beeinträchtigung der Betroffenen bewirken. Auch ist die Eingriffsbefugnis nicht eng begrenzt worden. Dies genügt verfassungsrechtlichen Anforderungen nur, wenn die Ermächtigung jedenfalls eine konkrete Gefahr für das Rechtsgut voraussetzt.

140

(cc) Die für die Rasterfahndung geltende Eingriffsschwelle muss von Verfassungs wegen allerdings nicht notwendig eine gegenwärtige Gefahr im überkommenen Sinn sein, darf aber die einer konkreten Gefahr nicht unterschreiten.

141

(α) § 31 PolG NW 1990 greift auf das traditionelle Tatbestandselement rechtsstaatlicher Begrenzung der Inanspruchnahme von Nichtstörern zurück, die gegenwärtige Gefahr. Gegenwärtig ist eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses entweder bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht (vgl. beispielsweise § 2 Nr. 1 Buchstabe b des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung [Nds. SOG]). Dies genügt den verfassungsrechtlichen Anforderungen an eine Ermächtigung zur Rasterfahndung.

142

Das Vorliegen einer gegenwärtigen Gefahr in diesem Sinne ist jedoch nicht von Verfassungs wegen geboten. Auch wenn nicht von vornherein ausgeschlossen werden kann, dass die Rasterfahndung im Einzelfall binnen

kurzer Zeit Erfolg haben kann, führt das gesetzliche Erfordernis eines in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit zu erwartenden Schadenseintritts angesichts des mit der Rasterfahndung regelmäßig verbundenen Aufwandes doch dazu, dass diese in den meisten Fällen, in welchen diese Voraussetzung erfüllt ist, zu spät kommen wird, um noch wirksam zu sein. Eine derart weit reichende Beschränkung dieses Fahndungsmittels ist angesichts des hohen Ranges der in § 31 Abs. 1 PolG NW 1990 genannten Rechtsgüter zur Wahrung der Verhältnismäßigkeit nicht gefordert.BVerfGE 115, 320 (363)

143

BVerfGE 115, 320 (364)(β) Ausreichend ist es vielmehr, wenn der Gesetzgeber die Zulässigkeit der Rasterfahndung an das Erfordernis einer konkreten Gefahr für die betroffenen Rechtsgüter knüpft. Vorausgesetzt ist danach eine Sachlage, bei der im konkreten Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für diese Rechtsgüter eintreten wird (vgl. etwa § 2 Nr. 1 Buchstabe a Nds. SOG). Den mit der Anwendung einer solchen Ermächtigung betrauten Instanzen ist es allerdings verfassungsrechtlich verwehrt, den polizeirechtlichen Gefahrenbegriff unter Ablösung von diesen Anforderungen auszulegen und dadurch die Gefahrenschwelle unter das für eine Rasterfahndung verfassungsrechtlich geforderte Maß herabzusenken.

144

Die für die Feststellung einer konkreten Gefahr erforderliche Wahrscheinlichkeitsprognose muss sich auf Tatsachen beziehen. Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen nicht aus (vgl. BVerfGE 44, 353 [381 f.]; 69, 315 [353 f.]).

145

(γ) Eine konkrete Gefahr in diesem Sinne kann auch eine Dauergefahr sein. Bei einer solchen besteht die hinreichende Wahrscheinlichkeit des Schadenseintritts über einen längeren Zeitraum hinweg zu jedem Zeitpunkt. Für die Feststellung einer solchen Dauergefahr gelten jedoch ebenfalls die mit dem Erfordernis einer konkreten Gefahr verbundenen Anforderungen an die hinreichende Wahrscheinlichkeit des Schadenseintritts sowie an die konkrete Tatsachenbasis der Wahrscheinlichkeitsprognose.

146

Für die Annahme einer etwa von so genannten terroristischen Schläfern ausgehenden konkreten Dauergefahr sind daher hinreichend fundierte konkrete Tatsachen erforderlich. Außenpolitische Spannungslagen, die von terroristischen Gruppierungen zum Anlass von Anschlägen gewählt werden können, gibt es immer wieder, und sie können lange anhalten. Insofern ist es praktisch nie ausgeschlossen, dass terroristische Aktionen auch Deutschland treffen oder dort vorbereitet werden können. Eine derartige allgemeine Bedrohungslage, wie sie spätestens seit dem 11. September 2001, also seit nunmehr über vier Jahren, praktisch ununterbrochen bestanden hat, oder außenpolitische Spannungslagen reichen für die AnBVerfGE 115, 320 (364)BVerfGE 115, 320 (365)ordnung einer Rasterfahndung nicht aus. Der durch die Rasterfahndung bewirkte Eingriff in das Recht auf informationelle Selbstbestimmung setzt vielmehr das Vorliegen weiterer Tatsachen voraus, aus denen sich eine konkrete Gefahr ergibt, etwa weil tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge oder dafür bestehen, dass sich in Deutschland Personen für Terroranschläge bereithalten, die in absehbarer Zeit in Deutschland selbst oder andernorts verübt werden sollen.

147

(δ) Die Begrenzung auf eine konkrete Gefahr ist im Übrigen auch als Grundlage zur Bestimmung der Verhältnismäßigkeit der Rasterfahndung im Einzelfall sowie zur näheren Konkretisierung der ergänzenden -- hier nicht zu überprüfenden -- verfahrensmäßigen und organisatorischen Voraussetzungen der Durchführung der Maßnahme geboten. Ohne diese Begrenzung wäre es nicht möglich, die weiteren Anforderungen so zu konkretisieren, dass rechtsstaatliche Bestimmtheitsgrundsätze gewahrt sind.

148

c) Die Ermächtigung des § 31 Abs. 1 PolG NW 1990 genügt dem Gebot der verfassungsrechtlichen Normenbestimmtheit und Normenklarheit, sofern ihr Anwendungsbereich im bezeichneten Sinne verstanden wird.

149

aa) Ermächtigungen zu Grundrechtseingriffen bedürfen einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht (vgl. BVerfGE 110, 33 [53]). Bei Eingriffen in das Grundrecht auf informationelle Selbstbestimmung -- wie auch in die Spezialgrundrechte der Art. 10 und 13 GG -- hat der Gesetzgeber insbesondere den Verwendungszweck der Daten bereichsspezifisch und präzise zu bestimmen (vgl. BVerfGE 65, 1 [46]; 110, 33 [70]; 113, 29 [51]). Gemäß § 31 Abs. 1 PolG NW 1990 dient die Datenübermittlung dem Zweck des automatisierten Abgleichs mit anderen Datenbeständen, soweit dies zur Abwehr bestimmter Gefahren, nämlich für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person, erforderlich ist. Als Verwendungszweck ist damit der automatisierte Abgleich der übermittelten Daten mit anderen Datenbeständen zur Abwehr der in § 31 Abs. 1 PolG NW 1990 benannten Gefahren festgelegt. Das ist hinreichend.BVerfGE 115, 320 (365)

150

BVerfGE 115, 320 (366)Auch dem für Übermittlungsregelungen geltenden Gebot einer hinreichend sicher erschließbaren Kennzeichnung der Empfangsbehörden, einhergehend mit Regeln, welche die Übermittlung auf deren jeweiligen spezifischen Aufgabenbereich konzentrieren (vgl. hierzu BVerfGE 110, 33 [70]), ist nur genügt, wenn der Gefahrenbegriff zur Einschränkung der Ermächtigung verfügbar ist. Als Empfangsbehörde für

die übermittelten Daten ist die Polizei benannt. Der Verwendungszweck ist auf den Zweck der Abwehr von Gefahren für im Einzelnen benannte, hochwertige Schutzgüter der öffentlichen Sicherheit begrenzt, also auf einen Zweck, dessen Verfolgung zum spezifischen Aufgabenbereich der Polizeibehörden zählt (vgl. § 1 Abs. 1 Satz 1 PolG NW 1990).

151

§ 31 PolG NW 1990 ist unter den genannten Bedingungen auch insoweit hinreichend bestimmt, als nicht nur die ausdrücklich aufgezählten Typen von Daten, sondern nach Absatz 2 auch "andere für den Einzelfall benötigte Daten" verlangt und verarbeitet werden dürfen. Die Bestimmtheitsanforderungen sind insoweit gewahrt, weil der Begriff der "anderen für den Einzelfall benötigten Daten" unter Berücksichtigung des Normzwecks der Gefahrenabwehr und damit auch hinsichtlich der Feststellung, wozu die Daten "benötigt" werden, so konkretisiert werden kann, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleibt.

152

bb) Ohne die Begrenzung auf das Vorliegen einer konkreten Gefahr gäbe es demgegenüber keine hinreichenden Anhaltspunkte zur teleologischen Bestimmung der erfassbaren Daten, insbesondere soweit es sich um "andere für den Einzelfall benötigte Daten" handelt. Fehlt es an einer konkreten Gefahr, ist nicht mit verfassungsrechtlich hinreichender Bestimmtheit ermittelbar, unter welchen Bedingungen Daten "für den Einzelfall" benötigt werden. Wäre Bezugspunkt der Rasterfahndung etwa eine allgemeine Terrorismusgefahr und würde diese somit zum Bezugspunkt der Konkretisierung der Art der Daten, die von der Polizei benötigt werden, wäre eine nahezu grenzenlose Ermächtigung geschaffen. Es fehlten jegliche Anhaltspunkte für die Prüfung, ob die zu erhebenden Daten "für den Einzelfall benötigt" werden. Dies würde verfassungsrechtliche Bestimmtheitsanforderungen verletzen.BVerfGE 115, 320 (366), BVerfGE 115, 320 (367)

153

II.

Die angegriffenen Entscheidungen genügen den verfassungsrechtlichen Anforderungen nicht. Sie beruhen auf einer diesen Grundsätzen widersprechenden ausweitenden Auslegung des Begriffs der gegenwärtigen Gefahr in § 31 Abs. 1 PolG NW 1990 und damit im Ergebnis auf einer Umformung der Ermächtigung zu einer Vorfeldbefugnis. Dadurch erhält diese Vorschrift einen Inhalt, den auch der Gesetzgeber nicht ohne Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hätte bestimmen können.

154

1. Die Auslegung des einfachen Rechts und seine Anwendung auf den konkreten Fall sind zwar Sache der dafür zuständigen Fachgerichte und der Nachprüfung durch das Bundesverfassungsgericht grundsätzlich entzogen (stRspr; vgl. BVerfGE 18, 85 [92 f.]). Diese haben jedoch die Tragweite der von ihren Entscheidungen berührten Grundrechte interpretationsleitend zu berücksichtigen, damit deren wertsetzende Bedeutung auch auf der Rechtsanwendungsebene gewahrt bleibt (stRspr; vgl. BVerfGE 7, 198 [205 ff.]; 101, 361 [388]). Bedeutung und Tragweite der Grundrechte sind unter anderem dann verkannt, wenn ein Fachgericht einer Norm durch ausweitende Auslegung ihres Anwendungsbereichs einen Inhalt gibt, den auch der Gesetzgeber nicht ohne Grundrechtsverstoß hätte bestimmen dürfen, und die Anwendung der Vorschrift im konkreten Fall auf einer solchen Auslegung beruht (vgl. BVerfGE 81, 29 [31 f.]; 82, 6 [15 f.]).

155

2. So liegt es hier. Die angegriffenen Entscheidungen geben dem Begriff der gegenwärtigen Gefahr in § 31 Abs. 1 PolG NW 1990 einen Inhalt, mit welchem er den grundrechtlichen Anforderungen an eine Ermächtigung zur Rasterfahndung, zu denen das Vorliegen jedenfalls einer konkreten Gefahr gehört, nicht genügt.

156

a) Die bundesweit koordinierte Rasterfahndung nach dem 11. September 2001 hat den Gerichten Entscheidungen in einer neuartigen Gefährdungssituation abverlangt. Dies bewirkte Unsicherheit im Umgang mit den Ermächtigungsgrundlagen. Einzelne Fachgerichte hielten bei der Beurteilung der Rasterfahndungen an dem überkommenen Verständnis des Begriffs der gegenwärtigen GefahrBVerfGE 115, 320 (367) BVerfGE 115, 320 (368)fest und verneinten deren Vorliegen (vgl. OLG Frankfurt, NVwZ 2002, S. 626 [626 f.]; LG Wiesbaden, DuD 2002, S. 240 [241]; LG Berlin, DuD 2002, S. 175 [176 f.]). Hingegen senkten andere Gerichte die Anforderungen an die Schadenswahrscheinlichkeit unter Berufung auf die Größe des drohenden Schadens herab und bejahten davon ausgehend eine gegenwärtige Gefahr (vgl. OLG Düsseldorf, DuD 2002, S. 241 ff.; DuD 2002, S. 244 f.; KG Berlin, MMR 2002, S. 616 [617]; OVG Koblenz, NVwZ 2002, S. 1528; VG Mainz, DuD 2002, S. 303 [305]; AG Wiesbaden, DuD 2001, S. 752 [753]; AG Tiergarten, DuD 2001, S. 691 [692]). So gingen auch die Gerichte in den angegriffenen Entscheidungen vor. Die ihnen zugrunde liegende Auslegung des § 31 Abs. 1 PolG NW 1990 entspricht den verfassungsrechtlichen Maßstäben nicht.

157

b) Die angegriffenen Entscheidungen lassen außer Acht, dass die Verfassungsmäßigkeit der Anordnung an das Vorliegen zumindest einer konkreten Gefahr gebunden ist und der dafür geforderte Grad der Wahrscheinlichkeit einer Rechtsgutverletzung nicht nur mit Rücksicht auf die Größe eines möglichen Schadens, sondern auch im Hinblick auf die Schwere und Erfolgsaussichten des Eingriffs zu bestimmen ist, der zur Gefahrenabwehr eingesetzt wird. Aus den dargestellten verfassungsrechtlichen Gründen darf der mit der Rasterfahndung verbundene

Eingriff in das Grundrecht auf informationelle Selbstbestimmung einer völlig verdachtslosen Person nur erfolgen, wenn jedenfalls eine in konkreten Tatsachen begründete Gefahr gegeben ist, die Anlass für die Annahme schafft, dass auf der Grundlage der Ermittlung von Daten eines bestimmten Personenkreises Maßnahmen ergriffen werden können, die zur Abwehr dieser Gefahr beitragen.

158

Demgegenüber hat etwa das Landgericht es schon für hinreichend erachtet, dass "die Möglichkeit eines besonders gravierenden Schadenseintritts nicht ausgeschlossen" ist, und das Oberlandesgericht will eine nur "entfernte Möglichkeit eines Schadenseintritts" ausreichen lassen. Sind -- wie das Oberlandesgericht für die damalige Situation ausführt -- "konkrete Anzeichen für Terroranschläge in Deutschland nicht bekannt", sondern besteht lediglich eine auf Vermutungen beruhende "Möglichkeit solcher Anschläge", dann hanBVerfGE 115, 320 (368)BVerfGE 115, 320 (369)delt es sich bei der dennoch durchgeführten Rasterfahndung um eine Maßnahme im Vorfeld der Gefahrenabwehr, nicht aber um die Abwehr einer konkreten Gefahr. Dementsprechend hat das Oberlandesgericht im Rahmen seiner weiteren Ausführungen zur Verhältnismäßigkeit die auf Nichtstörer ausgerichtete Rasterfahndung ausdrücklich den Vorfeldbefugnissen der Polizei zugeordnet, die nicht mehr an die Abwehr konkreter Gefahren und das Störerprinzip anknüpften.

159

Die zur Begründung der derart herabgesenkten Wahrscheinlichkeitsanforderungen herangezogene Tatsachenbasis war vorliegend zu diffus, um eine konkrete Gefahr bejahen zu können. So wurden außen- und sicherheitspolitische Ausgangstatsachen angeführt, die zwar -- wie der Militärschlag der Vereinigten Staaten von Amerika in Afghanistan und die Drohung des Botschafters dieses Landes mit Vergeltungsschlägen -- Ausweitungen der militärischen Auseinandersetzung, gegebenenfalls auch terroristische Anschläge hätten verursachen können. Es gab jedoch keine über diese allgemeine Lage hinausgehenden Erkenntnisse über konkrete Gefährdungen oder speziell über Anschläge oder Anschlagsvorbereitungen gerade in Deutschland. Ebenso vermögen sowohl der nicht näher konkretisierte Hinweis auf 42 in Nordrhein-Westfalen befindliche, der Polizei bekannte Personen, die als Unterstützer oder Kontaktpersonen im Netzwerk Usama Bin Ladens "gälten", als auch die Benennung möglicher Anschlagsziele in Nordrhein-Westfalen lediglich die allgemein gegebene Möglichkeit eines terroristischen Anschlages zu unterstreichen. Darin liegen keine hinreichend konkreten Tatsachen, aus welchen die in irgendeiner Weise verdichtete Wahrscheinlichkeit einer Vorbereitung terroristischer Anschläge durch Personen hätte gefolgert werden können, die als terroristische "Schläfer" einzustufen gewesen wären und dementsprechend durch die Rasterfahndung aufgefunden hätten werden können.

160

Mit der Absenkung der Wahrscheinlichkeitsschwelle auf eine bloße Möglichkeit terroristischer Anschläge nehmen die Gerichte einen von Verfassungs wegen unzulässigen Verzicht auf das Vorliegen einer konkreten, also im einzelnen Fall gegebenen und durch hinreichende Tatsachen zu belegenden Gefahrenlage vor. Dies wird daBVerfGE 115, 320 (369)BVerfGE 115, 320 (370)durch bewirkt, dass die Gerichte die Bedrohungslage gleichwohl dem Begriff der Gefahr zuordnen, wodurch sie diesem einen Gehalt geben, der aus verfassungsrechtlichen Gründen nicht für eine Befugnis zur Rasterfahndung ausreicht.

161

3. Die angegriffenen Entscheidungen beruhen auf diesen verfassungsrechtlichen Mängeln. Denn es liegt nahe, dass die Gerichte bei Beachtung der verfassungsrechtlichen Anforderungen an die Auslegung des Begriffs der gegenwärtigen Gefahr in § 31 Abs. 1 PolG NW 1990 zu einem anderen Ergebnis gelangt wären. […]

**5) BVerfGE 129, 208 – TKÜ-Neuregelung**

*a) Sachverhalt*

Die zur gemeinsamen Entscheidung verbundenen Verfassungsbeschwerden betreffen Art. 1 und Art. 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. 12. 2007 (BGBl I, 3198; im Folgenden: Gesetz zur Neuregelung der Telekommunikationsüberwachung), mit denen einzelne Vorschriften der StPO geändert worden sind.

Die Bf. in den Verfahren 2 BvR 236/08 und 2 BvR 237/08 haben Verfassungsbeschwerden gegen Art. 1 und Art. 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung sowie gegen Vorschriften des Passgesetzes, des Personalausweisgesetzes und der Abgabenordnung eingelegt. Die Bf. im Verfahren 2 BvR 422/08 haben sich mit ihrer Verfassungsbeschwerde gegen §§ 100 a IV 1, 100 f I und II, 100 g, 101 IV 3–5, V und VI, 160 a I, II und IV StPOsowie die §§ 113 a, 113 b TKG gewandt.

Soweit andere Normen als §§ 100 a II und IV, 100 f, 101, 110 III und 160 a StPOangegriffen werden, ist das Verfahren entsprechend § 44 II GeschOBVerfG vom Ersten Senat des BVerfG übernommen worden. Mit Urteil vom 2. 3. 2010 (BVerfG, NJW 2010, 833) hat der Erste Senat die §§ 113 a und 113 b TKG sowie § 100 g I 1 StPO, soweit danach Verkehrsdaten nach § 113 a TKG erhoben werden durften, jeweils in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung, wegen Verstoßes gegen Art. 10 I GG für nichtig erklärt. Die Anträge der Bf. auf Erlass einer einstweiligen Anordnung wurden zum Teil im Hinblick auf die

Rechtsprechung des Ersten Senats (BVerfG, NVwZ 2008, 543; NVwZ 2009, 96) für erledigt erklärt und zum Teil abgelehnt (BVerfG, NVwZ 2009, 103). Die Bf. in den Verfahren 2 BvR 236/08 und 2 BvR 237/08 trugen vor, sie seien wie jeder andere Bürger von den angegriffenen Regelungen unmittelbar betroffen. Sie hätten – beruflich wie privat – als Rechtsanwalt, Arzt, Gymnasiallehrer oder Privatperson Zugang zu einem Festnetztelefonanschluss, zu mindestens einem Mobiltelefon sowie Internetanschluss und vertrauten darauf, dass ihre damit geführte Kommunikation dem Zugriff des Staates entzogen sei.
Die Bf. im Verfahren 2 BvR 422/08 (Rechtsanwälte, Abgeordnete, ein Student und eine Publizistin) sahen sich durch die angegriffenen Vorschriften schon deswegen in ihren Grundrechten unmittelbar und direkt berührt, weil sie privat, freiberuflich oder in ihrer politischen Tätigkeit Festnetzanschlüsse, Mobiltelefone, Internetzugänge und E-Mail-Postfächer nutzen müssten. Sie hätten damit zu rechnen, dass auf ihre Daten zugegriffen werde, ohne nach den im Gesetz vorgesehenen Regeln von einer sicheren nachträglichen Benachrichtigung ausgehen zu können.
(Zusammenfassung nach NJW 2012, 833, beck-online)

*b) Leitsätze*

**1.** § 100a Abs. 2 und 4, § 101 Abs. 4 bis 6 und § 160a StPO in der Fassung, die sie durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 erhalten haben, sind verfassungsgemäß.

**2.** Das Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG fordert vom Gesetzgeber die Bezeichnung des einzuschränkenden Grundrechts nicht nur bei der Schaffung von Eingriffsnormen, sondern auch bei einer erheblichen Änderung solcher Bestimmungen. Eine erhebliche Gesetzesänderung liegt nicht darin, dass nach der Neuregelung des § 101 Abs. 6 Satz 3 StPO mit Zustimmung des Gerichts von der Benachrichtigung des von einer verdeckten Ermittlungsmaßnahme Betroffenen abgesehen werden kann. Der Gesetzgeber durfte davon absehen, das von der Vorschrift neben Art. 10 GG berührte Grundrecht auf Unverletzlichkeit der Wohnung zu bezeichnen.

**3.** Die Erweiterung des Katalogs von Straftaten, zu deren Aufklärung nach § 100a Abs. 2 StPO Maßnahmen der Telekommunikationsüberwachung zulässig sind, verletzt nicht den Grundsatz der Verhältnismäßigkeit, weil nach wie vor nur schwere Straftaten erfasst sind. Die Schwere ergibt sich zwar nicht allein aus der bei allen erfassten Taten angedrohten Höchststrafe von mindestens fünf Jahren Freiheitsstrafe, weil diese im Strafgesetzbuch den Regelfall darstellt. Jedoch sind in den Katalog nur Taten aufgenommen worden, die in erheblicher Weise entweder die Funktionsfähigkeit des Staates und seiner Einrichtungen oder Rechtsgüter Privater beeinträchtigen. Zur Wahrung der Verhältnismäßigkeit trägt daneben bei, dass die jeweilige Tat auch im Einzelfall schwer wiegen muss.

**4.** Die Menschenwürdegarantie des Art. 1 Abs. 1 GG gewährleistet, dass ein Kernbereich privater Lebensgestaltung vor Eingriffen durch Maßnahmen der Telekommunikationsüberwachung unberührt bleibt. Den Kernbereich betreffende Informationen dürfen nicht in einem Urteil verwertet oder sonst verwendet werden. Dem trägt § 100a Abs. 4 StPO angemessen Rechnung, indem er die zielgerichtete Erhebung kernbereichsrelevanter Daten verbietet und Überwachungsmaßnahmen untersagt, wenn etwa aufgrund des Gesprächspartners ein ausschließlicher Kernbereichsbezug zu erwarten ist. Für den Fall der versehentlichen (Mit-)Erfassung kernbereichsrelevanter Informationen stellt § 100a Abs. 4 StPO in der Auswertungsphase den Grundrechtsschutz hinreichend sicher, indem er Dokumentations- und Löschungspflichten sowie ein Verwertungsverbot vorsieht.

**5.** Das von Art. 19 Abs. 4 GG garantierte Recht auf effektiven Rechtsschutz gewährleistet, dass ein von einer verdeckten strafprozessualen Ermittlungsmaßnahme Betroffener zumindest nachträglich von der Maßnahme unterrichtet wird. Ausnahmen von diesem Grundsatz sind nur in engen Grenzen und nur in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter zulässig, etwa wenn die Maßnahme ansonsten ihren Zweck verfehlen würde, wenn die Benachrichtigung zu einer Gefährdung von Leib und Leben einer Person führen würde oder wenn sie den Grundrechtseingriff noch vertiefen würde. Diesen Vorgaben wird die Regelung in § 101 Abs. 4 bis Abs. 6 StPO gerecht.

**6.** Ein absolutes Beweiserhebungs- und Verwendungsverbot, wie es § 160a Abs. 1 StPO vorsieht, ist angesichts der verfassungsrechtlichen Verpflichtung des Staates, eine effektive Strafverfolgung zu gewährleisten, auf besondere Ausnahmefälle zu beschränken. Eine derartige Beschränkung kann geboten sein, wenn die keiner Abwägung zugängliche Menschenwürdegarantie berührt ist, weil die Kommunikation des Beschuldigten bei typisierender Betrachtung den unantastbaren Bereich privater Lebensgestaltung betrifft, wie dies etwa bei Gesprächen mit einem Geistlichen, dem Verteidiger oder - aufgrund der Nähe der Tätigkeitsfelder - einem Rechtsanwalt der Fall ist. Bei Abgeordneten rechtfertigt sich der absolute Schutz aus der verfassungsrechtlichen Gewährleistung der Institution des Parlaments und seiner Funktionsfähigkeit, die Art. 47 GG auch in strafprozessualer Hinsicht absichert. Die Kommunikation aller anderen Berufsgeheimnisträger mit dem Beschuldigten unterliegt

demgegenüber nur einem relativen Beweisverbot, was § 160 Abs. 2 StPO in verfassungsrechtlich nicht zu beanstandender Weise normiert.
(Leitsätze des Bearbeiters, http://www.hrr-strafrecht.de/hrr/bverfg/08/2-bvr-236-08-1.php )

*c) Begründung*

Die Verfassungsbeschwerden sind, soweit zulässig, nicht begründet. Die angegriffenen Vorschriften verletzen die Beschwerdeführer nicht in ihren Grundrechten. […]

II.

Soweit sich die Beschwerdeführer gegen die Erweiterung des Straftatenkatalogs in § 100a Abs. 2 StPO und gegen eine fehlende Präzisierung des Schwerwiegens der Anlasstat auch im Einzelfall nach § 100a Abs. 1 Nr. 2 StPO wenden, haben ihre Verfassungsbeschwerden ebenfalls keinen Erfolg. Auch die Rüge, dass der Kernbereich privater Lebensgestaltung durch § 100a Abs. 4 Satz 1 StPO nicht ausreichend geschützt werde, greift nicht durch.

196

1. § 100a StPO ermächtigt zur Überwachung und Aufzeichnung der Telekommunikation und ermöglicht damit einen schwerwiegenden Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis (vgl. BVerfGE 113, 348 [382]).

197

Vom Schutz des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG sind nicht nur die Kommunikationsinhalte, sondern auch dieBVerfGE 129, 208 (240) BVerfGE 129, 208 (241)näheren Umstände der Telekommunikation erfasst. Das Fernmeldegeheimnis schützt zwar in erster Linie den Kommunikationsinhalt, umfasst aber ebenso die Kommunikationsumstände. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 [172]; 85, 386 [396]; 107, 299 [312 f.]). Auch insoweit darf der Staat grundsätzlich keine Kenntnis nehmen. Das Grundrecht will die Bedingungen einer freien Telekommunikation aufrechterhalten. Die Nutzung des Kommunikationsmediums soll in allem vertraulich möglich sein (vgl. BVerfGE 100, 313 [358]). Mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen (vgl. BVerfGE 100, 313 [359]). Dabei erfasst Art. 10 Abs. 1 GG sämtliche, mit Hilfe der Telekommunikationstechniken erfolgenden Übermittlungen von Informationen, unabhängig davon, wer Betreiber der Übertragungs- und Vermittlungseinrichtungen ist (vgl. BVerfGE 107, 299 [322]).

198

Ein Eingriff in das Fernmeldegeheimnis liegt vor, wenn staatliche Stellen sich ohne Zustimmung der Beteiligten Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen (vgl. BVerfGE 100, 313 [366]; 107, 299 [313]).

199

2. Mit der Neufassung des Straftatenkatalogs des § 100a Abs. 2 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung wurden 19 Straftatbestände gestrichen und mehr als 30 Straftatbestände neu aufgenommen. Durchgreifende verfassungsrechtliche Bedenken gegen die Klassifizierung der neu aufgenommenen Delikte als Katalogtaten für Maßnahmen der Telekommunikationsüberwachung, deren legitimen Zweck der Gesetzgeber darin sieht, den Strafverfolgungsbehörden dieBVerfGE 129, 208 (241) BVerfGE 129, 208 (242)notwendigen Mittel zur Verfolgung schwerer und schwer ermittelbarer Kriminalität an die Hand zu geben (BTDrucks 16/5846, S. 40), bestehen mit Blick auf Art. 10 GG nicht. Insbesondere sind Verstöße gegen das Bestimmtheitsgebot und den Grundsatz der Verhältnismäßigkeit nicht auszumachen.

200

a) Das Gesetz erstreckt sich nach der Intention des Gesetzgebers auf alle neu aufgenommenen Straftatbestände, die sämtlich schwere und schwer ermittelbare Kriminalität betreffen (siehe zu den einzelnen, neu durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung in § 100a Abs. 2 StPO aufgenommenen Straftatbeständen BTDrucks 16/5846, S. 41 ff.; nach Erhebung der Verfassungsbeschwerden im Jahr 2008 hat der Gesetzgeber den Straftatenkatalog des § 100a Abs. 2 StPO noch um § 89a StGB -- durch Art. 3 Nr. 1 des Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten vom 30. Juli 2009, BGBl. I S. 2437, um § 184c Abs. 3 StGB -- durch Art. 2 Nr. 1 des Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie vom 31. Oktober 2008, BGBl. I S. 2149, und um § 19 Abs. 3 Satz 2 Grundstoffüberwachungsgesetz [GÜG] durch Art. 1 des Gesetzes zur Neuregelung des Grundstoffüberwachungsrechts vom 11. März 2008, BGBl. I S. 306, ergänzt).

201

b) Dem Bestimmtheitsgebot hat der Gesetzgeber dadurch Rechnung getragen, dass er den Einsatz der Telekommunikationsüberwachung streng auf den Ermittlungszweck -- insbesondere die Aufklärung der Straftat und die

Feststellung des Aufenthaltsorts des Beschuldigten -- begrenzt. Zudem werden die Anlasstaten, bei denen die Telekommunikationsüberwachung als Ermittlungsmaßnahme in Betracht kommt, nicht lediglich mittels abstrakter Kriterien definiert, sondern in einem Katalog einzeln benannt. Ferner bedarf es einer gesicherten Tatsachenbasis ("bestimmte Tatsachen") sowohl für die Annahme eines Tatverdachts als auch für die Erstreckung der Maßnahme auf Dritte als Nachrichtenmittler (vgl. BVerfGE 107, 299 [321 ff.]; 109, 279 [350 f.]; 113, 348 [373, 385 f.] zu § 100c Abs. 1 Nr. 3 StPO). Damit hat der Gesetz-BVerfGE 129, 208 (242) BVerfGE 129, 208 (243)geber die Voraussetzungen der Überwachungsmaßnahme in grundsätzlich nachvollziehbarer Weise umschrieben (vgl. BVerfGE 110, 33 [54]).

202

c) Darüber hinaus wahrt der erweiterte Straftatenkatalog des § 100a Abs. 2 StPO den Grundsatz der Verhältnismäßigkeit. Der Gesetzgeber verfügt über einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung darüber, welche Straftaten er zum Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen machen will (vgl. BVerfGE 109, 279 [347]). Eingriffe in das Fernmeldegeheimnis setzen jedoch die Qualifizierung einer Straftat als schwer voraus, was aber in der Strafnorm -- insbesondere etwa durch den Strafrahmen -- einen objektivierten Ausdruck finden muss (vgl. BVerfGE 125, 260 [329]). Für diese Qualifizierung können auch das geschützte Rechtsgut und dessen Bedeutung für die Rechtsgemeinschaft von Bedeutung sein.

203

Der Gesetzgeber hat in den Katalog des § 100a Abs. 2 StPO nur Delikte neu aufgenommen, deren Begehung mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe bedroht ist. Dies allein qualifiziert die Delikte allerdings noch nicht als schwere Straftaten, bei denen ein Eingriff in Art. 10 Abs. 1 GG erst verhältnismäßig ist (vgl. BVerfGE 124, 43 [63]; 125, 260 [328]). Eine Höchststrafe von fünf Jahren Freiheitsstrafe ist im Strafgesetzbuch der Regelfall. Mit ihr sind auch Straftaten bedroht, die angesichts des jeweils geschützten Rechtsguts und bei teilweise nicht erhöhter Mindeststrafe allenfalls dem mittleren Kriminalitätsbereich zuzuordnen sind (vgl. BVerfGE 109, 279 [348]).

204

Gleichwohl ist die gesetzgeberische Einstufung der in § 100a Abs. 2 StPO aufgenommenen Straftatbestände als "schwer" bei einer Gesamtschau vertretbar, die insbesondere die jeweils geschützten Rechtsgüter in den Blick nimmt.

205

Die in den Katalog des § 100a Abs. 2 StPO aufgenommenen, lediglich mit Freiheitsstrafe bis zu fünf Jahren bedrohten Delikte greifen entweder -- wie die Abgeordnetenbestechung (§ 108e StGB), wettbewerbsbeschränkende Absprachen bei Ausschreibungen (§ 298 StGB), gewerbs- oder bandenmäßige VorbereitungBVerfGE 129, 208 (243) BVerfGE 129, 208 (244)der Fälschung von amtlichen Ausweisen (§ 275 Abs. 2 StGB), sowie das gewerbs- oder bandenmäßige Sich-Verschaffen von falschen amtlichen Ausweisen (§ 276 Abs. 2 StGB) -- erheblich in die Funktionsfähigkeit des Staates oder seiner Einrichtungen ein, oder sie beeinträchtigen in einschneidender Weise die Rechtsgüter Privater -- wie die Verbreitung, der Erwerb und Besitz kinderpornografischer Schriften (§ 184b Abs. 1 StGB) sowie die Förderung des Menschenhandels (§ 233a Abs. 1 StGB). Daher ist die Zuordnung dieser Delikte zu den schweren Straftaten in qualitativer Hinsicht vom Gestaltungsspielraum des Gesetzgebers umfasst.

206

Ferner hat der Gesetzgeber die Überwachung der Telekommunikation nicht allein an den Verdacht geknüpft, dass jemand als Täter oder Teilnehmer eine Katalogtat im Sinne des § 100a Abs. 2 StPO begangen hat. § 100a Abs. 1 Nr. 2 StPO verlangt vielmehr, dass die zur Überwachung der Telekommunikation Anlass gebende Katalogtat auch im Einzelfall schwer wiegt. Hinzu kommt das Erfordernis, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten -- ohne die Überwachung der Telekommunikation -- wesentlich erschwert oder aussichtslos wäre (§ 100a Abs. 1 Nr. 3 StPO). Damit hat der Gesetzgeber ein Schutzkonzept geschaffen, das dem Verhältnismäßigkeitsgrundsatz entspricht.

207

d) Die tatbestandliche Voraussetzung des § 100a Abs. 1 Nr. 2 StPO, dass "die Tat auch im Einzelfall schwer wiegt", genügt entgegen dem Beschwerdevorbringen schließlich dem Bestimmtheitsgebot. Indizien hierfür können, wie in der Rechtsprechung des Bundesverfassungsgerichts bereits mehrfach angesprochen, die Schutzwürdigkeit der verletzten Rechtsgüter (vgl. BVerfGE 109, 279 [346]), der Grad der Bedrohung der Allgemeinheit (vgl. BVerfGE 107, 299 [322]; 113, 348 [388]), die Art der Begehung der Straftat (vgl. BVerfGE 107, 299 [324]; 109, 279 [346]), die Anzahl der Geschädigten (vgl. BVerfGE 107, 299 [324]) und/oder das Ausmaß des Schadens (vgl. BVerfGE 107, 299 [324]) sein. Da es bei dem Tatbestandsmerkmal entscheidend auf die Würdigung der Umstände des Einzelfalls ankommt (vgl. zur Bedeutung die-BVerfGE 129, 208 (244) BVerfGE 129, 208 (245)ser zusätzlichen, über die abstrakte Festlegung eines Straftatenkatalogs hinausgehenden Freiheitssicherung BVerfGE 125, 260 [329]; m.w.N.), bedarf es von Verfassungs wegen keiner weiteren Ausdifferenzierung auf gesetzlicher Ebene.

208

3. Die durch § 100a Abs. 4 StPO geschaffenen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Telekommunikationsüberwachung genügen sowohl auf der Erhebungsebene als auch in der Auswertungsphase den verfassungsrechtlichen Anforderungen.

209

a) Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes können je nach der Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein (vgl. BVerfGE 120, 274 [337]). Eine gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, hat so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden (vgl. BVerfGE 120, 274 [337]; Durner, in: Maunz/Dürig, GG, Art. 10 Rn. 157 [Januar 2010]; Hömig, Jura 2009, S. 207 [212]). Bestehen im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, hat sie grundsätzlich zu unterbleiben (vgl. BVerfGE 120, 274 [338]; Gudermann, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010, S. 208). Anders liegt es jedoch, wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern (vgl. BVerfGE 109, 279 [328]; 120, 274 [338]).

210

In vielen Fällen ist es allerdings praktisch unvermeidbar, dass die Ermittlungsbehörden Informationen zur Kenntnis nehmen, bevor sie deren Kernbereichsbezug erkennen. In derartigen Fällen ist es verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen (vgl. BVerfGE 80, 367 [375, 381]; 120, 274 [338]). Ermittlungsmaßnahmen dürfen daher auch dann vorgenommen werden, wenn bestimmte Tatsachen den Ver-BVerfGE 129, 208 (245) BVerfGE 129, 208 (246)dacht begründen, jemand habe als Täter oder Teilnehmer eine auch im Einzelfall schwer wiegende Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet, wenn die Aufklärung ansonsten wesentlich erschwert oder aussichtslos wäre (vgl. BVerfGE 120, 274 [337 f.]).

211

In Fällen dieser Art ist es geboten, für hinreichenden Schutz in der Auswertungsphase zu sorgen (vgl. BVerfGE 120, 274 [337 f.]; Durner, in: Maunz/Dürig, GG, Art. 10 Rn. 157 [Januar 2010]). Der Gesetzgeber hat durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben (vgl. BVerfGE 120, 274 [338]; Gudermann, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010, S. 209). Entscheidende Bedeutung hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte. Ergibt die Durchsicht, dass kernbereichsrelevante Inhalte erhoben wurden, sind diese unverzüglich zu löschen; eine Weitergabe oder sonstige Verwendung ist auszuschließen (vgl. BVerfGE 109, 279 [324, 331 ff.]; 113, 348 [392]; 120, 274 [339]; Hömig, Jura 2009, S. 207 [212]).

212

b) Die in § 100a Abs. 4 Satz 1 StPO getroffene Regelung, nach der eine Maßnahme zur Überwachung und Aufzeichnung der Telekommunikation unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, erfüllt die Anforderungen zum Schutz des Kernbereichs privater Lebensgestaltung auf der Ebene der Informationserhebung.

213

aa) Der Gesetzgeber hat mit der Neuregelung des § 100a Abs. 4 StPO ein zweistufiges Schutzkonzept entwickelt, um den Betroffenen vor Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung zu bewahren. § 100a Abs. 4 Satz 1 StPO ordnet an, dass eine zielgerichtete Erhebung kernbereichsrele-BVerfGE 129, 208 (246) BVerfGE 129, 208 (247)vanter Daten unterbleibt. Kommt es dennoch -- ohne dass dies im Vorfeld zu erwarten war -- zu einer Berührung des Kernbereichs, ist in § 100a Abs. 4 Sätze 2 bis 4 StPO eine Dokumentations- und Löschungspflicht sowie ein Verwertungsverbot vorgesehen.

214

bb) Ein ausschließlicher Kernbereichsbezug kann vor allem dann angenommen werden, wenn der Betroffene mit Personen kommuniziert, zu denen er in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis -- wie zum Beispiel engsten Familienangehörigen, Geistlichen, Telefonseelsorgern, Strafverteidigern oder im Einzelfall auch Ärzten -- steht (vgl. BVerfGE 109, 279 [321 ff.]). Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen der Telekommunikationsüberwachung nicht durchgeführt werden.

215

cc) Entgegen der Auffassung der Beschwerdeführer müssen Telekommunikationsüberwachungsmaßnahmen aber nicht schon deshalb von vornherein unterlassen werden, weil auch Tatsachen mit erfasst werden, die auch den Kernbereich des Persönlichkeitsrechts berühren. Ein entsprechendes umfassendes Erhebungsverbot würde die Telekommunikationsüberwachung in einem Maße einschränken, dass eine wirksame Strafverfolgung gerade im Bereich schwerer und schwerster Kriminalität nicht mehr gewährleistet wäre. Der Schutz des Kernbereichs

privater Lebensgestaltung ist in diesen Fällen durch einen hinreichenden Grundrechtsschutz in der Auswertungsphase sicherzustellen.

216

Ein umfassender Kernbereichsschutz schon auf der Ebene der Informationserhebung würde bei der Telekommunikationsüberwachung nach § 100a StPO -- ebenso wie beim heimlichen Zugriff auf informationstechnische Systeme (vgl. BVerfGE 120, 274 [337]) -- auf erhebliche praktische Schwierigkeiten stoßen, die überdies verschiedene Ursachen haben. Im Voraus lässt sich häufig kaum bestimmen, wann, wo und mit wem Telekommunikation stattfinden wird. Dementsprechend fehlt es in aller Regel an operationalisierbaren Kriterien, um eine Erhebung von Kommunikationsinhalten mit Kernbereichsbezug vorausschauend zu vermeiden (Käß, BayVBl 2010, S. 1 [10]).

217

Schwierigkeiten für einen umfassenden KernbereichsschutzBVerfGE 129, 208 (247) BVerfGE 129, 208 (248)schon auf der Erhebungsebene ergeben sich insbesondere daraus, dass Telekommunikationsüberwachung mittels automatisierter Aufzeichnung der Kommunikationsinhalte durchgeführt wird (vgl. Bär, in: Kleinknecht/Müller/Reitberger, StPO, 60. Lieferung [Mai 2011], § 100a Rn. 43; Gusy, Auswirkungen des Lauschangriffsurteils außerhalb der strafprozessualen Wohnungsüberwachung, in: Schaar [Hrsg.], Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung: Staatliche Eingriffsbefugnisse auf dem Prüfstand?, S. 35 [52, 58]) und eine persönliche Überwachung durch (paralleles) Mithören in Echtzeit in der Regel nur punktuell stattfinden kann.

218

Hinzu kommt, dass selbst bei persönlicher Überwachung der Telekommunikation durch ein Mithören in Echtzeit die Schwierigkeiten für einen wirkungsvollen Kernbereichsschutz auf der Erhebungsebene vielfach nicht zu beseitigen wären. So wird ein Großteil der zu Zwecken der Strafverfolgung überwachten Telekommunikation in fremden, zum Teil nicht ohne Weiteres identifizierbaren Sprachen und Dialekten und darüber hinaus unter Benutzung von Geheimcodes geführt (vgl. BTDrucks 16/5846, S. 44). Dies führt dazu, dass selbst bei ständigem Mithören in Echtzeit durch einen Beamten der Strafverfolgungsbehörde und einen Dolmetscher -- oder gegebenenfalls mehrere Dolmetscher, falls die Gesprächsteilnehmer ihr(e) Telefongespräch(e) in wechselnden Sprachen oder Dialekten führen -- der Inhalt der Gespräche und somit auch eine etwaige Kernbereichsrelevanz derselben nicht stets sofort zutreffend erfasst und beurteilt werden könnten (vgl. BVerfGE 120, 274 [338]; BTDrucks 16/5846, S. 44). Vielmehr ist hierfür oftmals das wiederholte Abspielen und Anhören der aufgezeichneten Kommunikation unabdingbar. Darüber hinaus sind Gespräche auch aus sonstigen, der Nutzung des Mediums geschuldeten Gründen wie zum Beispiel Hintergrundrauschen oder schlechter Empfang kaum ohne technische Aufbereitung beim ersten Hören zu verstehen (vgl. BTDrucks 16/5846, S. 44). Selbst in Fällen, in denen diese technisch bedingten Widrigkeiten nicht bestehen und das Telefongespräch in klarem, unverklausuliertem Deutsch geführt wird, gelingt die Zu-BVerfGE 129, 208 (248) BVerfGE 129, 208 (249)ordnung einer Stimme zu einer Person beim Mithören in Echtzeit nicht immer (vgl. Käß, BayVBl 2008, S. 225 [232 f.]), so dass die Strafverfolgungsbehörden auch unter günstigsten Voraussetzungen vielfach nicht in der Lage wären, durch simultanes Mithören zu erschließen, in welchen persönlichen Beziehungen die Gesprächspartner zueinander stehen, und eine (etwaige) -- echte und nicht lediglich zur Täuschung der Behörden vorgeschützte -- Kernbereichsrelevanz geführter Gespräche zu erkennen.

219

dd) Für den Fall, dass bei einer Überwachungsmaßnahme Daten erfasst werden, die den Kernbereich privater Lebensgestaltung berühren, bietet das in § 100a Abs. 4 Satz 2 StPO normierte Verwertungsverbot einen hinreichenden Schutz in der Auswertungsphase (vgl. Löffelmann, in: Krekeler/Löffelmann/Sommer, AnwaltKommentar StPO, 2. Aufl. 2010, § 100a Rn. 11). Es ist umfassend und verbietet jedwede Verwendung, auch als Ermittlungs- oder Spurenansatz (vgl. Schmitt, in: Meyer-Goßner, StPO, 54. Aufl. 2011, § 100a Rn. 25; Nöding, StraFo 2007, S. 456 [459]). Mit dem absoluten Verwertungsverbot, dem unverzüglichen Löschungsgebot und der dazugehörigen Dokumentationsverpflichtung entspricht das Gesetz den Anforderungen an einen effektiven Kernbereichsschutz.

220

c) Entgegen der Auffassung der Beschwerdeführer ist es von Verfassungs wegen nicht geboten, zusätzlich zu den staatlichen Ermittlungsbehörden eine unabhängige Stelle einzurichten, die über die (Nicht-)Verwendbarkeit der gewonnenen Erkenntnisse im weiteren Ermittlungsverfahren entscheidet.

221

Das Bundesverfassungsgericht hat in ständiger Rechtsprechung verfahrensrechtliche Sicherungen dafür gefordert, dass aus dem Kernbereich privater Lebensgestaltung erlangte Daten nicht gespeichert, verwertet und weitergegeben sondern unverzüglich gelöscht werden (vgl. BVerfGE 109, 279 [333]; 113, 348 [390 f.]; 120, 274 [338 f.]; 124, 43 [70]). In seinem Beschluss zur akustischen Wohnraumüberwachung hat es ausgeführt, dass es einer unabhängigen Stelle obliege, die Verwertbarkeit der gewonnenen Erkenntnisse im Hauptsacheverfahren oder als Ermittlungsansatz in anderen Verfahren zu beurteilen (vgl. BVerfGE 109, 279BVerfGE 129, 208 (249) BVerfGE 129, 208 (250)[333 f.]). Die von Verfassungs wegen geforderten verfahrensrechtlichen Sicherungen

gebieten jedoch nicht, dass in allen Fallkonstellationen neben staatlichen Ermittlungsbehörden weitere unabhängige Stellen eingerichtet werden, um die Einhaltung der gesetzlichen Bestimmungen zu gewährleisten.

222

Hier muss insbesondere berücksichtigt werden, dass Maßnahmen nach § 100a StPO einer gerichtlichen Anordnung bedürfen, es sei denn, es liegt Gefahr im Verzug vor, in welchem Fall sie grundsätzlich gerichtlich zu bestätigen sind (§ 100b Abs. 1 StPO). Durch die Vorbefassung eines Richters bei der Überwachung der Telekommunikationsüberwachung ist somit sichergestellt, dass der Kernbereichsschutz bereits im Vorfeld von einer unabhängigen Instanz in den Blick genommen wird und Beachtung findet. Im Übrigen ist das anordnende Gericht nach Beendigung der Maßnahme über deren Ergebnis zu unterrichten (§ 100b Abs. 4 Satz 2 StPO). Soweit die Ermittlungsbehörde in Einzelfällen ein Verwertungsverbot verneint, weil die erhobenen Daten nach ihrer Einschätzung nicht zum Kernbereich gehören, unterliegt diese Entscheidung ferner der gerichtlichen Überprüfung nach § 101 Abs. 7 Sätze 2 bis 4 StPO.

223

Vor diesem Hintergrund ist es nicht zu beanstanden, wenn die Staatsanwaltschaft über die (Nicht-)Verwendbarkeit der gewonnenen Erkenntnisse im weiteren Ermittlungsverfahren entscheidet.

224

III.

Die gegen die Ausgestaltung der Benachrichtigungspflicht in § 101 Abs. 4 bis 6 StPO gerichtete Rüge greift ebenfalls nicht durch.

225

1. Das Bundesverfassungsgericht hat in seinem Urteil zur (anlasslosen) Vorratsdatenspeicherung ausgeführt, dass der Gesetzgeber bei der heimlichen Erhebung von Daten seiner Bürger zur Transparenz verpflichtet sei. Er habe Regelungen zur Information der von Datenerhebungen oder -nutzungen Betroffenen zu schaffen, da diese allgemein zu den elementaren Instrumenten des grundrechtlichen Datenschutzes gehörten (vgl. BVerfGE 125, 260BVerfGE 129, 208 (250) BVerfGE 129, 208 (251)[335] unter Verweis auf BVerfGE 100, 313 [361]; 109, 279 [363 f.]; 118, 168 [207 f.]; 120, 351 [361 f.]). Nur durch die Information des Betroffenen kann ein effektiver Rechtsschutz gewährleistet werden. Ohne zumindest nachträgliche Kenntnis können die Betroffenen weder eine Unrechtmäßigkeit der Datenverwendung noch etwaige Rechte auf Löschung, Berichtigung oder Genugtuung geltend machen (vgl. BVerfGE 100, 313 [361]; 109, 279 [363]; 118, 168 [207 f.]; 120, 351 [361]; 125, 260 [335]).

226

Ausnahmen von der Benachrichtigungspflicht kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Sie sind jedoch auf das unbedingt Erforderliche zu beschränken (vgl. BVerfGE 109, 279 [364]; 125, 260 [336]). Bei der Strafverfolgung sind Ausnahmen von den Benachrichtigungspflichten denkbar, wenn beispielsweise die Kenntnis des Eingriffs in das Telekommunikationsgeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt, wenn die Benachrichtigung nicht ohne Gefährdung von Leib und Leben einer Person geschehen kann oder wenn ihr überwiegende Belange einer betroffenen Person entgegenstehen, etwa weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde (vgl. BVerfGE 100, 313 [361]; 109, 279 [364 ff.]; 125, 260 [336]). Darüber hinaus ist es verfassungsrechtlich nicht geboten, vergleichbar strenge Benachrichtigungspflichten gegenüber Personen zu begründen, die nur zufällig von einer Ermittlungsmaßnahme gegen einen Beschuldigten betroffen sind und somit nicht Ziel des behördlichen Handelns sind. Eine Benachrichtigung kann ihnen gegenüber im Einzelfall den Eingriff vielfach sogar vertiefen (vgl. BVerfGE 109, 279 [365]; 125, 260 [337]; BVerfGK 9, 62 [81]). In diesen Fällen kann eine Benachrichtigung grundsätzlich schon dann unterbleiben, wenn die Betroffenen von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben (vgl. BVerfGE 125, 260 [337]).

227

2. Gemessen an diesen Vorgaben halten die Regelungen des § 101 Abs. 4 bis 6 StPO einer verfassungsrechtlichen Prüfung stand.BVerfGE 129, 208 (251)

228

BVerfGE 129, 208 (252)In diesem Zusammenhang ist zu berücksichtigen, dass § 101 StPO eine grundrechtssichernde Verfahrensvorschrift ist, die einheitlich für die Ermittlungsmaßnahmen des § 101 Abs. 4 Satz 1 Nr. 1 bis 12 StPO die Kennzeichnungspflicht (Absatz 3), die Benachrichtigungspflicht (Absatz 4), deren vorübergehende oder endgültige Suspendierung (Absätze 5 und 6), den Rechtsschutz (Absatz 7) und die Löschungspflicht (Absatz 8) regelt. Daneben macht die Norm in Absatz 2 für die akustische Wohnraumüberwachung (§ 100c StPO), die akustische Überwachung außerhalb von Wohnungen (§ 100 f StPO), den Einsatz besonderer technischer Mittel für Observationszwecke (§ 100h Abs. 1 Nr. 2 StPO) und den Einsatz Verdeckter Ermittler (§ 110a StPO) gesetzliche Vorgaben für die Aktenführung. Den in § 101 Abs. 4 Satz 1 Nr. 1 bis 12 StPO aufgeführten Ermittlungsmaßnahmen ist gemein, dass sie eine begangene Straftat und konkrete Hinweise auf den Täter oder die Tatbeteiligten voraussetzen. Es handelt sich -- mit Ausnahme der vom Bundesverfassungsgericht für nichtig erklärten Vorratsdatenspeicherung nach § 100g Abs. 1 StPO in Verbindung mit § 113a TKG (vgl. BVerfGE 125, 260) -- somit nicht um eine anlasslose, verdachtsunabhängige Informationsbeschaffung mit großer Streu-

breite (vgl. zur Bedeutung dieser Kriterien für die Intensität von Grundrechtseingriffen BVerfGE 115, 320 [354]). Darüber hinaus steht die Anordnung aller Maßnahmen -- mit Ausnahme des § 100h StPO, der außerhalb von Wohnungen die Erstellung von Bildaufnahmen des Beschuldigten sowie den Einsatz technischer Hilfsmittel für Observationszwecke regelt -- unter Richtervorbehalt. Mithin sind die Maßnahmen, von denen Betroffene zu benachrichtigen sein können, von einem Richter auf ihre Rechtmäßigkeit zum Zeitpunkt ihrer Anordnung geprüft und gebilligt worden.

229

a) Nach § 101 Abs. 4 Satz 3 StPO unterbleibt die Benachrichtigung einer von einer verdeckten strafprozessualen Ermittlungsmaßnahme betroffenen Person, wenn der Benachrichtigung überwiegende schutzwürdige Belange einer anderen, von der Maßnahme ebenfalls betroffenen Person entgegenstehen. Dies ist etwa der Fall, wenn Gespräche des Beschuldigten mit einem an derBVerfGE 129, 208 (252) BVerfGE 129, 208 (253)Straftat unbeteiligten Geschäftspartner erfasst wurden (vgl. BT-Drucks 16/5846, S. 59; Schmitt, in: Meyer-Goßner, StPO, 54. Aufl. 2011, § 101 Rn. 16). Das kann zur Folge haben, dass insbesondere Personen nicht benachrichtigt werden dürfen, die durch eine Ermittlungsmaßnahme zufällig betroffen sind, aber nicht Anlass zu ihr gegeben haben. Damit trägt § 101 Abs. 4 Satz 3 StPO vor allem den Interessen des unmittelbar von der Ermittlungsmaßnahme Betroffenen Rechnung. Da zu diesem Zeitpunkt trotz vorhandenen Anfangsverdachts noch nicht feststeht, ob sich die Verdachtsmomente gegen ihn zu einem für die Eröffnung des Hauptverfahrens erforderlichen hinreichenden Tatverdacht (§ 203 StPO) verdichten oder nicht, ist der Beschuldigte zu diesem Zeitpunkt mit Blick auf seine persönlichen und beruflichen Beziehungen besonders schutzbedürftig.

230

Der Gesetzgeber hat mit der Regelung des § 101 Abs. 4 Satz 3 StPO die Erwägung des Bundesverfassungsgerichts aufgenommen, nach der es verfassungsrechtlich nicht geboten ist, vergleichbar strenge Benachrichtigungspflichten gegenüber Personen zu begründen, deren Daten nur zufällig miterfasst wurden (vgl. BVerfGE 125, 260 [337]). In Bezug auf diese Personengruppe bedarf es von Verfassungs wegen keiner richterlichen Bestätigung der Abwägungsentscheidung über einen Ausschluss der Benachrichtigung nach § 101 Abs. 4 Satz 3 StPO (vgl. BVerfGE 125, 260 [337]). Die Abwägung zwischen den Interessen des Beschuldigten und des Nichtbeschuldigten bei der Entscheidung über dessen Benachrichtigung darf im Hinblick auf die vergleichsweise geringe Eingriffsintensität diesem gegenüber von Verfassungs wegen der Staatsanwaltschaft überlassen bleiben.

231

b) Die Vorschrift des § 101 Abs. 4 Satz 4 StPO, nach der in den Fällen der Postbeschlagnahme, der Telekommunikationsüberwachung und der Telekommunikationsverkehrsdatenerhebung die Benachrichtigung einer Person unterbleiben kann, gegen die sich die Maßnahme nicht gerichtet hat, wenn sie von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat, ist ebenso wenig verfassungsrechtlich zu beanstanden. Denn bei lediglich uner-BVerfGE 129, 208 (253) BVerfGE 129, 208 (254)heblichen Grundrechtseingriffen gegen Personen, die nicht Ziel behördlichen Handelns waren, bedarf es keiner Bestätigung der Entscheidung, den Betroffenen hiervon nicht zu benachrichtigen, durch ein Gericht oder eine andere unabhängige Instanz (vgl. BVerfGE 125, 260 [337]).

232

c) § 101 Abs. 4 Satz 5 StPO befasst sich mit der Fallgestaltung, dass die Identität einer von einer heimlichen Ermittlungsmaßnahme betroffenen Person nicht bekannt ist, so dass eine Benachrichtigung praktisch nur erfolgen kann, wenn zuvor mittels entsprechender Nachforschungen ihre Identität festgestellt wird. Damit bezieht sich die Norm nicht auf einen Beschuldigten, dessen Identität in diesem Stadium des Ermittlungsverfahrens bereits bekannt ist, sondern -- ebenso wie § 101 Abs. 4 Satz 4 StPO -- auf einen zufällig von der Ermittlungsmaßnahme betroffenen, nicht tatverdächtigen Dritten. In Bezug auf diese Personengruppe können Nachforschungen den Grundrechtseingriff sowohl für die Zielperson als auch für sonstige Beteiligte vertiefen (vgl. BVerfGE 109, 279 [365]; 125, 260 [337]; siehe auch BTDrucks 16/5846 S. 60). Der Gesetzgeber durfte daher die in § 101 Abs. 4 Satz 5 StPO vorgesehene Entscheidung den Ermittlungsbehörden übertragen, zumal sich die Identität der betroffenen Personen häufig nur mit hohem Aufwand ermitteln lassen dürfte (vgl. BVerfGE 125, 260 [337]).

233

d) Auch die Regelung des § 101 Abs. 5 Satz 1 StPO, dass ein von der Ermittlungsmaßnahme Betroffener erst benachrichtigt wird, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist, ist mit dem Grundgesetz vereinbar.

234

Die Norm sieht differenzierte Regelungen vor, die den Grundsatz einer nachträglichen Benachrichtigung des Betroffenen verfassungsrechtlich tragfähig mit im Einzelfall ausnahmsweise entgegenstehenden überwiegenden Belangen in Ausgleich bringen (vgl. BVerfGE 125, 260 [353]).BVerfGE 129, 208 (254)

235

BVerfGE 129, 208 (255)aa) Entgegen der Ansicht der Beschwerdeführer ist das Tatbestandsmerkmal des "bedeutenden Vermögenswertes" hinreichend bestimmt. Um den rechtsstaatlichen Erfordernissen der Normklarheit

und Justitiabilität gerecht zu werden, genügt es, dass eine Norm mit herkömmlichen juristischen Methoden ausgelegt werden kann (vgl. BVerfGE 65, 1 [54]; 78, 205 [212 f.]; 103, 21 [33]). Gegebenenfalls darf hierzu auch auf die Rechtsprechung zu einem anderen Rechtsgebiet zurückgegriffen werden, falls dort eine ähnliche Norm oder deren Teile Gegenstand der Prüfung waren (vgl. BVerfGE 103, 23 [33 f.]). Vorliegend wird der Begriff des "Vermögenswertes" in gesetzlichen Bestimmungen vielfach verwendet (auf Verfassungsebene in Art. 135a Abs. 1 Nr. 2, Abs. 2 GG, auf einfachgesetzlicher Ebene beispielsweise in § 89a Abs. 2 Nr. 4, § 263 Abs. 3 Nr. 2, § 283a Nr. 2, § 283d Abs. 3 Nr. 2 StGB und in § 53 Abs. 2 Satz 2 Nr. 3, § 100a Abs. 2 Nr. 1 Buchstabe m, § 100c Abs. 2 Nr. 1 Buchstabe l, § 100d Abs. 5 Nr. 2 Satz 2, § 111e Abs. 4 Satz 3, § 111i Abs. 3 Satz 3, Abs. 5 Satz 1 und § 111l Abs. 1 StPO). Den Gerichten kann darüber hinaus überantwortet werden, bedeutende Vermögenswerte von unbedeutenden abzugrenzen. Sie können dazu beispielsweise die Rechtsprechung zum Merkmal der "Sachen von bedeutendem Wert" in § 315 Abs. 1, § 315a Abs. 1, § 315b Abs. 1, § 315c Abs. 1 StGB in den Blick nehmen.

236

bb) Soweit in § 101 Abs. 5 Satz 1 StPO die Benachrichtigung über den Einsatz eines Verdeckten Ermittlers mit Rücksicht auf die Möglichkeit seiner weiteren Verwendung zurückgestellt werden darf, genügt die vorgesehene Abwägung insbesondere den Anforderungen der Verhältnismäßigkeit im engeren Sinne. Der Zurückstellungsgrund ist hinreichend gewichtig, um eine gesetzliche Beschränkung der Benachrichtigungspflicht zu rechtfertigen.

237

Zwar greift der Staat in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein, wenn sich einer seiner Beamten unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt und sich unter Ausnutzung schutzwürdigen Vertrauens des Betrof-BVerfGE 129, 208 (255) BVerfGE 129, 208 (256)fenen Informationen über dessen kriminelles Verhalten verschafft, die er ansonsten nicht erhielte (vgl. BVerfGE 120, 274 [345]). Andererseits gestattet und verlangt das Rechtsstaatsprinzip auch die Berücksichtigung der Belange einer funktionstüchtigen Strafrechtspflege (vgl. BVerfGE 122, 248 [272]), dem der mögliche anderweitige Einsatz des Verdeckten Ermittlers dient. Der Verhinderung, Verfolgung und Aufklärung von Straftaten kommt nach dem Grundgesetz eine hohe Bedeutung zu (vgl. BVerfGE 100, 313 [388]; 113, 29 [54]; 115, 166 [192]; 122, 248 [270, 272]). Damit den Strafverfolgungsbehörden die Wahrnehmung ihres Auftrags gerade im Hinblick auf besonders gefährliche Kriminalitätsfelder nicht zusätzlich erheblich erschwert oder gar unmöglich gemacht wird, bedarf es Verdeckter Ermittler (vgl. BVerfGE 57, 250 [284]). Sollte deren Einsatz unmöglich werden, weil eine Unterrichtung des Betroffenen in einem bestimmten Zeitraum den Betroffenen und sein Umfeld in die Lage versetzt, Rückschlüsse auf deren Identität zu ziehen, gingen wichtige Ermittlungsmöglichkeiten gerade dort verloren, wo die Aufklärung besonders schwierig ist und der Rechtsfrieden und die Sicherheit in besonderer Weise bedroht sind. Der Gesetzgeber hat mit der Regelung in § 101 Abs. 5 StPO einen angemessenen Ausgleich zwischen dem Benachrichtigungsinteresse des von einer heimlichen Ermittlungsmaßnahme Betroffenen und dem Strafverfolgungsinteresse des Staates geschaffen.

238

Entgegen der Ansicht der Beschwerdeführer steht dem die Rechtsprechung des Bundesverfassungsgerichts nicht entgegen. Das Bundesverfassungsgericht hat sich in seinem Urteil zur akustischen Wohnraumüberwachung (BVerfGE 109, 279) nicht mit einer verzögerten oder gar suspendierten Benachrichtigungspflicht in Bezug auf den weiteren Einsatz eines Verdeckten Ermittlers auseinandergesetzt. Gegenstand der dort zur Prüfung stehenden Norm des § 101 Abs. 1 Satz 1 StPO a.F. war vielmehr eine Suspendierung der Benachrichtigungspflicht bis zu dem Zeitpunkt, in dem die weitere Verwendung eines nicht offen eingesetzten Beamten nicht mehr gefährdet ist (vgl. BVerfGE 109, 279 [289 f., 366]).BVerfGE 129, 208 (256)

239

BVerfGE 129, 208 (257)Ein nicht offen ermittelnder Beamter ist kein Verdeckter Ermittler, sondern ein Polizeibeamter, der nur gelegentlich -- ohne vorherige Schaffung einer Legende -- verdeckt auftritt und hierbei seine Funktion nicht offenlegt (vgl. Nack, in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 110a Rn. 6; m.w.N.). Im Gegensatz zu den strengen Voraussetzungen, unter denen ein Verdeckter Ermittler zum Einsatz kommen darf (§§ 110a und 110b StPO), richtet sich der Einsatz eines nicht offen ermittelnden Polizeibeamten nach den Generalnormen der §§ 161 und 163 StPO (vgl. Nack, in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 110a Rn. 6). Während die Polizei selbst einen offen ermittelnden Beamten zu einem nicht offen ermittelnden machen kann, bedarf es für den Einsatz eines Verdeckten Ermittlers der Zustimmung der Staatsanwaltschaft oder in besonderen Fällen des Ermittlungsgerichts als Kontrollinstanz (§ 110b Abs. 2 StPO). Eine Vermehrung der Anzahl der Verdeckten Ermittler liegt somit nicht in den Händen der Polizei. Darüber hinaus stellt der Einsatz Verdeckter Ermittler die ultima ratio der Ermittlungsbehörden bei ihrer Arbeit dar. Sie dürfen nach § 110a Abs. 1 Satz 3 StPO nur dann in den abschließend vom Gesetz aufgeführten Fällen zum Einsatz kommen, wenn die Aufklärung auf andere Weise aussichtslos oder erheblich erschwert wäre. Es bestehen mithin substantielle Unterschiede zwischen dem Einsatz eines Verdeckten Ermittlers und dem eines nicht offen ermittelnden Polizeibeamten.

240

e) Auch § 101 Abs. 6 Satz 3 StPO hält einer verfassungsrechtlichen Prüfung stand. Die Norm bestimmt, dass das Gericht dem endgültigen Absehen von der Benachrichtigung zustimmen kann, wenn die Voraussetzungen

für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. § 101 Abs. 6 Sätze 2 und 3 StPO tragen der Tatsache Rechnung, dass Gründe, die die Benachrichtigungspflicht zu suspendieren vermögen, von vorübergehender oder dauerhafter Natur sein können. Sind sie vorübergehender Natur, stellt § 101 Abs. 6 Satz 2 StPO die dann in Zeitabständen gebotene wiederkehrende gerichtliche Kontrolle sicher und sorgt dafür, dass die Zurückstellung der an sich zu veranlassenden Benach-BVerfGE 129, 208 (257) BVerfGE 129, 208 (258)richtigung in zeitlicher Hinsicht auf das unbedingt Erforderliche begrenzt bleibt. Das Gericht bestimmt dann gemäß § 101 Abs. 6 Satz 2 StPO eine weitere Zurückstellung und deren Dauer. Liegt hingegen ein Grund vor, der dauerhaft zur Suspendierung der Benachrichtigungspflicht führt, sieht § 101 Abs. 6 Satz 3 StPO eine einmalige gerichtliche Kontrolle vor, um gegebenenfalls ein endgültiges Absehen von der Benachrichtigung zu ermöglichen.

241

Der Gesetzgeber durfte davon absehen, die Strafverfolgungsbehörden und Gerichte zu wiederholten Prüfungen weiterer Zurückstellungen zu verpflichten, wenn sich an der eine Benachrichtigung hindernden Sachlage aller Wahrscheinlichkeit nach auf Dauer nichts ändern wird. Mit dem Tatbestandsmerkmal "an Sicherheit grenzender Wahrscheinlichkeit" errichtet er für die Prognose der Dauerhaftigkeit eine hinreichend hohe Hürde, um vorschnelle Beurteilungen wirkungsvoll zu verhindern.

[…]

## II) EuGH

### 1) EuGH C-465/00, C-138, C-139/01 – Rechnungshof

*a) Sachverhalt*

Zwischen dem Rechnungshof und einer Reihe seiner Kontrolle unterliegender Einrichtungen kam es im Zusammenhang mit 1998 und 1999 gezahlten Bezügen und Ruhebezügen zu Meinungsverschiedenheiten über die Auslegung von § 8 BezBegrBVG.

18.

So übermittelten die Antragsgegner des Ausgangsverfahrens, zu denen Gebietskörperschaften (ein Land und zwei Gemeinden), öffentliche Unternehmen, die zum Teil in Wettbewerb mit anderen nicht vom Rechnungshof kontrollierten inländischen und ausländischen Unternehmen stehen, und eine gesetzliche Interessenvertretung (die Wirtschaftskammer Steiermark) gehören, die Einkommensdaten nicht oder nur in - in unterschiedlichem Umfang - anonymisierter Form. Sie verweigerten die Einsicht in die maßgeblichen Unterlagen oder knüpften sie an Bedingungen, die vom Rechnungshof nicht akzeptiert wurden. Daraufhin rief dieser den Verfassungsgerichtshof gemäß Artikel 126a Bundes-Verfassungsgesetz an, nach dem der Verfassungsgerichtshof dafür zuständig ist, über die „Meinungsverschiedenheiten über die Auslegung der gesetzlichen Bestimmungen, die die Zuständigkeit des Rechnungshofes regeln“, zu entscheiden.

19.

Der Rechnungshof entnimmt § 8 BezBegrBVG die Verpflichtung, im Bericht die Namen der betroffenen Personen und deren Jahreseinkommen auszuweisen. Die Antragsgegner des Ausgangsverfahrens sind anderer Ansicht und halten sich nicht für verpflichtet, personenbezogene Einkommensdaten wie die Namen oder die Funktionen der betroffenen Personen in Verbindung mit deren Bezügen bekannt zu geben. Sie stützen sich im Wesentlichen auf die Richtlinie 95/46, auf Artikel 8 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK), der den Schutz des Privatlebens verbürge, sowie darauf, dass die Offenlegungspflicht zu einem gegen Artikel 39 EG verstoßenden Hindernis für die Mobilität der Arbeitnehmer führe.

20.

Der Verfassungsgerichtshof fragt sich im Wesentlichen, ob § 8 BezBegrBVG in der vom Rechnungshof vertretenen Auslegung mit dem Gemeinschaftsrecht vereinbar ist, um diese Vorschrift gegebenenfalls gemeinschaftsrechtskonform auslegen oder (teilweise) unangewendet lassen zu können.

21.

Das vorlegende Gericht betont in diesem Zusammenhang, dass es erforderlich sei, die Bestimmungen der Richtlinie 95/46, insbesondere ihre Artikel 6 Absatz 1 Buchstaben b und c und 7 Buchstaben c und e im Licht des Artikels 8 EMRK auszulegen. Die vom nationalen Gesetzgeber beabsichtigte umfassende Information der Öffentlichkeit über die Einkommen von Arbeitnehmern vom Rechnungshof kontrollierter Rechtsträger, deren Jahresbezüge einen bestimmten Grenzbetrag überschritten (1999: 1 127 486 ATS; 1998: 1 120 000 ATS), sei als Eingriff in die Privatsphäre anzusehen, der nach Artikel 8 Absatz 2 EMRK nur dann gerechtfertigt werden könne, wenn diese Information dem wirtschaftlichen Wohl des Landes diene. Es sei nämlich ausgeschlossen, den Eingriff in die Grundrechte mit dem Vorliegen eines bloßen „Informationsinteresses der Öffentlichkeit“ zu rechtfertigen. Der Verfassungsgerichtshof bezweifelt, dass die Offenlegung personenbezogener Einkommensdaten im Bericht das „wirtschaftliche Wohl des Landes“ fördert. Sie stelle jedenfalls einen unverhältnismäßigen Eingriff

in die Privatsphäre dar. Die Gebarungskontrolle durch den Rechnungshof sei zweifellos ausreichend, um den ordnungsgemäßen Einsatz öffentlicher Gelder zu gewährleisten.

22.

Das vorlegende Gericht stellt sich außerdem die Frage, ob die Reichweite des Gemeinschaftsrechts unterschiedlich ist, je nachdem, welcher Art von Rechtsträger die Offenlegung der personenbezogenen Einkommensdaten seiner Arbeitnehmer vorgeschrieben ist.

23.

Der Verfassungsgerichtshof hat daher das Verfahren ausgesetzt und dem Gerichtshof die beiden folgenden Fragen zur Vorabentscheidung vorgelegt:

1. Sind die gemeinschaftsrechtlichen Vorschriften, insbesondere jene über den Datenschutz so auszulegen, dass sie einer nationalen Regelung entgegenstehen, die ein staatliches Organ zur Erhebung und Weiterleitung von Einkommensdaten zum Zweck der Veröffentlichung der Namen und Einkommen der Dienstnehmer

   a) einer Gebietskörperschaft,
   b) einer öffentlichrechtlichen Rundfunkanstalt,
   c) einer nationalen Zentralbank,
   d) einer gesetzlichen Interessenvertretung
   e) einer erwerbswirtschaftlich geführten, teilweise unter Staatseinfluss stehenden Unternehmung

   verpflichten?

2. Für den Fall, dass der Europäische Gerichtshof die gestellte Frage zumindest teilweise bejaht:

   Sind jene Bestimmungen, die einer nationalen Regelung des geschilderten Inhalts entgegenstehen, in dem Sinn unmittelbar anwendbar, dass sich die zur Offenlegung verpflichteten Personen auf sie berufen können, um eine Anwendung entgegenstehender nationaler Vorschriften zu verhindern?

Rechtssachen C-138/01 und C-139/01

24.

Frau Neukomm und Herr Lauermann - Angestellte des ORF, bei dem es sich um einen der Kontrolle des Rechnungshofes unterliegenden Rechtsträger handelt - beantragten bei den österreichischen Gerichten den Erlass von einstweiligen Verfügungen, um dem ORF die Übermittlung der vom Rechnungshof angeforderten Daten zu untersagen.

25.

Die Anträge auf vorläufigen Rechtsschutz wurden in erster Instanz abgewiesen. Das Arbeits- und Sozialgericht Wien (C-138/01), das zwischen der Übermittlung der Daten an den Rechnungshof und deren Aufnahme in den Bericht unterschied, vertrat die Ansicht, dass Letzteres nur anonymisiert geschehen dürfe, während die bloße, auch namentliche Übermittlung an den Rechnungshof weder gegen Artikel 8 EMRK noch gegen die Richtlinie 95/46 verstoße. Demgegenüber hielt das Landesgericht St. Pölten (Österreich) (C-139/01) die namentliche Aufnahme der Daten in den Bericht für rechtmäßig, da eine anonymisierte Form keine ausreichende Kontrolle gewährleiste.

26.

Das Oberlandesgericht Wien bestätigte im Rekursverfahren die Zurückweisung der Anträge auf vorläufigen Rechtsschutz durch die erstinstanzlichen Gerichte. Während es in der Rechtssache C-138/01 darauf abstellte, dass der Dienstgeber mit der Übermittlung nur einem gesetzlichen Auftrag nachkomme und die weitere Behandlung der Daten durch den Rechnungshof nicht im Einflussbereich des Dienstgebers liege, betonte es in der Rechtssache C-139/01, dass § 8 BezBegrBVG auch bei namentlicher Nennung der betreffenden Personen mit den Grundrechten und der Richtlinie 95/46 vereinbar sei.

27.

Frau Neukomm und Herr Lauermann legten Revisionsrekurs beim Obersten Gerichtshof ein.

28.

Das vorlegende Gericht bezieht sich auf das Vorabentscheidungsersuchen in der Rechtssache C-465/00; es hat sich die Fragen des Verfassungsgerichtshofes zu Eigen gemacht und das Verfahren ausgesetzt, um dem Gerichtshof die beiden folgenden, in den Rechtssachen C-138/01 und C-139/01 identisch formulierten Fragen zur Vorabentscheidung vorzulegen:

1. Sind die gemeinschaftsrechtlichen Vorschriften, insbesondere jene über den Datenschutz (Artikel 1, 2, 6, 7 und 22 der Richtlinie 95/46/EG in Verbindung mit Artikel 6 [früher Artikel F] EU-Vertrag und Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten) so auszulegen, dass sie einer nationalen Regelung entgegenstehen, die eine öffentlich-rechtliche Rundfunkanstalt als Rechtsträger zur Mitteilung und ein staatliches Organ zur Erhebung und Weiterleitung von Einkommensdaten zum Zweck der Veröffentlichung der Namen und Einkommen der Arbeitnehmer einer öffentlich-rechtlichen Rundfunkanstalt verpflichten?

2. Für den Fall, dass der Gerichtshof der Europäischen Gemeinschaften die gestellte Frage bejaht: Sind jene Bestimmungen, die einer nationalen Regelung des geschilderten Inhalts entgegenstehen, in dem Sinn unmittelbar anwendbar, dass sich die zur Offenlegung verpflichtete Anstalt auf sie berufen kann, um eine Anwendung entgegenstehender nationaler Vorschriften zu verhindern und daher von der Offenlegung betroffenen Arbeitnehmern eine nationale gesetzliche Verpflichtung nicht entgegenhalten kann?

*b) Leitsätze*

**1.** Die Artikel 6 Absatz 1 Buchstabe c) und 7 Buchstaben c) und e) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr stehen einer nationalen Regelung nicht entgegen, sofern erwiesen ist, dass die Offenlegung, die nicht nur die Höhe der Jahreseinkommen der Beschäftigten von der Kontrolle des Rechnungshofes unterliegenden Rechtsträgern betrifft, wenn diese Einkommen einen bestimmten Betrag überschreiten, sondern auch die Namen der Bezieher dieser Einkommen umfasst, im Hinblick auf das vom Verfassungsgesetzgeber verfolgte Ziel der ordnungsgemäßen Verwaltung der öffentlichen Mittel notwendig und angemessen ist.
**2.** Die Artikel 6 Absatz 1 Buchstabe c) und 7 Buchstaben c) und e) der Richtlinie 95/46 sind in dem Sinne unmittelbar anwendbar, dass sich ein Einzelner vor den nationalen Gerichten auf sie berufen kann, um die Anwendung entgegenstehender Vorschriften des innerstaatlichen Rechts zu verhindern.
(EuR 2004, 276, beck-online)

*c) Begründung*

[…] Zur ersten Frage
48.

Mit der ersten Frage möchten die vorlegenden Gerichte im Wesentlichen wissen, ob die Richtlinie 95/46 dahin auszulegen ist, dass sie einer nationalen Regelung wie der der Ausgangsverfahren entgegensteht, die ein staatliches Kontrollorgan zur Erhebung und Weitergabe von Daten über die Einkommen der bei den seiner Kontrolle unterliegenden Einrichtungen beschäftigten Personen zum Zweck der Veröffentlichung verpflichtet, sofern diese Einkommen einen bestimmten Betrag überschreiten.
Beim Gerichtshof eingereichte Erklärungen
49.

Die dänische Regierung vertritt die Auffassung, die Richtlinie 95/46 enthalte keine Regelung des Rechts Dritter, auf Antrag Zugang zu Dokumenten zu erhalten. Insbesondere sehe Artikel 12 der Richtlinie nur ein jeder Person zustehendes Recht auf Zugang zu den sie selbst betreffenden Daten vor. Der Schutz personenbezogener, nicht sensibler Informationen müsse vor dem Grundsatz der Transparenz zurücktreten, der eine zentrale Stellung in der Gemeinschaftsrechtsordnung einnehme. Die dänische Regierung verweist insoweit - ebenso wie die schwedische Regierung - auf die 72. Begründungserwägung der Richtlinie, nach der bei der Umsetzung der Grundsatz des öffentlichen Zugangs zu amtlichen Dokumenten berücksichtigt werden dürfe.
50.

Der Rechnungshof, die österreichische, die italienische, die niederländische, die finnische und die schwedische Regierung sowie die Kommission sind der Ansicht, dass die den Ausgangsverfahren zugrunde liegende nationale Regelung mit der Richtlinie 95/46 vereinbar sei, da die Mitgliedstaaten bei der Umsetzung der Richtlinie grundsätzlich über ein weites Ermessen verfügten, was insbesondere dann gelte, wenn es um die Wahrnehmung einer im öffentlichen Interesse liegenden, gesetzlich vorgesehenen Aufgabe auf der Grundlage der Artikel 6 Buchstaben b und c sowie 7 Buchstaben c oder e der Richtlinie gehe. Hierfür werden die Grundsätze der Transparenz und der ordnungsgemäßen Verwaltung öffentlicher Mittel sowie die Verhinderung von Missbrauchsfällen angeführt.
51.

Diese im Allgemeininteresse liegenden Ziele könnten einen Eingriff in das durch Artikel 8 Absatz 2 EMRK garantierte Recht auf Achtung des Privatlebens rechtfertigen, wenn dieser Eingriff gesetzlich vorgesehen, in einer demokratischen Gesellschaft zur Verwirklichung berechtigter Zwecke notwendig und in Anbetracht des verfolgten Zieles nicht unverhältnismäßig sei.
52.

Die österreichische Regierung macht insbesondere geltend, im Rahmen der Verhältnismäßigkeitsprüfung sei auch zu berücksichtigen, wie stark der Bezug der Daten zum Privatleben sei. So seien Daten, die den intimsten Kern der Person, die Gesundheit, das Familienleben oder die Sexualität beträfen, in stärkerem Maße schutzwürdig als Einkommens- und Steuerdaten, die zwar ebenfalls personenbezogen seien, aber in geringerem Maße die Identität der Person beträfen und insofern weniger sensibel seien (in diesem Sinne EGMR, Urteil Fressoz und Roire/Frankreich vom 21. Januar 1999, *Recueil des arrêts et décisions* 1999-I, § 65).
53.

Auch die finnische Regierung ist der Auffassung, der Schutz der Privatsphäre sei nicht absolut. So fielen Daten, die einen öffentlichen Amts- oder Funktionsträger in seiner Tätigkeit beträfen, nicht unter den Schutz der Privatsphäre.
54.

Die italienische Regierung macht geltend, Daten wie die in den Ausgangsverfahren betroffenen seien in den meisten Mitgliedstaaten ihrem Wesen nach bereits öffentlich zugänglich, da sie sich aus in Gesetzen, Verordnungen oder Tarifverträgen enthaltenen Lohn- und Gehaltstabellen ergäben. Daher verstoße es nicht gegen den

Grundsatz der Verhältnismäßigkeit, ihre Verbreitung auch unter Nennung der einzelnen Empfänger der Bezüge vorzusehen. Diese Verbreitung solle nämlich nur einen bereits aus allgemein zugänglichen Daten hervorgehenden Sachverhalt verdeutlichen und stelle die am wenigsten einschneidende Maßnahme dar, um die Verwirklichung der Ziele der Transparenz und der ordnungsgemäßen Verwaltung sicherzustellen.

55.

Die niederländische Regierung weist darauf hin, dass die vorlegenden Gerichte für jeden der betroffenen Rechtsträger gesondert zu prüfen hätten, ob das im Allgemeininteresse liegende Ziel auch erreicht werden könne, wenn die personenbezogenen Daten in einer Weise verarbeitet würden, die weniger in die Privatsphäre der Betroffenen eingreife.

56.

Die Regierung des Vereinigten Königreichs macht geltend, die am 18. Dezember 2000 in Nizza vom Europäischen Rat proklamierte Charta der Grundrechte der Europäischen Union (ABl. C 364, S. 1), auf die der Verfassungsgerichtshof kurz eingegangen ist, sei für die Beantwortung der ersten Frage ohne Bedeutung.

57.

Die Kommission stellt sich in den Rechtssachen C-138/01 und C-139/01 bei der Verhältnismäßigkeitsprüfung im Rahmen von Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46 die Frage, ob es zur Erreichung des mit dem BezBegrBVG verfolgten Zieles nicht ausreiche, die Daten in anonymisierter Form zu übermitteln, etwa durch Angabe der Funktionsbezeichnung anstelle des Namens des Betroffenen. Selbst wenn der Rechnungshof zur genaueren Kontrolle über die individualisierten Daten verfügen müsse, könne man doch bezweifeln, ob es für die Kontrolle wirklich erforderlich sei, die Daten mit Namensnennung in den Bericht aufzunehmen, zumal wenn dieser nicht nur dem Parlament zugeleitet werde, sondern auch noch veröffentlicht werden müsse.

58.

Außerdem weist die Kommission darauf hin, dass die Mitgliedstaaten nach Artikel 13 der Richtlinie 95/46 u. a. von Artikel 6 Absatz 1 Buchstabe b der Richtlinie abweichen könnten, um bestimmte im Allgemeininteresse liegende Ziele zu verfolgen, zu denen auch „ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats“ (Artikel 13 Absatz 1 Buchstabe e) zähle. Die abweichenden Maßnahmen müssten jedoch ebenfalls dem Grundsatz der Verhältnismäßigkeit entsprechen, wobei dieselben Überlegungen wie in der vorstehenden Randnummer zu Artikel 6 Absatz 1 Buchstabe b der Richtlinie anzustellen seien.

59.

Die Antragsgegner des Ausgangsverfahrens in der Rechtssache C-465/00 sind durchweg der Auffassung, die streitige nationale Regelung sei unvereinbar mit Artikel 6 Absatz 1 Buchstaben b und c der Richtlinie 95/46 und könne auch nicht nach Artikel 7 Buchstaben c oder e der Richtlinie als zulässig angesehen werden, da sie einen nicht gerechtfertigten Eingriff in Artikel 8 Absatz 2 EMRK darstelle und jedenfalls unverhältnismäßig sei. Die Gebarungskontrolle durch den Rechnungshof reiche aus, um den sparsamen Einsatz öffentlicher Gelder zu gewährleisten.

60.

Insbesondere sei nicht erwiesen, dass die Veröffentlichung der Namen und der Einkommenshöhe aller bei einer öffentlichen Einrichtung Beschäftigten, deren Bezüge einen bestimmten Grenzbetrag überstiegen, eine Maßnahme darstelle, die dem wirtschaftlichen Wohl des Landes diene. Ziel des Verfassungsgebers sei es gewesen, auf die betroffenen Rechtsträger Druck auszuüben, um die Gehälter niedrig zu halten. Diese Maßnahme treffe Personen, bei denen es sich größtenteils nicht um Persönlichkeiten des öffentlichen Lebens handele.

61.

Selbst wenn man im Übrigen die Erstellung eines für die öffentliche Debatte bestimmten Berichts mit personenbezogenen Einkommensdaten durch den Rechnungshof für einen nach Artikel 8 Absatz 2 EMRK gerechtfertigten Eingriff in das Privatleben halte, verstößt diese Maßnahme nach Auffassung des Landes Niederösterreich und des ORF nichtdestoweniger gegen Artikel 14 EMRK. Es würden nämlich Bezieher gleich hoher Einkommen ungleich behandelt, je nachdem, ob sie bei einem vom Rechnungshof kontrollierten Rechtsträger beschäftigt seien oder nicht.

62.

Der ORF rügt noch eine weitere nach Artikel 14 EMRK nicht gerechtfertigte Ungleichbehandlung. Unter den Arbeitnehmern der vom Rechnungshof kontrollierten Rechtsträger müssten nur diejenigen einen Eingriff in ihre Privatsphäre dulden, deren Bezüge den Grenzbetrag nach § 8 BezBegrBVG überschritten. Wenn es dem Gesetzgeber wirklich um die Angemessenheit der Entlohnung von Arbeitnehmern bestimmter Rechtsträger ginge, so müssten die Gehälter aller Arbeitnehmer, unabhängig von ihrer Höhe, offen gelegt werden.

63.

Schließlich tragen der ORF, die Marktgemeinde Kaltenleutgeben und die Austrian Airlines, Österreichische Luftverkehrs-AG, vor, der Wortlaut von § 8 BezBegrBVG ermögliche eine gemeinschaftsrechtskonforme Auslegung dahin, dass die betreffenden Bezüge nur in anonymisierter Form an den Rechnungshof zu übermitteln und im Bericht zu veröffentlichen seien. Diese Auslegung verdiene den Vorzug, da sie den Widerspruch zwischen der genannten Bestimmung und der Richtlinie 95/46 auflösen könne.

Antwort des Gerichtshofes

64.

Vorab ist festzustellen, dass die in den Ausgangsverfahren betroffenen Daten, die sich sowohl auf die von bestimmten Rechtsträgern gezahlten Bezüge als auch auf deren Empfänger beziehen, personenbezogene Daten im Sinne von Artikel 2 Buchstabe a der Richtlinie 95/46 sind, da sie „Informationen über eine bestimmte oder bestimmbare natürliche Person“ darstellen. Die Speicherung und Nutzung dieser Daten durch die betroffene Einrichtung sowie ihre Übermittlung an den Rechnungshof und ihre Aufnahme in einen Bericht, der zur Vorlage bei verschiedenen politischen Organen und zur weiten Verbreitung bestimmt ist, erfüllen den Tatbestand der Verarbeitung personenbezogener Daten im Sinne von Artikel 2 Buchstabe b der genannten Richtlinie.

65.

Nach der Richtlinie 95/46 muss jedoch jede Verarbeitung personenbezogener Daten - vorbehaltlich der in Artikel 13 zugelassenen Ausnahmen - den in Artikel 6 der Richtlinie aufgestellten „Grundsätzen in Bezug auf die Qualität der Daten“ und einem der in Artikel 7 enthaltenen „Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten“ genügen.

66.

Die Daten müssen insbesondere „für festgelegte eindeutige und rechtmäßige Zwecke erhoben“ werden (Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46), sie müssen diesen „Zwecken entsprechen ..., dafür erheblich [sein] und [dürfen] nicht darüber hinausgehen“ (Artikel 6 Absatz 1 Buchstabe c). Gemäß Artikel 7 Buchstaben c und e der Richtlinie ist die Verarbeitung personenbezogener Daten zulässig, wenn sie „für die Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der für die Verarbeitung Verantwortliche unterliegt“ oder wenn sie „erforderlich [ist] für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen ..., dem die Daten übermittelt werden, übertragen wurde“.

67.

Allerdings können die Mitgliedstaaten gemäß Artikel 13 Buchstaben e und f der Richtlinie 95/46 u. a. von Artikel 6 Absatz 1 der Richtlinie abweichen, wenn dies notwendig ist für „ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten“ oder für „Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt“ für besondere Zwecke verbunden sind, zu denen der in Buchstabe e genannte gehört.

68.

Weiter ist zu berücksichtigen, dass die Bestimmungen der Richtlinie 95/46, soweit sie die Verarbeitung personenbezogener Daten betreffen, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung des Privatlebens führen kann, im Licht der Grundrechte auszulegen sind, die nach ständiger Rechtsprechung zu den allgemeinen Rechtsgrundsätzen gehören, deren Wahrung der Gerichtshof zu sichern hat (vgl. u. a. Urteil vom 6. März 2001 in der Rechtssache C-274/99 P, Connolly/Kommission, Slg. 2001, I-1611, Randnr. 37).

69.

Diese Grundsätze sind ausdrücklich in Artikel 6 Absatz 2 EU aufgenommen worden, der wie folgt lautet: „Die Union achtet die Grundrechte, wie sie in der [EMRK] gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.“

70.

Obwohl die Richtlinie 95/46 als Hauptziel die Gewährleistung des freien Verkehrs personenbezogener Daten anstrebt, bestimmt sie in Artikel 1 Absatz 1, dass „[d]ie Mitgliedstaaten ... den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“ gewährleisten. Dasselbe Erfordernis kommt auch in mehreren Begründungserwägungen der Richtlinie - insbesondere in der zehnten und elften - zum Ausdruck.

71.

Während in Artikel 8 Absatz 1 EMRK der Grundsatz aufgestellt wird, dass Behörden nicht in die Ausübung des Rechts auf Achtung des Privatlebens eingreifen dürfen, wird in Absatz 2 ein solcher Eingriff für zulässig erklärt, soweit er „gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten Anderer notwendig ist“.

72.

Für die Anwendung der Richtlinie 95/46 und insbesondere der Artikel 6 Absatz 1 Buchstabe c, 7 Buchstaben c und e und 13 ist daher zunächst zu prüfen, ob eine Regelung wie die den Ausgangsverfahren zugrunde liegende einen Eingriff in die Privatsphäre darstellt und gegebenenfalls ob ein solcher Eingriff nach Artikel 8 EMRK gerechtfertigt ist.

Zum Vorliegen eines Eingriffs in die Privatsphäre

73.

Hierzu ist sogleich festzustellen, dass die Erhebung personenbezogener Daten über die beruflichen Einkünfte Einzelner zur Weitergabe an Dritte in den Anwendungsbereich von Artikel 8 EMRK fällt. Der Europäische Gerichtshof für Menschenrechte hat insoweit entschieden, dass der Begriff „Privatleben“ nicht eng ausgelegt werden darf und dass es „grundsätzlich nicht in Betracht kommt, berufliche Tätigkeiten ... vom Begriff des

.Privatlebens‘ auszunehmen“ (vgl. insbesondere EGMR, Urteile Amann/Schweiz vom 16. Februar 2000, *Recueil des arrêts et décisions* 2000-II, § 65, und Rotaruc/Rumänien vom 4. Mai 2000, *Recueil des arrêts et décisions* 2000-V, § 43).

74.

Zwar kann die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber als solche keinen Eingriff in die Privatsphäre begründen, doch stellt die Weitergabe dieser Daten an einen Dritten - im vorliegenden Fall an eine Behörde - unabhängig von der späteren Verwendung der übermittelten Informationen eine Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens und damit einen Eingriff im Sinne von Artikel 8 EMRK dar.

75.

Für die Feststellung eines solchen Eingriffs kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben (in diesem Sinne Urteil Amann/Schweiz, § 70). Es genügt die Tatsache, dass Daten über die Einkünfte eines Arbeitnehmers oder eines Ruhegehaltsempfängers vom Arbeitgeber an einen Dritten weitergeleitet worden sind.

Zur Rechtfertigung des Eingriffs

76.

Ein Eingriff wie der in Randnummer 74 des vorliegenden Urteils beschriebene verstößt gegen Artikel 8 EMRK, es sei denn, er ist „gesetzlich vorgesehen“, verfolgt eines oder mehrere der in Absatz 2 dieses Artikels genannten berechtigten Ziele, und ist „in einer demokratischen Gesellschaft“ für die Erreichung dieses Zieles oder dieser Ziele notwendig.

77.

Der in den Ausgangsverfahren streitige Eingriff ist in § 8 BezBegrBVG vorgesehen. Allerdings stellt sich die Frage, ob diese Bestimmung so genau formuliert ist, dass die Adressaten des Gesetzes ihr Verhalten einrichten können, und damit dem Erfordernis der Vorhersehbarkeit genügt, wie es in der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte entwickelt worden ist (vgl. u. a. EGMR, Urteil Rekvényi/Ungarn vom 20. Mai 1999, *Recueil des arrêts et décisions* 1999-III, § 34).

78.

§ 8 Absatz 3 BezBegrBVG sieht vor, dass in den Bericht des Rechnungshofes „alle Personen aufzunehmen [sind], deren jährliche Bezüge und Ruhebezüge von Rechtsträgern, die der Kontrolle des Rechnungshofes unterliegen, insgesamt den im Absatz 1 genannten Betrag übersteigen“, ohne dass ausdrücklich die Offenlegung der Namen der Betroffenen in Verbindung mit dem von ihnen erzielten Einkommen vorgeschrieben würde. Nach den Angaben in den Vorlagebeschlüssen wurde diese Auslegung des Bundes-Verfassungsgesetzes erst in der Lehre auf der Grundlage der Gesetzesmaterialien entwickelt.

79.

Die vorlegenden Gerichte haben zu prüfen, ob die Auslegung, nach der § 8 Absatz 3 BezBegrBVG die Offenlegung der Namen der Betroffenen mit ihrem jeweiligen Einkommen verlangt, dem in Randnummer 77 des vorliegenden Urteils erwähnten Erfordernis der Vorhersehbarkeit entspricht.

80.

Diese Frage stellt sich jedoch gegebenenfalls erst nach der Prüfung der Vereinbarkeit einer solchen Auslegung der fraglichen nationalen Bestimmung mit Artikel 8 EMRK in Bezug auf das Erfordernis der Verhältnismäßigkeit im Hinblick auf die verfolgten Ziele. Diese letztgenannte Frage wird in den folgenden Randnummern untersucht.

81.

Hierzu ergibt sich aus dem Vorlagebeschluss in der Rechtssache C-465/00, dass der Zweck von § 8 BezBegrBVG darin besteht, auf die betroffenen Rechtsträger Druck auszuüben, um die Bezüge in angemessenen Grenzen zu halten. Die österreichische Regierung hat allgemein darauf hingewiesen, dass mit dem in dieser Bestimmung vorgesehenen Eingriff die sparsame und sachgerechte Verwendung öffentlicher Mittel durch die Verwaltung gewährleistet werden soll. Ein solches Ziel ist als berechtigter Zweck sowohl im Sinne von Artikel 8 Absatz 2 EMRK, der auf das „wirtschaftliche Wohl des Landes“ abstellt, als auch von Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46 anzusehen, der auf „festgelegte, eindeutige und rechtmäßige Zwecke“ Bezug nimmt.

82.

Es bleibt zu prüfen, ob der fragliche Eingriff in einer demokratischen Gesellschaft für die Erreichung des mit ihm verfolgten berechtigten Zweckes notwendig ist.

83.

Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte bedeutet das Eigenschaftswort „notwendig“ in Artikel 8 Absatz 2 EMRK, dass ein „zwingendes gesellschaftliches Bedürfnis“ bestehen und die Maßnahme „in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck“ stehen muss (vgl. u. a. EGMR, Urteil Gillow/Vereinigtes Königreich vom 24. November 1986, Série A, Nr. 109, § 55). Die nationalen Behörden verfügen zudem über ein Ermessen, „dessen Umfang nicht nur von der Zielsetzung, sondern auch vom Wesen des Eingriffs abhängig ist“ (vgl. EGMR, Urteil Leander/Schweden vom 26. März 1987, Série A, Nr. 116, § 59).

84.

In diesem Sinne ist das Interesse der Republik Österreich an der Gewährleistung der bestmöglichen Verwendung öffentlicher Mittel und insbesondere an einer angemessenen Begrenzung der Bezüge gegen die Schwere der Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens abzuwägen.

85.

Einerseits müssen der Rechnungshof und die verschiedenen parlamentarischen Organe zweifellos die Höhe der Personalkosten der verschiedenen öffentlichen Einrichtungen kennen, um die ordnungsgemäße Verwendung der öffentlichen Mittel kontrollieren zu können. Außerdem haben in einer demokratischen Gesellschaft die Steuerzahler und ganz allgemein die Öffentlichkeit einen Anspruch darauf, über die Verwendung der öffentlichen Gelder gerade im Bereich der Personalkosten informiert zu werden. Die Verbreitung solcher Informationen in einem Bericht kann zur öffentlichen Diskussion über Fragen von allgemeinem Interesse beitragen; sie dient daher dem öffentlichen Interesse.

86.

Dennoch stellt sich die Frage, ob die Angabe der Namen der Betroffenen in Verbindung mit deren Einkünften in einem angemessenen Verhältnis zu dem mit der Maßnahme verfolgten berechtigten Zweck steht und ob die im Verfahren vor dem Gerichtshof zur Rechtfertigung einer solchen Veröffentlichung angeführten Gründe stichhaltig und ausreichend sind.

87.

Hierzu ist festzustellen, dass § 8 BezBegrBVG nach der Auslegung der vorlegenden Gerichte die Veröffentlichung der Namen der Betroffenen in Verbindung mit deren Einkünften, soweit diese einen bestimmten Betrag überschreiten, nicht nur für Inhaber von Ämtern vorschreibt, deren Bezüge aus einer öffentlich zugänglichen Tabelle hervorgehen, sondern allgemein für alle Personen, die von einem der Kontrolle des Rechnungshofes unterliegenden Rechtsträger bezahlt werden. Außerdem werden diese Informationen nicht nur dem Rechnungshof und über diesen den verschiedenen parlamentarischen Organen zugeleitet, sondern auch einer breiten Öffentlichkeit zugänglich gemacht.

88.

Die vorlegenden Gerichte haben zu prüfen, ob eine solche Veröffentlichung notwendig ist und in einem angemessenen Verhältnis zu dem Ziel steht, die Bezüge innerhalb angemessener Grenzen zu halten; sie haben insbesondere zu untersuchen, ob dieser Zweck nicht ebenso wirksam erreicht werden könnte, wenn die personenbezogenen Daten nur den Kontrollorganen zugänglich gemacht würden. Weiter stellt sich die Frage, ob es nicht ausreichend wäre, die Öffentlichkeit nur über die Bezüge und anderen geldwerten Vorteile zu unterrichten, auf die die Beschäftigten öffentlicher Einrichtungen auf vertraglicher oder statutarischer Grundlage Anspruch haben, ohne die Beträge anzugeben, die die jeweiligen Beschäftigten in einem bestimmten Jahr erhalten haben und die in unterschiedlichem Ausmaß von deren familiärer und persönlicher Situation abhängig sein können.

89.

Was andererseits die Schwere der Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens angeht, so ist nicht ausgeschlossen, dass diese Personen durch die negativen Auswirkungen der Veröffentlichung ihres beruflichen Einkommens insbesondere im Hinblick auf ihre Einstellungsmöglichkeiten bei anderen Unternehmen innerhalb oder außerhalb Österreichs, die nicht der Kontrolle des Rechnungshofes unterliegen, geschädigt werden können.

90.

Folglich ist festzustellen, dass der mit der Anwendung einer nationalen Regelung wie der der Ausgangsverfahren verbundene Eingriff nur dann nach Artikel 8 Absatz 2 EMRK gerechtfertigt werden kann, wenn die Offenlegung, die nicht nur die Höhe der Jahreseinkommen der Beschäftigten von der Kontrolle des Rechnungshofes unterliegenden Rechtsträgern betrifft, sofern diese Einkommen einen bestimmten Betrag überschreiten, sondern auch die Namen der Bezieher dieser Einkommen umfasst, im Hinblick auf das Ziel einer sachgerechten Begrenzung der Bezüge sowohl notwendig als auch angemessen ist, was die vorlegenden Gerichte zu prüfen haben.

Zu den Auswirkungen auf die Bestimmungen der Richtlinie 95/46

91.

Sollten die vorlegenden Gerichte die den Ausgangsverfahren zugrunde liegende nationale Regelung für unvereinbar mit Artikel 8 EMRK halten, so kann diese Regelung auch nicht dem Erfordernis der Verhältnismäßigkeit nach Artikel 6 Absatz 1 Buchstabe c und Artikel 7 Buchstaben c oder e der Richtlinie 95/46 genügen. Sie kann nicht unter eine der Ausnahmen nach Artikel 13 der Richtlinie fallen, da auch dies die Einhaltung des Erfordernisses der Verhältnismäßigkeit im Hinblick auf das mit der Maßnahme verfolgte, im Allgemeininteresse liegende Ziel voraussetzen würde. Jedenfalls kann diese Bestimmung nicht so ausgelegt werden, dass sie eine gegen Artikel 8 EMRK verstoßende Beeinträchtigung des Rechts auf Achtung des Privatlebens rechtfertigen könnte.

92.

Sollten die vorlegenden Gerichte dagegen zu dem Ergebnis gelangen, dass § 8 BezBegrBVG im Hinblick auf das mit der Bestimmung verfolgte, im Allgemeininteresse liegende Ziel sowohl notwendig als auch angemessen ist, so haben sie - wie sich aus den Randnummern 77 bis 79 des vorliegenden Urteils ergibt - weiter zu prüfen, ob Artikel 8 BezBegrBVG, der nicht ausdrücklich die Veröffentlichung der Namen der Betroffenen in Verbindung mit deren Einkommen vorsieht, dem Erfordernis der Vorhersehbarkeit entspricht.

93.

In Anbetracht der vorstehenden Erwägungen ist schließlich darauf hinzuweisen, dass die nationalen Gerichte jede Bestimmung des innerstaatlichen Rechts so weit wie möglich anhand des Wortlauts und des Zweckes der einschlägigen Richtlinie auszulegen haben, um das mit der Richtlinie verfolgte Ziel zu erreichen und Artikel 249 Absatz 3 EG nachzukommen (vgl. Urteil vom 13. November 1990 in der Rechtssache C-106/89, Marleasing, Slg. 1990, I-4135, Randnr. 8).

94.

Nach alledem ist auf die erste Vorlagefrage zu antworten, dass die Artikel 6 Absatz 1 Buchstabe c und 7 Buchstaben c und e der Richtlinie 95/46 einer nationalen Regelung wie der den Ausgangsverfahren zugrunde liegenden nicht entgegenstehen, sofern erwiesen ist, dass die Offenlegung, die nicht nur die Höhe der Jahreseinkommen der Beschäftigten von der Kontrolle des Rechnungshofes unterliegenden Rechtsträgern betrifft, wenn diese Einkommen einen bestimmten Betrag überschreiten, sondern auch die Namen der Bezieher dieser Einkommen umfasst, im Hinblick auf das vom Verfassungsgesetzgeber verfolgte Ziel der ordnungsgemäßen Verwaltung der öffentlichen Mittel notwendig und angemessen ist, was die vorlegenden Gerichten zu prüfen haben.

Zur zweiten Frage

95.

Mit der zweiten Frage möchten die vorlegenden Gerichte wissen, ob die Bestimmungen der Richtlinie 95/46, die einer nationalen Regelung wie der den Ausgangsverfahren zugrunde liegenden entgegenstehen, in dem Sinne unmittelbar anwendbar sind, dass sich ein Einzelner vor den nationalen Gerichten auf sie berufen kann, um die Anwendung dieser Regelung zu verhindern.

96.

Die Antragsgegner des Ausgangsverfahrens in der Rechtssache C-465/00 sowie die niederländische Regierung sind der Auffassung, dass die Artikel 6 Absatz 1 und 7 der Richtlinie 95/46 den in der Rechtsprechung des Gerichtshofes aufgestellten Voraussetzungen für eine unmittelbare Wirkung genügten. Die genannten Bestimmungen seien so genau und unbedingt, dass sich die zur Weitergabe von Daten über die Einkommen der Betroffenen verpflichteten Einrichtungen auf sie berufen könnten, um die Anwendung entgegenstehender nationaler Regelungen zu verhindern.

97.

Die österreichische Regierung macht dagegen geltend, die einschlägigen Bestimmungen der Richtlinie 95/46 seien nicht unmittelbar anwendbar. Insbesondere seien die Artikel 6 Absatz 1 und 7 der Richtlinie nicht inhaltlich unbedingt, da ihre Umsetzung erfordere, dass die Mitgliedstaaten, die über ein weites Ermessen verfügten, besondere Ausführungsmaßnahmen erließen.

98.

Hierzu ist daran zu erinnern, dass sich der Einzelne in Ermangelung fristgemäß erlassener Umsetzungsmaßnahmen auf Bestimmungen einer Richtlinie, die inhaltlich unbedingt und hinreichend genau sind, gegenüber allen nicht richtlinienkonformen innerstaatlichen Vorschriften berufen kann; er kann sich auf diese Bestimmungen auch berufen, soweit sie so geartet sind, dass sie Rechte festlegen, die der Einzelne dem Staat gegenüber geltend machen kann (vgl. u. a. Urteile vom 19. Januar 1982 in der Rechtssache 8/81, Becker, Slg. 1982, 53, Randnr. 25, und vom 10. September 2002 in der Rechtssache C-141/00, Kügler, Slg. 2002, I-6833, Randnr. 51).

99.

Angesichts der Antwort auf die erste Frage läuft die zweite Frage darauf hinaus, ob Artikel 6 Absatz 1 Buchstabe c der Richtlinie 95/46, wonach personenbezogene Daten „den Zwecken entsprechen müssen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich [sein müssen] und nicht darüber hinausgehen [dürfen]“, und Artikel 7 Buchstaben c und e der Richtlinie, wonach die Verarbeitung personenbezogener Daten nur erfolgen darf, wenn sie „für die Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der für die Verarbeitung Verantwortliche unterliegt“, oder wenn sie „erforderlich [ist] für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen ..., dem die Daten übermittelt werden, übertragen wurde“, diese Voraussetzungen erfüllen.

100.

Diese Bestimmungen sind so genau, dass sich ein Einzelner auf sie berufen und ein nationales Gericht sie anwenden kann. Zwar räumt die Richtlinie 95/46 den Mitgliedstaaten unbestreitbar ein mehr oder weniger großes Ermessen bei der Umsetzung einiger ihrer Bestimmungen ein, doch begründen die Artikel 6 Absatz 1 Buchstabe c und 7 Buchstaben c und e unbedingte Verpflichtungen.

101.

Damit ist auf die zweite Frage zu antworten, dass die Artikel 6 Absatz 1 Buchstabe c und 7 Buchstaben c und e der Richtlinie 95/46 in dem Sinne unmittelbar anwendbar sind, dass sich ein Einzelner vor den nationalen Gerichten auf sie berufen kann, um die Anwendung entgegenstehender Vorschriften des innerstaatlichen Rechts zu verhindern. […]

**2) EuGH C-92, C-93/09 - Volker und Markus Schecke GbR, Hartmut Eifert**

*a) Sachverhalt*

Bei den Klägern der Ausgangsverfahren, von denen einer in Hessen niedergelassen ist und der andere dort wohnt, handelt es sich um einen landwirtschaftlichen Betrieb in Form einer Gesellschaft bürgerlichen Rechts (Rechtssache C‑92/09) und um einen Inhaber eines landwirtschaftlichen Vollerwerbsbetriebs (Rechtssache C‑93/09). Sie haben für das Wirtschaftsjahr 2008 bei der zuständigen lokalen Behörde Anträge auf Agrarbeihilfen aus dem EGFL oder dem ELER gestellt, denen mit Bescheiden vom 5. Dezember 2008 (Rechtssache C‑93/09) und vom 31. Dezember 2008 (Rechtssache C‑92/09) entsprochen wurde.

26 In beiden Fällen enthielt das Antragsformular folgenden Hinweis:

„Mir ist bekannt, dass nach Art. 44a der [Verordnung] Nr. 1290/2005 vorgeschrieben ist, Informationen über die Empfänger von EGFL- und ELER-Mitteln sowie die Beträge, die jeder Begünstigte erhalten hat, zu veröffentlichen. Die Veröffentlichung betrifft alle Maßnahmen, die im Zusammenhang mit dem Gemeinsamen Antrag als Sammelantrag im Sinne von Art. 11 der [Verordnung] Nr. 796/2004 beantragt werden und erfolgt alljährlich bis spätestens zum 31. März des Folgejahres."

27 Das vorlegende Gericht führt aus, auf der Internetseite der Bundesanstalt würden die Namen der Empfänger von EGFL- und ELER-Mitteln, der Niederlassungs- oder Wohnort der Empfänger mit Postleitzahl und die Höhe der Jahresbeträge bereitgestellt. Die Seite sei mit einer Suchfunktion ausgestattet.

28 Die Kläger der Ausgangsverfahren erhoben am 26. September 2008 (Rechtssache C‑92/09) bzw. am 18. Dezember 2008 (Rechtssache C‑93/09) Klage mit dem Ziel, die Veröffentlichung ihrer Daten zu verhindern. Die Veröffentlichung der ihnen aus dem EGFL oder dem ELER gewährten Beträge sei nicht durch überwiegende Allgemeininteressen gerechtfertigt. Im Übrigen sei in den Regeln zum Europäischen Sozialfonds keine namentliche Nennung der Empfänger vorgesehen. Sie beantragen, das Land Hessen zu verpflichten, die Weitergabe oder Veröffentlichung dieser Daten zu unterlassen bzw. durch Anordnung zu untersagen, soweit die Weitergabe zum Zweck der allgemeinen Veröffentlichung von Informationen über die den Klägern gewährten finanziellen Beträge aus dem EGFL und dem ELER erfolgen soll.

29 Das Land Hessen, das der Ansicht ist, die Pflicht zur Veröffentlichung der die Kläger der Ausgangsverfahren betreffenden Daten ergebe sich aus den Verordnungen Nrn. 1290/2005 und 259/2008, hat gleichwohl zugesichert, die von den Klägern der Ausgangsverfahren als Empfänger von EGFL- und ELER-Mitteln erhaltenen Beträge nicht vor dem Erlass einer rechtskräftigen Entscheidung in den Ausgangsverfahren zu veröffentlichen.

30 Das vorlegende Gericht sieht in der Pflicht zur Veröffentlichung nach Art. 44a der Verordnung Nr. 1290/2005 einen Eingriff in das Grundrecht auf Schutz der personenbezogenen Daten, der nicht gerechtfertigt sei. Diese Vorschrift, die das Ziel verfolge, die Transparenz in Bezug auf die Verwendung der Mittel aus europäischen Fonds zu erhöhen, verbessere nicht die Verhütung von Unregelmäßigkeiten, für die umfangreiche Kontrollmechanismen bestünden. Unter Hinweis auf das Urteil des Gerichtshofs vom 20. Mai 2003, Österreichischer Rundfunk u. a. (C‑465/00, C‑138/01 und C‑139/01, Slg. 2003, I‑4989), vertritt es die Meinung, dass diese Pflicht zur Veröffentlichung jedenfalls nicht in einem angemessenen Verhältnis zu dem verfolgten Zweck stehe. Außerdem gewähre Art. 42 Nr. 8b der Verordnung Nr. 1290/2005 der Kommission bei der Festlegung, welche Daten in welcher Weise veröffentlicht würden, einen zu weiten Ermessensspielraum und sei deshalb mit Art. 202 dritter Gedankenstrich EG und Art. 211 vierter Gedankenstrich EG unvereinbar.

31 Unabhängig von der Frage der Gültigkeit der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 verstößt nach Auffassung des vorlegenden Gerichts die Verordnung Nr. 259/2008, die die Veröffentlichung von Informationen über die Empfänger von EGFL- und ELER-Mitteln ausschließlich im Internet vorsieht, gegen das Grundrecht auf Schutz personenbezogener Daten. Es hebt hervor, dass diese Verordnung den Zugriff auf die betreffende Internetseite nicht auf „Internet Protocol"-Adressen (im Folgenden: IP-Adressen) aus der Europäischen Union beschränke. Im Übrigen sei es nicht möglich, die Daten nach Ablauf des in Art. 3 Abs. 3 der Verordnung Nr. 259/2008 vorgesehenen Zeitraums von zwei Jahren aus dem Internet zu entfernen. Zudem habe die ausschließliche Veröffentlichung der Daten im Internet abschreckenden Charakter. Zum einen müssten diejenigen Bürger, die sich informieren wollten, Zugang zum Internet haben. Zum anderen setzten sich diese Bürger einer Vorratsdatenspeicherung nach der Richtlinie 2006/24 aus. Es sei ein Wertungswiderspruch darin zu sehen, einerseits die Telekommunikation verstärkt zu überwachen und andererseits Informationen, die der Teilnahme der Bürger an öffentlichen Angelegenheiten dienen sollten, nur elektronisch zugänglich zu machen.

32 Für den Fall, dass der Gerichtshof die in den Randnrn. 30 und 31 des vorliegenden Urteils genannten Vorschriften für gültig erachten sollte, ersucht das vorlegende Gericht ferner um Auslegung bestimmter Vorschriften der Richtlinie 95/46. Seiner Ansicht nach darf eine Veröffentlichung von personenbezogenen Daten erst erfolgen, wenn die Maßnahmen nach Art. 18 Abs. 2 zweiter Gedankenstrich dieser Richtlinie durchgeführt worden seien. Nach den Angaben des vorlegenden Gerichts hat der deutsche Gesetzgeber und insbesondere der hessische Gesetzgeber von der in dieser Bestimmung vorgesehenen Möglichkeit Gebrauch gemacht. Jedoch sei die Meldung des Hessischen Ministeriums für Umwelt, ländlichen Raum und Verbraucherschutz bei dem Datenschutzbeauftragten unvollständig erfolgt. Bestimmte Angaben wie die Datenverarbeitung durch die Bundesanstalt, gegebenenfalls unter Einschaltung eines privaten Dritten, konkrete Angaben zu den Löschungsfristen und zum Provider sowie Angaben über die Speicherung von IP-Adressen seien ihm nicht übermittelt worden.

33 Außerdem hätte bei der Veröffentlichung von Informationen über die Empfänger von Agrarbeihilfen eine Vorabkontrolle nach Art. 20 der Richtlinie 95/46 durchgeführt werden müssen. In den vorliegenden Fällen sei diese Vorabkontrolle jedoch nicht durch eine zentrale Kontrollstelle, sondern bei der verantwortlichen Stelle durch deren betrieblichen oder behördlichen Datenschutzbeauftragten und auf der Grundlage unvollständiger Meldungen erfolgt.

34 Schließlich stellt sich für das vorlegende Gericht noch die Frage, ob im Hinblick auf Art. 7 Buchst. e der Richtlinie 95/46 die IP-Adressen der Benutzer, die die Informationen über die Empfänger von EGFL- und ELER-Mitteln auf der Internetseite der Bundesanstalt abrufen, gespeichert werden dürfen.

35 Unter diesen Umständen hat das Verwaltungsgericht Wiesbaden beschlossen, die Verfahren auszusetzen und dem Gerichtshof folgende, in den beiden Rechtssachen C‑92/09 und C‑93/09 gleichlautende Fragen zur Vorabentscheidung vorzulegen:

1. Sind die Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005, eingefügt durch die Verordnung Nr. 1437/2007, ungültig?

2. Ist die Verordnung Nr. 259/2008

a) ungültig,

b) oder nur deshalb gültig, weil die Richtlinie 2006/24 ungültig ist?

Falls die in der ersten und der zweiten Frage genannten Vorschriften gültig sind:

3. Ist Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 dahin auszulegen, dass die Veröffentlichung nach der Verordnung Nr. 259/2008 erst erfolgen darf, wenn die in diesem Artikel vorgesehene Verfahrensweise, die die Meldung an die Kontrollstelle ersetzt, durchgeführt worden ist?

4. Ist Art. 20 der Richtlinie 95/46 dahin auszulegen, dass die Veröffentlichung nach der Verordnung Nr. 259/2008 erst erfolgen darf, wenn die Vorabkontrolle erfolgt ist, die das nationale Recht für diesen Fall vorschreibt?

5. Falls die vierte Frage bejaht wird: Ist Art. 20 der Richtlinie 95/46 dahin auszulegen, dass keine wirksame Vorabkontrolle vorliegt, wenn sie auf der Grundlage eines Verzeichnisses nach Art. 18 Abs. 2 zweiter Gedankenstrich dieser Richtlinie erfolgt ist, das eine vorgeschriebene Information nicht enthält?

6. Ist Art. 7 – und hier insbesondere Buchst. e – der Richtlinie 95/46 dahin auszulegen, dass er einer Praxis, die IP-Adressen der Benutzer einer Homepage ohne deren ausdrückliche Einwilligung zu speichern, entgegensteht?

*b) Leitsätze*

**1.** Die Mitgliedstaaten sind verpflichtet, vor der Offenlegung von eine natürliche Person betreffenden Informationen das Interesse der Union daran, die Transparenz ihrer Handlungen zu gewährleisten, und die Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte zum Ausgleich zu bringen.

**2.** Dem Ziel der Transparenz kann nicht ohne Weiteres Vorrang gegenüber dem Recht auf Schutz der personenbezogenen Daten zuerkannt werden, selbst wenn erhebliche wirtschaftliche Interessen betroffen sind.

**3.** Um den Zweck einer solchen Veröffentlichung vergebener Beihilfen zu erreichen, zugleich aber in das Recht der Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen weniger stark einzugreifen, sind die Modalitäten der Veröffentlichung anzupassen, etwa durch die Beschränkung der Zeiträume des Bezugs, der Häufigkeit oder auch von Art und Umfang der Beihilfen.
(https://www.bfdi.bund.de/DE/Infothek/Gesetze_Rechtsprechung/RechtsprechungDS/BDSG_Allgemein/Artikel/091111_NamentlicheVeroeffentlichungEmpfaengerAgrarhilfen.html?nn=5217172 )

*c) Begründung*

[…]1. Zur ersten Frage und zum ersten Teil der zweiten Frage

a) Vorbemerkungen

43 Mit seiner ersten Frage und dem ersten Teil seiner zweiten Frage ersucht das vorlegende Gericht den Gerichtshof um Prüfung der Gültigkeit von Art. 44a der Verordnung Nr. 1290/2005 sowie der Verordnung Nr. 259/2008 mit Durchführungsbestimmungen zu der in diesem Art. 44a angeordneten Veröffentlichungspflicht auf der einen und von Art. 42 Nr. 8b der Verordnung Nr. 1290/2005, der die Rechtsgrundlage für die Verordnung Nr. 259/2008 bildet, auf der anderen Seite.

44 Nach Auffassung des vorlegenden Gerichts stellt die Pflicht zur Veröffentlichung die Empfänger von EGFL- und ELER-Mitteln betreffender Daten, die sich aus den in der vorstehenden Randnummer angeführten Bestimmungen ergibt, einen Eingriff in das Grundrecht auf Schutz der personenbezogenen Daten dar, der nicht gerechtfertigt sei. Es nimmt insoweit im Wesentlichen auf Art. 8 EMRK Bezug.

45 Es ist darauf hinzuweisen, dass nach Art. 6 Abs. 1 EUV die Union die Rechte, Freiheiten und Grundsätze anerkennt, die in der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) niedergelegt sind; danach sind „die Charta und die Verträge … rechtlich gleichrangig".

46 Demnach ist die Gültigkeit der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und die der Verordnung Nr. 259/2008 im Hinblick auf die Bestimmungen der Charta zu prüfen.

47 Gemäß Art. 8 Abs. 1 der Charta hat „[j]ede Person … das Recht auf Schutz der sie betreffenden personenbezogenen Daten". Dieses Grundrecht steht in engem Zusammenhang mit dem in Art. 7 der Charta verankerten Recht auf Achtung des Privatlebens.

48 Das Recht auf Schutz der personenbezogenen Daten kann jedoch keine uneingeschränkte Geltung beanspruchen, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden (vgl. in diesem Sinne Urteil vom 12. Juni 2003, Schmidberger, C‑112/00, Slg. 2003, I‑5659, Randnr. 80 und die dort angeführte Rechtsprechung).

49 So erlaubt Art. 8 Abs. 2 der Charta die Verarbeitung personenbezogener Daten, sofern bestimmte Voraussetzungen erfüllt sind. Er sieht insoweit vor, dass personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden [dürfen]".

50 Ferner lässt Art. 52 Abs. 1 der Charta Einschränkungen der Ausübung der Rechte wie derjenigen zu, die in ihren Art. 7 und 8 verankert sind, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Rechte und Freiheiten achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

51 Schließlich geht aus Art. 52 Abs. 3 der Charta hervor, dass, soweit diese Charta Rechte enthält, die den durch die EMRK garantierten Rechten entsprechen, diese die gleiche Bedeutung und Tragweite haben, wie sie ihnen in der genannten Konvention verliehen wird. In Art. 53 der Charta heißt es hierzu ergänzend, dass keine ihrer Bestimmungen als eine Einschränkung oder Verletzung der Rechte auszulegen ist, die u. a. durch die EMRK anerkannt werden.

52 Demnach ist zum einen davon auszugehen, dass sich die in den Art. 7 und 8 der Charta anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (vgl. insbesondere EGMR, Urteile Amann/Schweiz vom 16. Februar 2000, Recueil des arrêts et décisions 2000-II, § 65, und Rotaru/Rumänien vom 4. Mai 2000, Recueil des arrêts et décisions 2000–V, § 43), und zum anderen, dass Einschränkungen des Rechts auf Schutz

der personenbezogenen Daten gerechtfertigt sein können, wenn sie denen entsprechen, die im Rahmen von Art. 8 EMRK geduldet werden.

b) Zur Gültigkeit von Art. 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008

53 Als Erstes ist darauf hinzuweisen, dass die durch Art. 44a der Verordnung Nr. 1290/2005 und durch die Verordnung Nr. 259/2008 zur Durchführung dieser Bestimmung vorgeschriebene Veröffentlichung namentlich alle Empfänger von EGFL- und ELER-Mitteln bestimmt, zu denen sowohl natürliche als auch juristische Personen zählen. In Anbetracht der Ausführungen in Randnr. 52 des vorliegenden Urteils können sich juristische Personen gegenüber einer solchen Bestimmung auf den durch die Art. 7 und 8 der Charta verliehenen Schutz nur berufen, soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt.

54 Dies ist bei der Klägerin des Ausgangsverfahrens in der Rechtssache C‑92/09 der Fall. Der Name der betreffenden Gesellschaft bestimmt nämlich unmittelbar natürliche Personen, die deren Gesellschafter sind.

55 Als Zweites ist zu prüfen, ob Art. 44a der Verordnung Nr. 1290/2005 und die Verordnung Nr. 259/2008 bei den Empfängern von EGFL- und ELER-Mitteln, die bestimmte oder bestimmbare natürliche Personen sind (im Folgenden: betroffene Empfänger) zu einer Verletzung der ihnen durch die Art. 7 und 8 der Charta zuerkannten Rechte führen und ob eine solche Verletzung gegebenenfalls im Hinblick auf Art. 52 dieser Charta gerechtfertigt ist.

i) Zum Vorliegen einer Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte

56 Art. 44a der Verordnung Nr. 1290/2005 verpflichtet die Mitgliedstaaten, jedes Jahr die nachträgliche Veröffentlichung der Informationen über die Empfänger von EGFL- und ELER-Mitteln sowie der Beträge, die jeder Begünstigte aus diesen Fonds erhalten hat, zu gewährleisten. Aus dem 14. Erwägungsgrund der Verordnung Nr. 1437/2007 zur Änderung der Verordnung Nr. 1290/2005 geht hervor, dass diese Informationen „allgemein zu veröffentlichen“ sind.

57 In Art. 1 Abs. 1 Buchst. d der Verordnung Nr. 259/2008 wird der Inhalt der Veröffentlichung präzisiert; er sieht vor, dass neben den in der vorstehenden Randnummer genannten Angaben und weiteren Informationen über die erhaltenen Mittel „die Gemeinde, in der der Empfänger wohnt oder eingetragen ist, sowie gegebenenfalls die Postleitzahl bzw. der Teil der Postleitzahl, der für die betreffende Gemeinde steht“, veröffentlicht werden. Nach Art. 2 dieser Verordnung werden die Informationen in jedem Mitgliedstaat auf einer speziellen Website veröffentlicht und sind über eine Suchfunktion zugänglich.

58 Es ist unbestritten, dass die Beträge, die die betroffenen Empfänger aus dem EGFL und dem ELER erhalten, einen – häufig beträchtlichen – Teil ihrer Einkünfte ausmachen. Die Veröffentlichung von Daten mit den Namen dieser Empfänger und den genauen Beträgen, die sie erhalten haben, auf einer Internetseite stellt aufgrund der Tatsache, dass Dritte Zugang zu diesen Daten erhalten, somit einen Eingriff in ihr Privatleben im Sinne des Art. 7 der Charta dar (vgl. in diesem Sinne Urteil Österreichischer Rundfunk u. a., Randnrn. 73 und 74).

59 Der Umstand, dass sich die veröffentlichten Daten auf berufliche Tätigkeiten beziehen, ist insoweit ohne Belang (vgl. Urteil Österreichischer Rundfunk u. a., Randnrn. 73 und 74). Der Europäische Gerichtshof für Menschenrechte hat in Bezug auf die Auslegung von Art. 8 EMRK insoweit entschieden, dass der Begriff „Privatleben“ nicht eng ausgelegt werden darf und dass es „grundsätzlich nicht in Betracht kommt, berufliche Tätigkeiten … vom Begriff des ‚Privatlebens‘ auszunehmen“ (vgl. insbesondere EGMR, Urteile Amann/Schweiz, § 65, und Rotaru/Rumänien, § 43).

60 Im Übrigen stellt die durch Art. 44a der Verordnung Nr. 1290/2005 und durch die Verordnung Nr. 259/2008 vorgeschriebene Veröffentlichung eine Verarbeitung personenbezogener Daten im Sinne von Art. 8 Abs. 2 der Charta dar.

61 Das Land Hessen zieht jedoch in Zweifel, dass überhaupt ein Eingriff in das Privatleben der Kläger der Ausgangsverfahren vorliegt, da diese in dem Vordruck für die Beantragung von Beihilfen über die zwingende Veröffentlichung ihrer Daten unterrichtet worden seien und mit der Einreichung ihres Antrags gemäß Art. 8 Abs. 2 der Charta ihre Einwilligung in diese Veröffentlichung gegeben hätten.

62 Hierzu ist festzustellen, dass Art. 42 Nr. 8b der Verordnung Nr. 1290/2005 lediglich vorsieht, dass „die Mittelempfänger darüber unterrichtet werden, dass [ihre] Daten[, also ihr Name und die jeweils aus den Fonds erhaltenen Beträge] der Öffentlichkeit zugänglich gemacht … werden können“. Art. 4 Abs. 1 der Verordnung

Nr. 259/2008 enthält eine entsprechende Bestimmung, indem er vorsieht, dass „[d]ie Mitgliedstaaten … die Empfänger von Fondsmitteln [unterrichten], dass ihre Daten … veröffentlicht werden“.

63 Die fraglichen Unionsrechtsvorschriften, die lediglich vorsehen, dass die Mittelempfänger vorab über die Veröffentlichung ihrer Daten unterrichtet werden, stützen demnach die mit ihnen eingeführte Verarbeitung personenbezogener Daten nicht auf die Einwilligung der betroffenen Empfänger. Im Übrigen ist festzustellen, dass in den Ausgangsverfahren die Kläger in den Vordrucken für die Beantragung der Beihilfen lediglich bekundet haben, ihnen sei „bekannt, dass nach Art. 44a der [Verordnung] Nr. 1290/2005 vorgeschrieben ist, Informationen über die Empfänger von EGFL- und ELER-Mitteln … zu veröffentlichen“.

64 Da zum einen die Veröffentlichung von Daten unter Nennung der Namen der betroffenen Empfänger und der genauen Beträge, die sie aus dem EGFL und dem ELER erhalten haben, bei diesen Empfängern eine Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte darstellt und diese Verarbeitung personenbezogener Daten zum anderen nicht auf der Einwilligung dieser Empfänger beruht, ist zu prüfen, ob diese Verletzung nach Art. 52 Abs. 1 der Charta gerechtfertigt ist.

ii) Zur Rechtfertigung der Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte

65 Art. 52 Abs. 1 der Charta lässt Einschränkungen der Ausübung der Rechte wie derjenigen zu, die in ihren Art. 7 und 8 verankert sind, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Rechte und Freiheiten achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

66 Erstens steht fest, dass der Eingriff, der sich daraus ergibt, dass Daten unter Nennung der Namen der betroffenen Empfänger auf einer Internetseite veröffentlicht werden, als im Sinne von Art. 52 Abs. 1 der Charta „gesetzlich vorgesehen“ anzusehen ist. In Art. 1 Abs. 1 und Art. 2 der Verordnung Nr. 259/2008 ist eine solche Veröffentlichung nämlich ausdrücklich vorgesehen.

67 Zweitens geht hinsichtlich der Frage, ob dieser Eingriff einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung im Sinne des Art. 52 Abs. 1 der Charta entspricht, aus dem 14. Erwägungsgrund der Verordnung Nr. 1437/2007 zur Änderung der Verordnung Nr. 1290/2005 und aus dem sechsten Erwägungsgrund der Verordnung Nr. 259/2008 hervor, dass die Veröffentlichung der Namen der Empfänger von EGFL- und ELER-Mitteln sowie der Beträge, die sie aus diesen Fonds erhalten, darauf abzielt, „die Transparenz in Bezug auf die Verwendung der Gemeinschaftsmittel in der [GAP zu erhöhen] und …, insbesondere durch eine stärkere öffentliche Kontrolle der verwendeten Mittel, die Wirtschaftlichkeit der Haushaltsführung bei diesen Fonds [zu verbessern]“.

68 Der Transparenzgrundsatz ist in den Art. 1 EUV und 10 EUV sowie in Art. 15 AEUV verankert. Er ermöglicht eine bessere Beteiligung der Bürger am Entscheidungsprozess und gewährleistet eine größere Legitimität, Effizienz und Verantwortung der Verwaltung gegenüber dem Bürger in einem demokratischen System (vgl. Urteile vom 6. März 2003, Interporc/Kommission, C‑41/00 P, Slg. 2003, I‑2125, Randnr. 39, und vom 29. Juni 2010, Kommission/Bavarian Lager, C‑28/08 P, noch nicht in der amtlichen Sammlung veröffentlicht, Randnr. 54).

69 Indem die Veröffentlichung, die in den Bestimmungen vorgeschrieben ist, deren Gültigkeit in Zweifel gezogen wird, die öffentliche Kontrolle der Verwendung der durch den EGFL und den ELER verausgabten Beträge stärkt, trägt sie zur angemessenen Verwendung öffentlicher Mittel durch die Verwaltung bei (vgl. in diesem Sinne Urteil Österreichischer Rundfunk u. a., Randnr. 81).

70 Im Übrigen wird diese Veröffentlichung in Bezug auf die Verwendung der durch die betreffenden Landwirtschaftsfonds verausgabten Beträge den Bürgern eine bessere Beteiligung an der öffentlichen Debatte ermöglichen, die den Rahmen für die Entscheidungen über die Ausrichtung der GAP bildet.

71 Indem Art. 44a der Verordnung Nr. 1290/2005 und die Verordnung Nr. 259/2008 darauf abzielen, die Transparenz in Bezug auf die Mittelverwendung im Rahmen der GAP zu erhöhen, verfolgen sie mithin eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung.

72 Drittens ist weiter zu prüfen, ob die Einschränkung der in den Art. 7 und 8 der Charta verankerten Rechte in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck steht (vgl. u. a. EGMR, Urteil Gil-

low/Vereinigtes Königreich vom 24. November 1986, Série A, Nr. 109, § 55, und Urteil Österreichischer Rundfunk u. a., Randnr. 83).

73 Die Kläger der Ausgangsverfahren weisen hierzu darauf hin, dass die Daten, deren Veröffentlichung in Art. 44a der Verordnung Nr. 1290/2005 und in der Verordnung Nr. 259/2008 vorgesehen ist, Dritten ermöglichten, Schlüsse auf ihre Einkünfte zu ziehen. Diese Beihilfen machten zwischen 30 % und 70 % des Gesamteinkommens der betroffenen Empfänger aus. Dem berechtigten Interesse der Öffentlichkeit werde durch die Veröffentlichung anonymer statistischer Daten Genüge getan.

74 Nach ständiger Rechtsprechung verlangt der Grundsatz der Verhältnismäßigkeit, der zu den allgemeinen Grundsätzen des Unionsrechts gehört, dass die von einem Unionsrechtsakt eingesetzten Mittel zur Erreichung des verfolgten Ziels geeignet sind und nicht über das dazu Erforderliche hinausgehen (Urteil vom 8. Juni 2010, Vodafone u. a., C‑58/08, noch nicht in der amtlichen Sammlung veröffentlicht, Randnr. 51 und die dort angeführte Rechtsprechung).

75 Es wird nicht bestritten, dass die Veröffentlichung von Daten unter Nennung der Namen der betroffenen Empfänger und der genauen Beträge, die sie aus dem EGFL und dem ELER erhalten haben, im Internet geeignet ist, die Transparenz in Bezug auf die Verwendung der betreffenden Agrarbeihilfen zu erhöhen. Solche den Bürgern zur Verfügung gestellten Informationen stärken die öffentliche Kontrolle der Verwendung der betreffenden Beträge und leisten einen Beitrag zur bestmöglichen Verwendung öffentlicher Mittel.

76 Was die Erforderlichkeit der Maßnahme betrifft, ist darauf hinzuweisen, dass das mit der in Rede stehenden Veröffentlichung verfolgte Ziel nicht erreicht werden kann, ohne den Umstand zu berücksichtigen, dass dieses Ziel mit den in den Art. 7 und 8 der Charta verankerten Grundrechten in Einklang gebracht werden muss (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C‑73/07, Slg. 2008, I‑9831, Randnr. 53).

77 Daher ist zu prüfen, ob der Rat der Europäischen Union und die Kommission das Interesse der Union, die Transparenz ihrer Handlungen und eine bestmögliche Verwendung öffentlicher Mittel zu gewährleisten, auf der einen und die Verletzung des Rechts der betroffenen Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen auf der anderen Seite ausgewogen gewichtet haben. Der Gerichtshof hat hierzu bereits entschieden, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen (Urteil Satakunnan Markkinapörssi und Satamedia, Randnr. 56).

78 Die Mitgliedstaaten, die schriftliche Erklärungen beim Gerichtshof eingereicht haben, sowie der Rat und die Kommission tragen vor, dass das Ziel, das mit der durch Art. 44a der Verordnung Nr. 1290/2005 und durch die Verordnung Nr. 259/2008 vorgeschriebenen Veröffentlichung verfolgt werde, nicht durch Maßnahmen erreicht werden könne, die weniger stark in das Recht der betroffenen Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen eingriffen. Informationen, die auf die betroffenen Empfänger beschränkt seien, die einen bestimmten Schwellenwert überschreitende Beihilfen erhielten, vermittelten dem Steuerzahler kein wirklichkeitsgetreues Bild der GAP. Dieser hätte nämlich den Eindruck, dass es nur „Großempfänger“ von Beihilfen aus den betreffenden Landwirtschaftsfonds gebe, während doch die „Kleinempfänger“ sehr zahlreich seien. Auch eine Beschränkung der Veröffentlichung auf juristische Personen sei nicht zufriedenstellend. Die Kommission macht insoweit geltend, dass zu den größten Empfängern von Agrarbeihilfen natürliche Personen zählten.

79 Auch wenn in einer demokratischen Gesellschaft die Steuerzahler zwar einen Anspruch darauf haben, über die Verwendung der öffentlichen Gelder informiert zu werden (Urteil Österreichischer Rundfunk u. a., Randnr. 85), erforderte eine ausgewogene Gewichtung der verschiedenen beteiligten Interessen gleichwohl vor dem Erlass der Bestimmungen, deren Gültigkeit in Zweifel gezogen wird, die Prüfung der Frage durch die betreffenden Organe, ob die Veröffentlichung von Daten unter namentlicher Nennung aller betroffenen Empfänger und der genauen Beträge, die jeder von ihnen aus dem EGFL und dem ELER erhalten hat, in jedem Mitgliedstaat auf einer speziellen frei zugänglichen Internetseite – und zwar ohne dass nach Bezugsdauer, Häufigkeit oder Art und Umfang der erhaltenen Beihilfen unterschieden wird – in Anbetracht insbesondere der durch eine solche Veröffentlichung ausgelösten Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte nicht über das hinausging, was zur Erreichung der verfolgten berechtigten Ziele erforderlich war.

80 Es ist jedoch nicht ersichtlich, dass der Rat und die Kommission bestrebt gewesen wären, hinsichtlich natürlicher Personen als Empfänger von EGFL- und ELER-Mitteln eine solche ausgewogene Gewichtung des Interesses der Union, die Transparenz ihrer Handlungen und eine bestmögliche Verwendung der öffentlichen

Mittel zu gewährleisten, auf der einen und der in den Art. 7 und 8 der Charta verankerten Grundrechte auf der anderen Seite vorzunehmen.

81 Es gibt nämlich keinen Hinweis darauf, dass der Rat und die Kommission beim Erlass von Art. 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 Modalitäten der Veröffentlichung von Informationen über die betroffenen Empfänger erwogen hätten, die im Einklang mit dem Zweck einer solchen Veröffentlichung gestanden, zugleich aber auch in das Recht dieser Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen weniger stark eingegriffen hätten, wie etwa die Beschränkung der Veröffentlichung von Daten unter namentlicher Nennung der Empfänger nach Maßgabe der Zeiträume, während deren sie Beihilfen erhalten haben, der Häufigkeit oder auch von Art und Umfang dieser Beihilfen.

82 Mit einer in dieser Weise beschränkten namentlichen Veröffentlichung könnten gegebenenfalls einschlägige Erläuterungen in Bezug auf die übrigen natürlichen Personen, die Empfänger von Mitteln aus diesen Fonds sind, und auf die daraus erhaltenen Beträge einhergehen.

83 Die Organe hätten daher im Rahmen einer ausgewogenen Gewichtung der verschiedenen beteiligten Interessen prüfen müssen, ob eine eingeschränkte namentliche Veröffentlichung wie die in Randnr. 81 des vorliegenden Urteils dargestellte nicht ausreichend gewesen wäre, um die Ziele der in den Ausgangsverfahren in Rede stehenden Unionsrechtsvorschriften zu erreichen. Es ist insbesondere nicht ersichtlich, dass eine solche Beschränkung, die einige der betroffenen Empfänger vor einem Eingriff in ihr Privatleben bewahren würde, dem Bürger nicht ein hinreichend wirklichkeitsgetreues Bild der aus dem EGFL und dem ELER gezahlten Beihilfen vermitteln und zugleich die Erreichung der Ziele der in Rede stehenden Vorschriften ermöglichen würde.

84 Die Mitgliedstaaten, die schriftliche Erklärungen beim Gerichtshof eingereicht haben, sowie der Rat und die Kommission verweisen ferner auf den bedeutenden Anteil der GAP am Haushalt der Union, um die Notwendigkeit der durch Art. 44a der Verordnung Nr. 1290/2005 und durch die Verordnung Nr. 259/2008 vorgeschriebenen Veröffentlichung zu rechtfertigen.

85 Dieses Vorbringen ist zurückzuweisen. Die Mitgliedstaaten sind verpflichtet, vor der Offenlegung von eine natürliche Person betreffenden Informationen das Interesse der Union daran, die Transparenz ihrer Handlungen zu gewährleisten, und die Verletzung der durch die Art. 7 und 8 der Charta anerkannten Rechte zum Ausgleich zu bringen. Dem Ziel der Transparenz kann aber nicht ohne Weiteres Vorrang gegenüber dem Recht auf Schutz der personenbezogenen Daten zuerkannt werden (vgl. in diesem Sinne Urteil Kommission/Bavarian Lager, Randnrn. 75 bis 79), selbst wenn erhebliche wirtschaftliche Interessen betroffen sind.

86 Dem Vorstehenden ist zu entnehmen, dass nicht ersichtlich ist, dass die Organe eine ausgewogene Gewichtung der Ziele des Art. 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 auf der einen und der den natürlichen Personen durch die Art. 7 und 8 der Charta zuerkannten Rechte auf der anderen Seite vorgenommen haben. In Anbetracht der Tatsache, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen (Urteil Satakunnan Markkinapörssi und Satamedia, Randnr. 56) und dass Maßnahmen vorstellbar sind, die dieses Grundrecht der natürlichen Personen weniger stark beeinträchtigen, den Zielen der in Rede stehenden Unionsrechtsvorschriften aber ebenso in wirksamer Weise dienen, ist festzustellen, dass der Rat und die Kommission die durch die Wahrung des Grundsatzes der Verhältnismäßigkeit vorgegebenen Grenzen überschritten haben, indem sie die Veröffentlichung der Namen aller natürlichen Personen, die Empfänger von EGFL- und ELER-Mitteln sind, sowie der genauen aus diesen Fonds erhaltenen Beträge vorgeschrieben haben.

87 Was schließlich juristische Personen betrifft, die Empfänger von EGFL- und ELER-Mitteln sind, ist, soweit sie sich auf die durch die Art. 7 und 8 der Charta anerkannten Rechte berufen können (vgl. Randnr. 53 des vorliegenden Urteils), davon auszugehen, dass die Verpflichtung zur Veröffentlichung, die sich aus den Unionsrechtsvorschriften ergibt, deren Gültigkeit in Zweifel gezogen wird, nicht über die durch die Wahrung des Grundsatzes der Verhältnismäßigkeit vorgegebenen Grenzen hinausgeht. Die Verletzung des Rechts auf Schutz der personenbezogenen Daten hat nämlich bei juristischen Personen ein anderes Gewicht als bei natürlichen Personen. Juristische Personen unterliegen insoweit bereits einer erweiterten Verpflichtung zur Veröffentlichung ihrer Daten. Im Übrigen würde die Verpflichtung der zuständigen nationalen Behörden, vor der Veröffentlichung der in Rede stehenden Daten bei jeder juristischen Person, die Empfänger von EGFL- und ELER-Mitteln ist, zu prüfen, ob deren Name natürliche Personen bestimmt, diesen Behörden eine unverhältnismäßige Verwaltungslast aufbürden (vgl. in diesem Sinne EGMR, Urteil K. U./Finnland vom 2. März 2009, Klage Nr. 2872/02, noch nicht veröffentlicht, § 48).

88 Unter diesen Umständen ist davon auszugehen, dass die Unionsrechtsvorschriften, deren Gültigkeit vom vorlegenden Gericht in Zweifel gezogen wird, soweit sie sich auf die Veröffentlichung juristische Personen betreffender Daten beziehen, bei der Berücksichtigung der jeweils vorliegenden Interessen einen gerechten Ausgleich wahren.

89 Auf der Grundlage all dessen sind Art. 44a der Verordnung Nr. 1290/2005 und die Verordnung Nr. 259/2008 für ungültig zu erklären, soweit diese Bestimmungen bei natürlichen Personen, die Empfänger von EGFL- und ELER-Mitteln sind, die Veröffentlichung personenbezogener Daten hinsichtlich aller Empfänger vorschreiben, ohne nach einschlägigen Kriterien wie den Zeiträumen, während deren sie solche Beihilfen erhalten haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu unterscheiden.

c) Zur Gültigkeit von Art. 42 Nr. 8b der Verordnung Nr. 1290/2005

90 Art. 42 Nr. 8b der Verordnung Nr. 1290/2005 ermächtigt die Kommission, die Durchführungsbestimmungen nur für Art. 44a dieser Verordnung festzulegen.

91 Da aber Art. 44a der Verordnung Nr. 1290/2005 aus den oben angegebenen Gründen für ungültig zu erklären ist, ist auch Art. 42 Nr. 8b dieser Verordnung in gleicher Weise für ungültig zu erklären.

92 Daher ist auf die erste Frage und den ersten Teil der zweiten Frage zu antworten, dass die Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und die Verordnung Nr. 259/2008 ungültig sind, soweit diese Bestimmungen bei natürlichen Personen, die Empfänger von EGFL- und ELER-Mitteln sind, die Veröffentlichung personenbezogener Daten hinsichtlich aller Empfänger vorschreiben, ohne nach einschlägigen Kriterien wie den Zeiträumen, während deren sie solche Beihilfen erhalten haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu unterscheiden.

d) Zu den zeitlichen Wirkungen der festgestellten Ungültigkeit

93 Es ist festzustellen, dass der Gerichtshof, wenn zwingende Erwägungen der Rechtssicherheit es rechtfertigen, gemäß Art. 264 Abs. 2 AEUV, der im Rahmen von Vorabentscheidungsersuchen gemäß Art. 267 AEUV zur Beurteilung der Gültigkeit von Handlungen der Organe der Union entsprechend anwendbar ist, die Befugnis hat, in jedem einzelnen Fall anzugeben, welche Wirkungen der betreffenden Handlung Bestand haben (vgl. in diesem Sinne Urteil vom 22. Dezember 2008, Regie Networks, C‑333/07, Slg. 2008, I‑10807, Randnr. 121 und die dort angeführte Rechtsprechung).

94 In Anbetracht der großen Zahl von Veröffentlichungen, die in den Mitgliedstaaten auf der Grundlage von Rechtsvorschriften erfolgt sind, die als gültig angesehen wurden, ist darauf zu erkennen, dass die Ungültigkeit der in Randnr. 92 des vorliegenden Urteils genannten Bestimmungen nicht zulässt, die Wirkungen der Veröffentlichung der Listen von Empfängern von EGFL- und ELER-Mitteln in Frage zu stellen, die die nationalen Behörden in der Zeit vor dem Tag der Verkündung des vorliegenden Urteils auf der Grundlage dieser Bestimmungen vorgenommen haben.

2. Zur dritten Frage

95 Mit seiner dritten Frage möchte das vorlegende Gericht wissen, ob Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 dahin auszulegen ist, dass die Veröffentlichung der sich aus den Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 sowie der Verordnung Nr. 259/2008 ergebenden Informationen erst erfolgen darf, wenn der Datenschutzbeauftragte vor einer solchen Veröffentlichung die Führung eines vollständigen Verzeichnisses im Sinne dieses Art. 18 Abs. 2 zweiter Gedankenstrich aufgenommen hat.

96 Hierzu ist darauf hinzuweisen, dass Art. 18 Abs. 1 der Richtlinie 95/46 den Grundsatz aufstellt, dass die Meldung bei der Kontrollstelle erfolgt, bevor eine vollständige oder teilweise automatisierte Verarbeitung personenbezogener Daten oder eine Gesamtheit solcher Verarbeitungen mit der gleichen Zielsetzung oder mit ihr in Zusammenhang stehenden Zielsetzungen durchgeführt wird. Wie im 48. Erwägungsgrund dieser Richtlinie erläutert wird, dienen „[d]ie Meldeverfahren … der Offenlegung der Zweckbestimmungen der Verarbeitungen sowie ihrer wichtigsten Merkmale mit dem Zweck der Überprüfung ihrer Vereinbarkeit mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie“.

97 Nach Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 können die Mitgliedstaaten jedoch die Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht u. a. dann vorsehen, wenn der für die Verarbeitung Verantwortliche einen Datenschutzbeauftragten bestellt. Den Vorlagebeschlüssen ist zu entneh-

men, dass in Bezug auf die Veröffentlichung von Informationen im Sinne der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 im Land Hessen eine solche Bestellung erfolgt ist.

98 Gemäß Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 obliegen einem Datenschutzbeauftragten verschiedene Aufgaben, die geeignet sind, sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht verletzt werden können. So hat der Beauftragte u. a. die Aufgabe der „Führung eines Verzeichnisses mit den in Artikel 21 Absatz 2 [der Richtlinie 95/46] vorgesehenen Informationen über die durch den für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung“. Diese letztgenannte Bestimmung verweist auf Art. 19 Abs. 1 Buchst. a bis e dieser Richtlinie.

99 Entgegen der Auffassung des vorlegenden Gerichts enthält Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 jedoch keine Bestimmung, nach der der Datenschutzbeauftragte bereits vor der Durchführung der betreffenden Datenverarbeitung zur Führung eines Verzeichnisses mit den in Art. 21 Abs. 2 dieser Richtlinie in Verbindung mit ihrem Art. 19 Abs. 1 Buchst. a bis e vorgesehenen Informationen verpflichtet wäre. Das Verzeichnis, auf das in Art. 18 Abs. 2 zweiter Gedankenstrich dieser Richtlinie Bezug genommen wird, muss nämlich nur die „vorgenommene Verarbeitung“ enthalten.

100 Demnach kann das vom vorlegenden Gericht festgestellte Fehlen eines vor der Datenverarbeitung angelegten vollständigen Verzeichnisses die Rechtmäßigkeit einer Veröffentlichung wie der im Sinne der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 nicht berühren.

101 Auf die dritte Frage ist daher zu antworten, dass Art. 18 Abs. 2 zweiter Gedankenstrich der Richtlinie 95/46 dahin auszulegen ist, dass er den Datenschutzbeauftragten nicht zur Führung des in dieser Bestimmung vorgesehenen Verzeichnisses verpflichtet, bevor eine Verarbeitung personenbezogener Daten im Sinne der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 durchgeführt wurde.

3. Zur vierten Frage

102 Mit seiner vierten Frage möchte das vorlegende Gericht wissen, ob Art. 20 der Richtlinie 95/46 dahin auszulegen ist, dass er die Veröffentlichung von Informationen im Sinne der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 der in diesem Art. 20 vorgesehenen Vorabkontrolle unterwirft.

103 Zunächst ist darauf hinzuweisen, dass nach Art. 20 Abs. 1 der Richtlinie 95/46 „[d]ie Mitgliedstaaten [festlegen], welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und … dafür Sorge [tragen], dass diese Verarbeitungen vor ihrem Beginn geprüft werden“.

104 Folglich unterwirft die Richtlinie 95/46 die Verarbeitung personenbezogener Daten keiner allgemeinen Vorabkontrolle. Wie dem 52. Erwägungsgrund dieser Richtlinie zu entnehmen ist, ist der Unionsgesetzgeber nämlich davon ausgegangen, dass „die nachträgliche Kontrolle durch die zuständigen Stellen im Allgemeinen als ausreichende Maßnahme anzusehen [ist]“.

105 Was die einer Vorabkontrolle unterworfenen Verarbeitungen angeht, also die, die im Hinblick auf die Rechte und Freiheiten der betroffenen Personen spezifische Risiken aufweisen können, heißt es im 53. Erwägungsgrund der Richtlinie 95/46, dass Verarbeitungen „aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung“ solche Risiken aufweisen können. Auch wenn es den Mitgliedstaaten gestattet ist, in ihren Rechtsvorschriften näher zu erläutern, welche Verarbeitungen im Hinblick auf die Rechte und Freiheiten der betroffenen Personen spezifische Risiken aufweisen können, sieht diese Richtlinie ausweislich ihres 54. Erwägungsgrundes vor, dass deren Zahl „sehr beschränkt“ sein sollte.

106 Ferner ist darauf hinzuweisen, dass die Verarbeitungen personenbezogener Daten, die besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, nach Art. 27 Abs. 1 der Verordnung Nr. 45/2001 auch dann einer Vorabkontrolle unterliegen, wenn sie von den Organen und Einrichtungen der Union durchgeführt werden. Art. 27 Abs. 2 dieser Verordnung präzisiert, welche Verarbeitungen solche Risiken beinhalten können. In Anbetracht der Parallelität der Bestimmungen der Richtlinie 95/46 und der Verordnung Nr. 45/2001 betreffend die Vorabkontrolle ist die Aufzählung der Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, in Art. 27 Abs. 2 dieser Verordnung als für die Auslegung von Art. 20 der Richtlinie 95/46 maßgebend anzusehen.

107 Es ist aber nicht ersichtlich, dass die durch die Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und die Verordnung Nr. 259/2008 vorgeschriebene Veröffentlichung unter eine der in Art. 27 Abs. 2 der Verordnung Nr. 45/2001 genannten Verarbeitungskategorien fällt.

108 Demnach ist auf die vierte Frage zu antworten, dass Art. 20 der Richtlinie 95/46 dahin auszulegen ist, dass er die Mitgliedstaaten nicht verpflichtet, die Veröffentlichung von Informationen im Sinne der Art. 42 Nr. 8b und 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 der in dieser Bestimmung vorgesehenen Vorabkontrolle zu unterwerfen.

109 Angesichts der Antwort auf die vierte Frage ist die fünfte Frage nicht mehr zu beantworten. […]

**3) EuGH C-293, C-594/12 - Digital Rights Ireland Ltd**

*a) Sachverhalt*

Das Urteil betrifft die Auslegung der Art. 2 II Buchst. i, 10 IV und 15 I, II Buchst. a, III der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt (ABl. 2006 L 376, 36; im Folgenden: RL 2006/123). Es ergeht im Rahmen eines Revisionsverfahrens zwischen Herrn Hiebler und Herrn Schlagbauer, zwei österreichischen Staatsangehörigen, die das Rauchfangkehrergewerbe ausüben, das eine Klage von Herrn Schlagbauer auf Untersagung eines Herrn Hiebler vorgeworfenen unlauteren geschäftlichen Verhaltens in Ausübung seiner gewerblichen Tätigkeit zum Gegenstand hat.
Herr Hiebler übt im Land Kärnten auf Grund einer für das Kehrgebiet „A“ dieses Landes gültigen Gewerbeberechtigung gem. § 123 öst. GewO das Rauchfangkehrergewerbe aus. Bis zum 26.7.2011 übten nicht mehr als zwei Rauchfangkehrer ihre Tätigkeit im Kehrgebiet „B“ aus. Folglich durften die Rauchfangkehrer, die, wie Herr Hiebler, zur Ausübung ihrer Tätigkeit in anderen Kehrgebieten berechtigt waren, nach § 124 öst. GewO auch Kunden im Kehrgebiet „B“ werben. Eine am 27.7.2011 in Kraft getretene Änderung der Rechtsvorschriften über die Gebietsaufteilung für die Ausübung des Rauchfangkehrergewerbes im Land Kärnten führte zur Schaffung eines neuen Kehrgebiets „C“, das aus der Vereinigung des Kehrgebiets „B“ mit einem anderen Kehrgebiet hervorging. Obwohl aber nach dieser Vereinigung vier Rauchfangkehrer ihre Tätigkeit im neuen Kehrgebiet „C“ ausübten, fuhr Herr Hiebler damit fort, dort ansässige Kunden mit Postwurfsendungen zu werben und bei einigen von ihnen, die ihn mit der Reinigung ihrer Rauchfänge beauftragt hatten, als Rauchfangkehrer tätig zu werden. Diese Tätigkeit zog für Herrn Schlagbauer, der über eine Gewerbeberechtigung in diesem Kehrgebiet „C“ verfügte, einen Verdienstausfall nach sich. Er erhob daher Klage beim Landesgericht Klagenfurt auf Untersagung der – als unlauter eingestuften – gewerblichen Tätigkeit Herrn Hieblers, dessen Verurteilung zur Zahlung von Schadensersatz iHv 2594,65 Euro zzgl. Zinsen und Kosten sowie Veröffentlichung des zu erlassenden Urteils. Herr Hiebler beantragte die Abweisung der Klage, wofür er geltend machte, die RL 2006/123 stehe der im Ausgangsverfahren in Rede stehenden österreichischen Regelung entgegen, soweit diese eine vorsehe.
Das Landesgericht Klagenfurt gab der Klage Herrn Schlagbauers statt und entschied, dass die in § 123 öst. GewO vorgesehene territoriale Beschränkung in Einklang mit der Richtlinie stehe, da sie nicht diskriminierend, erforderlich und verhältnismäßig sei. Das OLG Graz bestätigte diese Entscheidung. Die hoheitlichen Aufgaben der Rauchfangkehrer im Bereich der „Feuerpolizei“ rechtfertigten die territoriale Beschränkung der Gewerbeberechtigung der Rauchfangkehrer. Herr Hiebler legte beim OGH Revision ein. Dort machte er geltend, dass die im Ausgangsverfahren in Rede stehende nationale Regelung zwar als mit dem Unionsrecht in Einklang stehend angesehen werden könne, soweit die streitgegenständliche territoriale Beschränkung sich auf die von den Rauchfangkehrern im Bereich der „Feuerpolizei“ wahrgenommenen Aufgaben beziehe, aber nicht, soweit diese Beschränkung auch ihre privatwirtschaftliche Tätigkeit, wie Reinigung und Unterhaltung von Rauch- und Abgasfängen, von Rauch- und Abgasleitungen sowie von den dazugehörenden Feuerstätten, betreffe. Der OGH ist der Auffassung, dass die RL 2006/123 nach ihrem Art. 2 II Buchst. i nicht auf die hoheitlichen Aufgaben im Rahmen der „Feuerpolizei“ anwendbar sei, sondern nur auf die privatwirtschaftlichen Tätigkeiten der Rauchfangkehrer. Allerdings stellt er sich die Frage, ob wegen des zwischen diesen Aufgaben und Tätigkeiten bestehenden Zusammenhangs die Richtlinie nicht auf die Ausübung des Rauchfangkehrergewerbes insgesamt unanwendbar sein könnte. Ferner äußert der OGH für den Fall, dass die privatwirtschaftlichen Tätigkeiten in den Anwendungsbereich der RL 2006/123 fallen sollten, Zweifel an der Vereinbarkeit der im Ausgangsverfahren in Rede stehenden österreichischen Regelung mit den in den Art. 10 und 15 dieser Richtlinie aufgestellten Regeln über die Niederlassungsfreiheit von Dienstleistern in der Union. Unter diesen Umständen hat der OGH das Verfahren ausgesetzt und dem EuGH seine Fragen zur Vorabentscheidung vorgelegt (OGH, E-CLI:AT:OGH0002:2014:0040OB00031.14H.0520.000).
(EuZW 2016, 224, beck-online)

*b) Leitsätze*

**1.** Die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt ist dahin auszulegen, dass sie auf die Ausübung eines Gewerbes wie des im Ausgangsverfahren fraglichen des Rauchfangkehrers insgesamt anwendbar ist, auch wenn dieses Gewerbe nicht nur die Ausübung privatwirtschaftlicher Tätigkeiten umfasst, sondern auch die Erfüllung von Aufgaben der „Feuerpolizei“.

**2.** Die Art. Artikel 10 Absatz II Buchst. a und Artikel 10 Absatz III der Richtlinie 2006/123/EG sind dahin auszulegen, dass sie einer nationalen Regelung wie der im Ausgangsverfahren fraglichen, die die Genehmigung für die Ausübung des Rauchfangkehrergewerbes insgesamt auf ein bestimmtes geografisches Gebiet beschränkt, entgegenstehen, wenn diese Regelung nicht in kohärenter und systematischer Weise das Ziel des Schutzes der öffentlichen Gesundheit verfolgt. Es ist Sache des vorlegenden Gerichts, dies zu prüfen. Art. EWG_RL_2006_123 Artikel 15 EWG_RL_2006_123 Artikel 15 Absatz IV der Richtlinie 2006/123/EG ist dahin auszulegen, dass er einer solchen Regelung nicht entgegensteht, wenn die Aufgaben der „Feuerpolizei“ als mit einer Dienstleistung von allgemeinem wirtschaftlichen Interesse in Zusammenhang stehend einzustufen wären, sofern die vorgesehene territoriale Beschränkung für die Erfüllung dieser Aufgaben unter Bedingungen eines wirtschaftlichen Gleichgewichts erforderlich und verhältnismäßig ist. Es ist Sache des vorlegenden Gerichts, dies zu prüfen.
(EuZW 2016, 224, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Feuzw%2F2016%2Fcont%2Feuzw.2016.224.1.htm&pos=1&hlwords=on )

*c) Begründung*

[…]Zur zweiten Frage, Buchst. b bis d, in der Rechtssache C‑293/12 und zur ersten Frage in der Rechtssache C‑594/12

23 Mit der zweiten Frage, Buchst. b bis d, in der Rechtssache C‑293/12 und mit der ersten Frage in der Rechtssache C‑594/12, die zusammen zu prüfen sind, ersuchen die vorlegenden Gerichte den Gerichtshof um die Prüfung der Gültigkeit der Richtlinie 2006/24 im Licht der Art. 7, 8 und 11 der Charta.

Zur Relevanz der Art. 7, 8 und 11 der Charta für die Frage der Gültigkeit der Richtlinie 2006/24

24 Wie sich aus Art. 1 sowie den Erwägungsgründen 4, 5, 7 bis 11, 21 und 22 der Richtlinie 2006/24 ergibt, sollen mit ihr in erster Linie die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugter oder verarbeiteter Daten harmonisiert werden, um sicherzustellen, dass die Daten, unter Wahrung der in den Art. 7 und 8 der Charta verankerten Rechte, zwecks Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie organisierter Kriminalität und Terrorismus zur Verfügung stehen.

25 Die in Art. 3 der Richtlinie 2006/24 vorgesehene Pflicht der Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder der Betreiber eines öffentlichen Kommunikationsnetzes, die in Art. 5 der Richtlinie aufgezählten Daten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, wirft Fragen hinsichtlich des in Art. 7 der Charta verankerten Schutzes sowohl des Privatlebens als auch der Kommunikation, hinsichtlich des von Art. 8 der Charta erfassten Schutzes personenbezogener Daten und hinsichtlich der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung auf.

26 Hierzu ist festzustellen, dass es sich bei den Daten, die von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes nach den Art. 3 und 5 der Richtlinie 2006/24 auf Vorrat zu speichern sind, u. a. um die zur Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie zur Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte benötigten Daten handelt, zu denen Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden Anschlusses und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse gehören. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand. Ferner ist ihnen zu entnehmen, wie häufig der Teilnehmer oder registrierte Benutzer während eines bestimmten Zeitraums mit bestimmten Personen kommuniziert hat.

27 Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.

28 Unter solchen Umständen ist es – auch wenn die Richtlinie 2006/24, wie sich aus ihren Art. 1 Abs. 2 und 5 Abs. 2 ergibt, keine Vorratsspeicherung des Inhalts einer Nachricht und der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen gestattet – nicht ausgeschlossen, dass die Vorratsspeicherung

der fraglichen Daten Auswirkungen auf die Nutzung der von dieser Richtlinie erfassten Kommunikationsmittel durch die Teilnehmer oder registrierten Benutzer und infolgedessen auf deren Ausübung der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung hat.

29 Die in der Richtlinie 2006/24 vorgesehene Vorratsspeicherung der Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, betrifft unmittelbar und speziell das Privatleben und damit die durch Art. 7 der Charta garantierten Rechte. Eine solche Vorratsspeicherung der Daten fällt zudem unter Art. 8 der Charta, weil sie eine Verarbeitung personenbezogener Daten im Sinne dieses Artikels darstellt und deshalb zwangsläufig die ihm zu entnehmenden Erfordernisse des Datenschutzes erfüllen muss (Urteil Volker und Markus Schecke und Eifert, C‑92/09 und C‑93/09, EU:C:2010:662, Rn. 47).

30 Zwar werfen die Vorabentscheidungsersuchen in den vorliegenden Rechtssachen insbesondere die grundsätzliche Frage auf, ob die Daten der Teilnehmer und der registrierten Benutzer im Hinblick auf Art. 7 der Charta auf Vorrat gespeichert werden dürfen, doch betreffen sie auch die Frage, ob die Richtlinie 2006/24 den in Art. 8 der Charta aufgestellten Erfordernissen des Schutzes personenbezogener Daten genügt.

31 In Anbetracht der vorstehenden Erwägungen ist zur Beantwortung der zweiten Frage, Buchst. b bis d, in der Rechtssache C‑293/12 und der ersten Frage in der Rechtssache C‑594/12 die Gültigkeit der Richtlinie anhand der Art. 7 und 8 der Charta zu prüfen.

Zum Vorliegen eines Eingriffs in die Rechte, die in den Art. 7 und 8 der Charta verankert sind

32 Durch die Verpflichtung zur Vorratsspeicherung der in Art. 5 Abs. 1 der Richtlinie 2006/24 aufgeführten Daten und durch die Gestattung des Zugangs der zuständigen nationalen Behörden zu diesen Daten weicht die Richtlinie, wie der Generalanwalt insbesondere in den Nrn. 39 und 40 seiner Schlussanträge ausgeführt hat, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikationsvorgänge von der durch die Richtlinien 95/46 und 2002/58 geschaffenen Regelung zum Schutz des Rechts auf Achtung der Privatsphäre ab, denn die letztgenannten Richtlinien sehen die Vertraulichkeit der Kommunikation und der Verkehrsdaten sowie die Pflicht vor, diese Daten zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, ausgenommen die zur Gebührenabrechnung erforderlichen Daten und nur solange diese dafür benötigt werden.

33 Für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung des Privatlebens kommt es nicht darauf an, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten (vgl. in diesem Sinne Urteil Österreichischer Rundfunk u. a., C‑465/00, C‑138/01 und C‑139/01, EU:C:2003:294, Rn. 75).

34 Daraus folgt, dass die den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes durch die Art. 3 und 6 der Richtlinie 2006/24 auferlegte Pflicht, die in Art. 5 dieser Richtlinie aufgeführten Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Art. 7 der Charta garantierten Rechte darstellt.

35 Zudem stellt der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht dar (vgl., zu Art. 8 EMRK, Urteile des EGMR Leander/Schweden vom 26. März 1987, Serie A, Nr. 116, § 48, Rotaru/Rumänien [GK], Nr. 28341/95, § 46, Rep. 2000‑V, sowie Weber und Saravia/Deutschland (Entsch.), Nr. 54934/00, § 79, Rep. 2006‑XI). Auch die Art. 4 und 8 der Richtlinie 2006/24, die Regeln für den Zugang der zuständigen nationalen Behörden zu den Daten aufstellen, greifen daher in die durch Art. 7 der Charta garantierten Rechte ein.

36 Desgleichen greift die Richtlinie 2006/24 in das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht.

37 Der mit der Richtlinie 2006/24 verbundene Eingriff in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte ist, wie auch der Generalanwalt insbesondere in den Nrn. 77 und 80 seiner Schlussanträge ausgeführt hat, von großem Ausmaß und als besonders schwerwiegend anzusehen. Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen – wie der Generalanwalt in den Nrn. 52 und 72 seiner Schlussanträge ausgeführt hat – das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.

Zur Rechtfertigung des Eingriffs in die durch Art. 7 und Art. 8 der Charta garantierten Rechte

38 Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten; unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

39 Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie, wie sich aus ihrem Art. 1 Abs. 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.

40 Die Vorratsspeicherung von Daten ist auch nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten, weil die Richtlinie 2006/24 in ihrem Art. 7 eine Vorschrift zum Datenschutz und zur Datensicherheit enthält, nach der Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes, unbeschadet der zur Umsetzung der Richtlinien 95/46 und 2002/58 erlassenen Vorschriften, bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssen. Nach diesen Grundsätzen stellen die Mitgliedstaaten sicher, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen.

41 Zu der Frage, ob der fragliche Eingriff einer dem Gemeinwohl dienenden Zielsetzung entspricht, ist festzustellen, dass mit der Richtlinie 2006/24 zwar die Vorschriften der Mitgliedstaaten über die Pflichten der genannten Anbieter oder Betreiber im Bereich der Vorratsspeicherung bestimmter von ihnen erzeugter oder verarbeiteter Daten harmonisiert werden sollen, doch besteht das materielle Ziel dieser Richtlinie, wie sich aus ihrem Art. 1 Abs. 1 ergibt, darin, die Verfügbarkeit der Daten zwecks Ermittlung, Feststellung und Verfolgung schwerer Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, sicherzustellen. Materielles Ziel der Richtlinie ist es demnach, zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit beizutragen.

42 Nach der Rechtsprechung des Gerichtshofs stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union dar (vgl. in diesem Sinne Urteile Kadi und Al Barakaat International Foundation/Rat und Kommission, C‑402/05 P und C‑415/05 P, EU:C:2008:461, Rn. 363, sowie Al-Aqsa/Rat, C‑539/10 P und C‑550/10 P, EU:C:2012:711, Rn. 130). Das Gleiche gilt für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit (vgl. in diesem Sinne Urteil Tsakouridis, C‑145/09, EU:C:2010:708, Rn. 46 und 47). Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat.

43 Hierzu geht aus dem siebten Erwägungsgrund der Richtlinie 2006/24 hervor, dass der Rat „Justiz und Inneres“ am 19. Dezember 2002 wegen der beträchtlichen Zunahme der Möglichkeiten bei der elektronischen Kommunikation die Ansicht vertrat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig seien und daher ein nützliches Mittel bei der Verhütung von Straftaten und der Bekämpfung der Kriminalität, insbesondere der organisierten Kriminalität, darstellten.

44 Somit ist festzustellen, dass die durch die Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich machen zu können, eine dem Gemeinwohl dienende Zielsetzung darstellt.

45 Unter diesen Umständen ist die Verhältnismäßigkeit des festgestellten Eingriffs zu prüfen.

46 Insoweit ist darauf hinzuweisen, dass der Grundsatz der Verhältnismäßigkeit nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist (vgl. in diesem Sinne Urteile Afton Chemical, C‑343/09, EU:C:2010:419, Rn. 45, Volker und Markus Schecke und Eifert, EU:C:2010:662, Rn. 74, Nelson u. a., C‑581/10 und C‑629/10, EU:C:2012:657, Rn. 71, Sky Österreich, C‑283/11, EU:C:2013:28, Rn. 50, und Schaible, C‑101/12, EU:C:2013:661, Rn. 29).

47 Was die gerichtliche Überprüfung der Einhaltung dieser Voraussetzungen anbelangt, kann, da Grundrechtseingriffe in Rede stehen, der Gestaltungsspielraum des Unionsgesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein; zu ihnen gehören u. a. der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs sowie dessen Zweck (vgl. entsprechend, zu Art. 8 EMRK, Urteil des EGMR S und Marper/Vereinigtes Königreich [GK], Nrn. 30562/04 und 30566/04, § 102, Rep. 2008‑V).

48 Im vorliegenden Fall ist angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des Ausmaßes und der Schwere des mit der Richtlinie 2006/24 verbundenen Eingriffs in dieses Recht der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt, so dass die Richtlinie einer strikten Kontrolle unterliegt.

49 Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.

50 Diese Beurteilung kann nicht durch den – insbesondere von Herrn Tschohl und Herrn Seitlinger sowie der portugiesischen Regierung in ihren beim Gerichtshof eingereichten schriftlichen Erklärungen angeführten – Umstand in Frage gestellt werden, dass es mehrere elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie 2006/24 fielen oder die eine anonyme Kommunikation ermöglichten. Dieser Umstand vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Maßnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber, wie der Generalanwalt in Nr. 137 seiner Schlussanträge ausgeführt hat, nicht zur Ungeeignetheit dieser Maßnahme.

51 Zur Erforderlichkeit der durch die Richtlinie 2006/24 vorgeschriebenen Vorratsspeicherung der Daten ist festzustellen, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme – wie sie die Richtlinie 2006/24 vorsieht – für die Kriminalitätsbekämpfung nicht rechtfertigen.

52 Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt nach ständiger Rechtsprechung des Gerichtshofs jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen (Urteil IPI, C‑473/12, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung).

53 Insoweit ist darauf hinzuweisen, dass der Schutz personenbezogener Daten, zu dem Art. 8 Abs. 1 der Charta ausdrücklich verpflichtet, für das in ihrem Art. 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung ist.

54 Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen (vgl. entsprechend, zu Art. 8 EMRK, Urteile des EGMR Liberty u. a./Vereinigtes Königreich vom 1. Juli 2008, Nr. 58243/00, §§ 62 und 63, Rotaru/Rumänien, §§ 57 bis 59, sowie S und Marper/Vereinigtes Königreich, § 99).

55 Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten, wie in der Richtlinie 2006/24 vorgesehen, automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht (vgl. entsprechend, zu Art. 8 EMRK, Urteil des EGMR S und Marper/Vereinigtes Königreich, § 103, sowie M. K./Frankreich vom 18. April 2013, Nr. 19522/09, § 35).

56 Zu der Frage, ob der mit der Richtlinie 2006/24 verbundene Eingriff auf das absolut Notwendige beschränkt ist, ist festzustellen, dass nach Art. 3 dieser Richtlinie in Verbindung mit ihrem Art. 5 Abs. 1 alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf

Vorrat zu speichern sind. Sie gilt somit für alle elektronischen Kommunikationsmittel, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung ist. Außerdem erfasst die Richtlinie nach ihrem Art. 3 alle Teilnehmer und registrierten Benutzer. Sie führt daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

57 Hierzu ist erstens festzustellen, dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

58 Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

59 Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.

60 Zweitens kommt zu diesem generellen Fehlen von Einschränkungen hinzu, dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.

61 Überdies enthält die Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Art. 4 der Richtlinie, der den Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind, sondern sieht lediglich vor, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

62 Insbesondere sieht die Richtlinie 2006/24 kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Beschränkungen zu schaffen.

63 Drittens schreibt die Richtlinie 2006/24 hinsichtlich der Dauer der Vorratsspeicherung in ihrem Art. 6 vor, dass die Daten für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern sind, ohne dass eine Unterscheidung zwischen den in Art. 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird.

64 Die Speicherungsfrist liegt zudem zwischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

65 Aus dem Vorstehenden folgt, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

66 Darüber hinaus ist in Bezug auf die Regeln zur Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Erstens sieht Art. 7 der Richtlinie 2006/24 keine speziellen Regeln vor, die der großen nach der Richtlinie auf Vorrat zu speichernden Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Derartige Regeln müssten namentlich klare und strikte Vorkehrungen für den Schutz und die Sicherheit der fraglichen Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Regeln zu schaffen.

67 Art. 7 der Richtlinie 2006/24 in Verbindung mit Art. 4 Abs. 1 der Richtlinie 2002/58 und Art. 17 Abs. 1 Unterabs. 2 der Richtlinie 95/46 gewährleistet nicht, dass die genannten Anbieter oder Betreiber durch technische und organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestattet es ihnen u. a., bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen zu berücksichtigen. Vor allem gewährleistet die Richtlinie 2006/24 nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

68 Zweitens schreibt die Richtlinie nicht vor, dass die fraglichen Daten im Unionsgebiet auf Vorrat gespeichert werden, so dass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der in den beiden vorstehenden Randnummern angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird. Eine solche Überwachung auf der Grundlage des Unionsrechts ist aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten (vgl. in diesem Sinne Urteil Kommission/Österreich, C‑614/10, EU:C:2012:631, Rn. 37).

69 Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste.

70 Unter diesen Umständen ist die Vereinbarkeit der Richtlinie 2006/24 mit Art. 11 der Charta nicht zu prüfen.

71 Infolgedessen ist auf die zweite Frage, Buchst. b bis d, in der Rechtssache C‑293/12 und auf die erste Frage in der Rechtssache C‑594/12 zu antworten, dass die Richtlinie 2006/24 ungültig ist. […]

**4) EuGH C-131/12 - Google Spain SL, Google Inc.**

*a) Sachverhalt*

2010 erhob ein spanischer Staatsbürger bei der spanischen Datenschutzagentur AEPD eine Beschwerde gegen eine in Spanien weitverbreitete Tageszeitung sowie gegen Google Inc. und Google Spain. Er machte geltend, bei Eingabe seines Namens in die Suchmaschine würden den Internetnutzern in der Ergebnisliste Links zu zwei Seiten der Tageszeitung angezeigt, auf denen die Versteigerung seines Grundstücks im Zusammenhang mit einer Pfändung angekündigt ist und beanspruchte Löschung beziehungsweise eine Unkenntlichmachung. Die Beschwerde gegen die Zeitung wurde von der AEPD zurückgewiesen, der Beschwerde gegen Google dagegen stattgegeben. Die AEPD forderte Google auf, die erforderlichen Maßnahmen zu ergreifen, um die betreffenden Daten aus ihrem Index zu entfernen und den Zugang zu ihnen in Zukunft zu verhindern. Google klagte vor einem spanischen Gericht, das sich zur Vorabentscheidung an den EuGH wandte. Der Gerichtshof hat die Klage von Google abgewiesen.
(becklink 1032458, beck-online)

14 Herr Costeja González, der die spanische Staatsangehörigkeit besitzt und seinen Wohnsitz in Spanien hat, erhob am 5. März 2010 bei der AEPD gegen die La Vanguardia Ediciones SL, die Herausgeberin einer insbesondere in Katalonien (Spanien) weitverbreiteten Tageszeitung (im Folgenden: La Vanguardia), sowie gegen Google Spain und Google Inc. eine Beschwerde, der Folgendes zugrunde lag: Bei Eingabe seines Namens in die Suchmaschine des Google-Konzerns (im Folgenden: Google Search) wurden den Internetnutzern Links zu zwei Seiten der Tageszeitung La Vanguardia vom 19. Januar bzw. 9. März 1998 angezeigt, die eine Anzeige enthielten, in der unter Nennung des Namens von Herrn Costeja González auf die Versteigerung eines Grundstücks im Zusammenhang mit einer wegen Forderungen der Sozialversicherung erfolgten Pfändung hingewiesen wurde.

15 Herr Costeja González beantragte, La Vanguardia anzuweisen, entweder die genannten Seiten zu löschen oder zu ändern, so dass die ihn betreffenden personenbezogen Daten dort nicht mehr angezeigt würden, oder zum Schutz der Daten von bestimmten, von den Suchmaschinen zur Verfügung gestellten technischen Möglichkeiten Gebrauch zu machen. Er beantragte ferner, Google Spain oder Google Inc. anzuweisen, ihn betreffende personenbezogene Daten zu löschen oder zu verbergen, so dass diese weder in den Suchergebnissen noch in Links zu La Vanguardia erschienen. Herr Costeja González behauptete in diesem Zusammenhang, dass die Pfändung, von der er betroffen gewesen sei, seit Jahren vollständig erledigt sei und keine Erwähnung mehr verdiene.

16 Mit Entscheidung vom 30. Juli 2010 wies die AEPD die Beschwerde, soweit sie sich gegen La Vanguardia richtete, mit der Begründung zurück, die Veröffentlichung der betreffenden Informationen durch diese Gesellschaft sei rechtlich gerechtfertigt gewesen, da sie auf Anordnung des Arbeits- und Sozialministeriums und mit dem Ziel einer höchstmöglichen Publizität der Zwangsversteigerung und somit einer höchstmöglichen Zahl an Bietern erfolgt sei.

17 Soweit sie sich gegen Google Spain und Google Inc. richtete, wurde der Beschwerde hingegen stattgegeben. Die AEPD begründete dies damit, dass Suchmaschinenbetreiber eine Datenverarbeitung vornähmen, für die sie verantwortlich seien, und als Mittler der Informationsgesellschaft fungierten; sie unterlägen deshalb den Datenschutzvorschriften. Die AEPD sei befugt, gegenüber Suchmaschinenbetreibern die Entfernung der Daten und das Verbot des Zugangs zu bestimmten Daten anzuordnen, wenn durch das Aufspüren und die Verbreitung der Daten das Grundrecht auf Datenschutz und die Würde der betroffenen Personen im weiteren Sinne, was auch den bloßen Willen der betroffenen Person umfasse, dass Dritte keine Kenntnis von diesen Daten hätten, beeinträchtigt werden könnten. Diese Verpflichtung könne unmittelbar die Suchmaschinenbetreiber treffen, ohne dass die Daten oder Informationen auf der betreffenden Website entfernt werden müssten, insbesondere wenn die Beibehaltung der Informationen auf der Website durch eine Gesetzesvorschrift gerechtfertigt sei.

18 Gegen diese Entscheidung haben Google Spain und Google Inc. bei der Audiencia Nacional zwei gesonderte Klagen erhoben; die Audiencia Nacional hat die beiden Verfahren verbunden.

19 Die Audiencia Nacional führt in der Vorlageentscheidung aus, in den beiden Verfahren stelle sich die Frage, welche Verpflichtungen die Suchmaschinenbetreiber hinsichtlich des Schutzes personenbezogener Daten von betroffenen Personen träfen, die nicht wollten, dass bestimmte auf Websites Dritter veröffentlichte Informationen, die sie betreffende personenbezogene Daten enthielten, mit denen die Informationen ihnen zugeordnet werden könnten, lokalisiert, indexiert und den Internetnutzern unbegrenzt zur Verfügung gestellt würden. Die Antwort auf diese Frage hänge davon ab, wie die Richtlinie 95/46 im Kontext solcher Technologien, die nach ihrer Bekanntmachung aufgekommen seien, auszulegen sei.

20 Die Audiencia Nacional hat daher das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Zum räumlichen Anwendungsbereich der Richtlinie 95/46 und somit der spanischen Rechtsvorschriften über den Schutz personenbezogener Daten:

a) Besteht eine „Niederlassung“ im Sinne von Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46, wenn eine oder mehrere der nachstehenden Fallgestaltungen vorliegen:

– wenn das die Suchmaschine betreibende Unternehmen in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staats ausgerichtet ist,

oder

– wenn die Muttergesellschaft eine in diesem Mitgliedstaat ansässige Tochtergesellschaft als ihre Vertreterin und für zwei konkrete Dateien mit den Daten ihrer Werbekunden als für die Verarbeitung Verantwortliche benennt

oder

– wenn die in einem Mitgliedstaat ansässige Niederlassung oder Tochtergesellschaft Beschwerden und Anordnungen, die von den betroffenen Personen bzw. den zuständigen Behörden an sie gerichtet werden, um zu erwirken, dass das Recht auf Schutz personenbezogener Daten beachtet wird, an die außerhalb der Europäischen Union ansässige Muttergesellschaft weiterleitet, auch wenn diese Zusammenarbeit freiwillig erfolgt?

b) Ist Art. 4 Abs. 1 Buchst. c der Richtlinie 95/46 dahin auszulegen, dass ein „Rückgriff" auf „Mittel, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind", gegeben ist,

– wenn eine Suchmaschine „Webcrawler" oder Indexierungsbots einsetzt, um Informationen auf Websites, die auf Servern in diesem Mitgliedstaat gehostet sind, zu lokalisieren und zu indexieren,

oder

– eine länderspezifische Domain eines Mitgliedstaats nutzt und Suche und Suchergebnisse an der Sprache dieses Mitgliedstaats ausrichtet?

c) Kann die vorübergehende Speicherung der durch die Internetsuchmaschinen indexierten Informationen als Rückgriff auf Mittel im Sinne von Art. 4 Abs. 1 Buchst. c der Richtlinie 95/46 betrachtet werden? Wenn ja: Kann davon ausgegangen werden, dass dieses Anknüpfungskriterium erfüllt ist, wenn sich das Unternehmen aus Gründen der Wettbewerbsfähigkeit weigert, den Ort offenzulegen, an dem es die Indexe speichert?

d) Unabhängig von der Antwort auf die vorstehenden Fragen und insbesondere für den Fall, dass der Gerichtshof der Auffassung sein sollte, dass die in Art. 4 der Richtlinie vorgesehenen Anknüpfungskriterien nicht erfüllt sind:

Ist die Richtlinie 95/46 im Licht des Art. 8 der Charta in dem Mitgliedstaat anzuwenden, in dem sich der Schwerpunkt des Konflikts befindet und die Rechte der Unionsbürger am wirksamsten geschützt werden können?

2. In Bezug auf die Tätigkeit der Suchmaschinen als Anbieter von Inhalten unter dem Blickwinkel der Richtlinie 95/46:

a) Zur Tätigkeit von Google Search als Anbieterin von Inhalten, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen:

Fällt, wenn die genannten Informationen personenbezogene Daten Dritter enthalten, eine solche Tätigkeit unter den Begriff „Verarbeitung personenbezogener Daten" im Sinne von Art. 2 Buchst. b der Richtlinie 95/46?

b) Bei Bejahung der vorstehenden Frage, ebenfalls im Zusammenhang mit einer Tätigkeit wie der zuvor beschriebenen:

Ist Art. 2 Buchst. d der Richtlinie 95/46 dahin auszulegen, dass das Unternehmen, das Google Search betreibt, hinsichtlich der auf den von ihr indexierten Websites befindlichen Daten der „für die Verarbeitung Verantwortliche" ist?

c) Bei Bejahung der vorstehenden Frage:

Kann die AEPD zum Schutz der durch Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 gewährleisteten Rechte Google Search unmittelbar anweisen, von Dritten veröffentlichte Informationen aus ihren Indexen zu entfernen, ohne sich zuvor oder gleichzeitig an den Inhaber der Website, die diese Informationen enthält, wenden zu müssen?

d) Bei Bejahung der vorstehenden Frage:

Entfällt die Verpflichtung der Suchmaschinenbetreiber zum Schutz der genannten Rechte, wenn die in den personenbezogenen Daten enthaltenen Informationen von Dritten rechtmäßig veröffentlicht worden sind und sich nach wie vor auf der ursprünglichen Website befinden?

3. Zur Tragweite des Rechts auf Löschung und/oder auf Widerspruch gegen die Verarbeitung die eigene Person betreffender Daten in Verbindung mit dem Recht auf Vergessenwerden:

Sind das Recht auf Löschung und Sperrung personenbezogener Daten gemäß Art. 12 Buchst. b der Richtlinie 95/46 und das Recht auf Widerspruch gegen eine Verarbeitung gemäß Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen, dass sich die betroffene Person an die Suchmaschinenbetreiber wenden kann, um die Indexierung auf sie bezogener Informationen zu verhindern, die auf Websites Dritter veröffentlicht sind, und sie sich hierzu auf ihren Willen berufen kann, dass sie den Internetnutzern nicht bekannt werden, wenn sie der Ansicht ist, dass sie ihr schaden können, oder sie sich wünscht, dass sie vergessen werden, selbst wenn es sich um Informationen handelt, die von Dritten rechtmäßig veröffentlicht wurden?

*b) Leitsätze*

Tenor

**1.** Art. 2 Buchst. b und d der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten“ im Sinne von Art. 2 Buchst. b der Richtlinie 95/46 einzustufen ist und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher“ im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 anzusehen ist.
**2.** Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 ist dahin auszulegen, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist.
**3.** Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.
**4.** Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass im Rahmen der Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u. a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am Zugang zu der Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen — wie der Rolle der betreffenden Person im öffentlichen Leben — ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist.
(EuGH Gerichtsmitteilung v. 13.5.2014 – C-131/12, BeckEuRS 2014, 418504, beck-online)

*c) Begründung*

[…]Zu Frage 1 Buchst. a bis d (räumlicher Anwendungsbereich der Richtlinie 95/46)

42 Mit Frage 1 Buchst. a bis d möchte das vorlegende Gericht wissen, ob die nationalen Rechtsvorschriften, mit denen die Richtlinie 95/46 umgesetzt wurde, unter Umständen wie denen des Ausgangsverfahrens angewandt werden können.

43 Das vorlegende Gericht hat insoweit folgende Tatsachen festgestellt:

– Google Search wird weltweit über die Website „www.google.com“ angeboten. Für viele Länder gibt es lokale, an die jeweilige Landessprache angepasste Versionen. Die spanischsprachige Version von Google Search wird über die seit dem 16. September 2003 registrierte Website „www.google.es“ angeboten. Google Search ist in Spanien eine der am meisten verwendeten Suchmaschinen.

– Google Search wird von Google Inc., der Muttergesellschaft des Google-Konzerns mit Sitz in den Vereinigten Staaten, betrieben.

– Google Search indexiert die Websites der ganzen Welt, u. a. die Websites in Spanien. Die Informationen, die von seinen „Webcrawlern“ oder Indexierungsbots – Computerprogrammen zum systematischen und automatischen Auffinden und Durchsuchen des Inhalts von Internetseiten – indexiert werden, werden vorübergehend auf Servern gespeichert, von denen nicht bekannt ist, in welchem Staat sie sich befinden, da diese Information aus Wettbewerbsgründen geheim gehalten wird.

– Google Search beschränkt sich nicht darauf, Zugang zu den Inhalten der indexierten Websites zu gewähren, sondern zieht aus dieser Tätigkeit Gewinn, indem es für Unternehmen, die diese Funktion nutzen möchten, um den Internetnutzern ihre Waren oder Dienstleistungen anzubieten, gegen Entgelt Werbeanzeigen einbettet, die mit den von den Internetnutzern eingegebenen Suchwörtern verknüpft sind.

– Der Google-Konzern bedient sich seiner Tochtergesellschaft Google Spain, um Werbung für den Verkauf der Werbeflächen auf der Website „www.google.com“ zu machen. Die Gesellschaft wurde am 3. September 2003 gegründet und hat eigene Rechtspersönlichkeit; ihr Sitz befindet sich in Madrid (Spanien). Als Handelsvertreter des Google-Konzerns in Spanien wendet sich Google Spain im Wesentlichen an in Spanien ansässige Unternehmen. Gesellschaftszweck ist die Förderung, Erleichterung und Durchführung des Verkaufs von Produkten und Diensten der Onlinewerbung an Dritte und das entsprechende Marketing.

– Google Inc. hat für zwei von ihr bei der AEPD angemeldete Dateien mit den ihre Werbekunden betreffenden personenbezogenen Daten Google Spain als für die Verarbeitung in Spanien Verantwortlicher angegeben.

44 Konkret sind für das vorlegende Gericht in erster Linie der Begriff „Niederlassung“ im Sinne von Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 und der Begriff „Rückgriff auf Mittel, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind“, im Sinne von Art. 4 Abs. 1 Buchst. c der Richtlinie fraglich.

Zu Frage 1 Buchst. a

45 Mit Frage 1 Buchst. a möchte das vorlegende Gericht wissen, ob Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, ausgeführt wird, wenn eine oder mehrere der drei nachstehenden Voraussetzungen erfüllt sind:

– der Suchmaschinenbetreiber gründet in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist,

– die Muttergesellschaft benennt eine in diesem Mitgliedstaat ansässige Tochtergesellschaft als ihre Vertreterin und für zwei spezifische Dateien mit den Daten ihrer Werbekunden als für die Verarbeitung Verantwortliche und/oder

– die in einem Mitgliedstaat ansässige Zweigniederlassung oder Tochtergesellschaft leitet Beschwerden und Anordnungen, die von den betroffenen Personen bzw. den zuständigen Behörden an sie gerichtet werden, um zu erwirken, dass das Recht auf Schutz personenbezogener Daten beachtet wird, an die außerhalb der Union ansässige Muttergesellschaft weiter, auch wenn diese Zusammenarbeit freiwillig erfolgt.

46 Zur ersten dieser drei Voraussetzungen führt das vorlegende Gericht aus, Google Search werde von Google Inc. betrieben und verwaltet; es sei nicht erwiesen, dass Google Spain in Spanien eine Tätigkeit ausübe, die unmittelbar mit der Indexierung oder Speicherung von in Websites Dritter enthaltener Informationen oder Daten zusammenhänge. Die Tätigkeit des Verkaufs der Werbeflächen und der Förderung dieses Verkaufs, um die sich für Spanien Google Spain kümmere, stelle aber den wesentlichen Teil der geschäftlichen Tätigkeit des

Google-Konzerns dar; es könne davon ausgegangen werden, dass diese Tätigkeit eng mit Google Search zusammenhänge.

47 Herr Costeja González, die spanische, die italienische, die österreichische und die polnische Regierung sowie die Kommission sind der Ansicht, dass Google Spain wegen der untrennbaren Verbindung, die zwischen ihrer Tätigkeit und der der von Google Inc. betriebenen Suchmaschine bestehe, als Niederlassung von Google Inc. anzusehen sei; die Verarbeitung personenbezogener Daten werde im Rahmen der Tätigkeiten dieser Niederlassung ausgeführt. Google Spain, Google Inc. und die griechische Regierung meinen hingegen, Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 finde auf die Fallgestaltung der ersten der drei vom vorlegenden Gericht angeführten Voraussetzungen keine Anwendung.

48 Hierzu ist zunächst festzustellen, dass es im 19. Erwägungsgrund der Richtlinie 95/46 heißt, dass „[e]ine Niederlassung im Hoheitsgebiet eines Mitgliedstaats … die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus[setzt]“ und „[d]ie Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, … in dieser Hinsicht nicht maßgeblich [ist]“.

49 Dass Google Spain in Spanien effektiv und tatsächlich eine Tätigkeit mittels einer festen Einreichung ausübt, ist aber unstreitig. Google Spain verfügt außerdem über eigene Rechtspersönlichkeit, so dass sie eine Tochtergesellschaft von Google Inc. in Spanien und somit eine „Niederlassung“ im Sinne von Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 darstellt.

50 Diese Bestimmung setzt ferner voraus, dass die Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen „im Rahmen der Tätigkeiten“ einer Niederlassung ausgeführt wird, die dieser im Hoheitsgebiet eines Mitgliedstaats besitzt.

51 Google Spain und Google Inc. sind der Ansicht, diese Voraussetzung sei im vorliegenden Fall nicht erfüllt, da die im Ausgangsverfahren in Rede stehende Verarbeitung personenbezogener Daten ausschließlich von Google Inc. ausgeführt werde, die Google Search betreibe, ohne dass Google Spain daran in irgendeiner Weise mitwirke; die Tätigkeit von Google Spain beschränke sich auf die Unterstützung der Tätigkeit des Google-Konzerns auf dem Gebiet der Werbung, die von seinem Suchmaschinendienst verschieden sei.

52 Wie insbesondere die spanische Regierung und die Kommission geltend machen, verlangt Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 aber nicht, dass die in Rede stehende Verarbeitung personenbezogener Daten „von“ der betreffenden Niederlassung selbst ausgeführt wird, sondern lediglich, dass sie „im Rahmen der Tätigkeiten“ der Niederlassung ausgeführt wird.

53 Außerdem kann diese Wendung im Hinblick auf das Ziel der Richtlinie 95/46, nämlich bei der Verarbeitung personenbezogener Daten einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere des Rechts auf Privatleben, zu gewährleisten, nicht eng ausgelegt werden (vgl. entsprechend Urteil L’Oréal u. a., C‑324/09, EU:C:2011:474, Rn. 62 und 63).

54 Insoweit ergibt sich insbesondere aus den Erwägungsgründen 18 bis 20 und Art. 4 der Richtlinie 95/46, dass der Unionsgesetzgeber vermeiden wollte, dass der gemäß der Richtlinie gewährleistete Schutz einer Person vorenthalten und umgangen wird, und deshalb einen besonders weiten räumlichen Anwendungsbereich vorgesehen hat.

55 Im Hinblick auf dieses Ziel der Richtlinie 95/46 und den Wortlaut ihres Art. 4 Abs. 1 Buchst. a ist davon auszugehen, dass die Verarbeitung personenbezogener Daten, die für den Dienst einer Suchmaschine wie Google Search erfolgt, die von einem Unternehmen betrieben wird, das seinen Sitz in einem Drittstaat hat, jedoch in einem Mitgliedstaat über eine Niederlassung verfügt, „im Rahmen der Tätigkeiten“ dieser Niederlassung ausgeführt wird, wenn diese die Aufgabe hat, in dem Mitgliedstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine, mit denen die Dienstleistung der Suchmaschine rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen.

56 Unter solchen Umständen sind nämlich die Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung in dem betreffenden Mitgliedstaat untrennbar miteinander verbunden, da die die Werbeflächen betreffenden Tätigkeiten das Mittel darstellen, um die in Rede stehende Suchmaschine wirtschaftlich rentabel zu machen, und die Suchmaschine gleichzeitig das Mittel ist, das die Durchführung dieser Tätigkeiten ermöglicht.

57 Wie in den Rn. 26 bis 28 des vorliegenden Urteils ausgeführt, stellt bereits die Anzeige personenbezogener Daten auf einer Seite mit Suchergebnissen eine Verarbeitung dieser Daten dar. Da aber zusammen mit den Er-

gebnissen auf derselben Seite die mit den Suchbegriffen verknüpften Werbeanzeigen angezeigt werden, ist festzustellen, dass die in Rede stehende Verarbeitung personenbezogener Daten im Rahmen der Werbetätigkeit erfolgt, die von der Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats – im vorliegenden Fall in Spanien – besitzt, ausgeübt wird.

58 Daher kann es nicht angehen, dass die Verarbeitung personenbezogener Daten, die zum Betrieb der Suchmaschine ausgeführt wird, den in der Richtlinie 95/46 vorgesehenen Verpflichtungen und Garantien entzogen wird, was die praktische Wirksamkeit der Richtlinie und den wirksamen und umfassenden Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, die mit ihr gewährleistet werden sollen, einschränken würde (vgl. entsprechend Urteil L'Oréal u. a., EU:C:2011:474, Rn. 62 und 63), insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, dem die Richtlinie eine besondere Bedeutung beimisst, wie u. a. aus ihrem Art. 1 Abs. 1 und ihren Erwägungsgründen 2 und 10 hervorgeht (vgl. in diesem Sinne Urteile Österreichischer Rundfunk u. a., C‑465/00, C‑138/01 und C‑139/01, EU:C:2003:294, Rn. 70, Rijkeboer, C‑553/07, EU:C:2009:293, Rn. 47, und IPI, C‑473/12, EU:C:2013:715, Rn. 28 und die dort angeführte Rechtsprechung).

59 Da die erste der drei vom vorlegenden Gericht angeführten Voraussetzungen bereits für die Feststellung genügt, dass eine Niederlassung wie Google Spain das Kriterium des Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 erfüllt, brauchen die beiden anderen Voraussetzungen nicht geprüft zu werden.

60 Somit ist auf Frage 1 Buchst. a zu antworten, dass Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, ausgeführt wird, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist.

Zu Frage 1 Buchst. b, c und d

61 In Anbetracht der Antwort auf Frage 1 Buchst. a ist Frage 1 Buchst. b, c und d nicht zu beantworten.

Zu Frage 2 Buchst. c und d (Umfang der Verantwortlichkeit des Suchmaschinenbetreibers nach der Richtlinie 95/46)

62 Mit Frage 2 Buchst. c und d möchte das vorlegende Gericht wissen, ob Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen sind, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.

63 Google Spain und Google Inc. sind der Ansicht, dass Anträge auf Löschung von Informationen nach dem Grundsatz der Verhältnismäßigkeit an den Herausgeber der betreffenden Website zu richten seien, da dieser die Verantwortung für die Veröffentlichung der Informationen übernehme, die Rechtmäßigkeit der Veröffentlichung beurteilen könne und über die wirksamsten und am wenigsten beeinträchtigenden Mittel zur Unzugänglichmachung der Informationen verfüge. Außerdem werde den Grundrechten der Websiteherausgeber, der anderen Internetnutzer und des Suchmaschinenbetreibers nicht hinreichend Rechnung getragen, wenn Letzterer angewiesen werde, im Internet veröffentlichte Informationen aus seinen Indexen zu entfernen.

64 Die österreichische Regierung vertritt die Auffassung, eine nationale Kontrollstelle könne nur dann anordnen, dass der Suchmaschinenbetreiber von Dritten veröffentlichte Informationen aus seinen Dateien lösche, wenn vorher festgestellt worden sei, dass die betreffenden Daten rechtswidrig oder unzutreffend seien, oder die betroffene Person beim Herausgeber der Website, auf der die Informationen veröffentlicht worden seien, mit Erfolg Widerspruch eingelegt habe.

65 Herr Costeja González, die spanische, die italienische und die polnische Regierung sowie die Kommission vertreten die Auffassung, die nationale Behörde könne den Betreiber einer Suchmaschine unmittelbar anweisen, aus seinen Indexen und seinem Zwischenspeicher Informationen zu entfernen, die von Dritten veröffentlichte personenbezogene Daten enthielten, ohne sich vorher oder gleichzeitig an den Herausgeber der Website wenden zu müssen, auf der sich die Informationen befänden. Nach Auffassung von Herrn Costeja González, der spani-

schen und der italienischen Regierung sowie der Kommission kommt es für die Verpflichtungen des Suchmaschinenbetreibers aus der Richtlinie 95/46 ferner nicht darauf an, dass die Informationen rechtmäßig veröffentlicht worden sind und sich nach wie vor auf der ursprünglichen Internetseite befinden. Nach Auffassung der polnischen Regierung dagegen kann dieser Umstand den Suchmaschinenbetreiber von seinen Verpflichtungen befreien.

66 Zunächst ist zu beachten, dass die Richtlinie 95/46, wie sich aus ihrem Art. 1 und ihrem 10. Erwägungsgrund ergibt, darauf abzielt, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten, insbesondere der Privatsphäre, natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. in diesem Sinne Urteil IPI, EU:C:2013:715, Rn. 28).

67 Nach dem 25. Erwägungsgrund der Richtlinie 95/46 finden die in der Richtlinie vorgesehenen Schutzprinzipien zum einen ihren Niederschlag in den Pflichten, die den für die Verarbeitung verantwortlichen Personen obliegen und insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann, betreffen, und kommen zum anderen in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Daten zu erhalten, ihre Berichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können, zum Ausdruck.

68 Der Gerichtshof hat bereits entschieden, dass die Bestimmungen der Richtlinie 95/46, soweit sie Verarbeitungen personenbezogener Daten betreffen, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung des Privatlebens führen können, im Licht der Grundrechte auszulegen sind, die nach ständiger Rechtsprechung zu den allgemeinen Rechtsgrundsätzen gehören, deren Wahrung der Gerichtshof zu sichern hat, und nun in der Charta verankert sind (vgl. u. a. Urteile Connolly/Kommission, C‑274/99 P, EU:C:2001:127, Rn. 37, und Österreichischer Rundfunk u. a., EU:C:2003:294, Rn. 68).

69 So garantiert Art. 7 der Charta das Recht auf Achtung des Privatlebens, und Art. 8 der Charta proklamiert ausdrücklich das Recht auf Schutz der personenbezogenen Daten. In den Abs. 2 und 3 des letztgenannten Artikels wird präzisiert, dass diese Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen, dass jede Person das Recht hat, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, und dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht wird. Diese Erfordernisse werden insbesondere durch die Art. 6, 7, 12, 14 und 28 der Richtlinie 95/46 durchgeführt.

70 Nach Art. 12 Buchst. b der Richtlinie 95/46 garantieren die Mitgliedstaaten jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen je nach Fall die Berichtigung, Löschung oder Sperrung von Daten zu erhalten, deren Verarbeitung nicht den Bestimmungen der Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind. Da diese letztgenannte Präzisierung in Bezug auf die Nichterfüllung bestimmter in Art. 6 Abs. 1 Buchst. d der Richtlinie 95/46 genannter Erfordernisse exemplarischen, und nicht abschließenden Charakter hat, kann eine Verarbeitung auch deshalb nicht den Bestimmungen der Richtlinie entsprechen und somit für die betroffene Person das in Art. 12 Buchst. b der Richtlinie garantierte Recht begründen, weil andere Voraussetzungen für die Zulässigkeit der Verarbeitung personenbezogener Daten gemäß der Richtlinie nicht erfüllt sind.

71 Jede Verarbeitung personenbezogener Daten muss – vorbehaltlich der in Art. 13 der Richtlinie 95/46 zugelassenen Ausnahmen – den in Art. 6 der Richtlinie aufgestellten Grundsätzen in Bezug auf die Qualität der Daten und einem der in Art. 7 der Richtlinie aufgeführten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten genügen (vgl. Urteile Österreichischer Rundfunk u. a., EU:C:2003:294, Rn. 65; ASNEF und FECEMD, C‑468/10 und C‑469/10, EU:C:2011:777, Rn. 26, und Worten, C‑342/12, EU:C:2013:355, Rn. 33).

72 Vorbehaltlich besonderer Vorschriften, die die Mitgliedstaaten für die Verarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke vorsehen können, hat der für die Verarbeitung Verantwortliche nach dem Wortlaut des genannten Art. 6 der Richtlinie 95/46 dafür zu sorgen, dass die personenbezogenen Daten „nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden“, „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden“, „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“, „sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind“ und „nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht“. Der für die Verarbeitung Verantwortliche hat insofern alle angemessenen Maßnah-

men zu treffen, damit Daten, die die Anforderungen der genannten Bestimmung nicht erfüllen, gelöscht oder berichtigt werden.

73 Was die Zulässigkeit gemäß Art. 7 der Richtlinie 95/46 angeht, kommt für eine von einem Suchmaschinenbetreiber ausgeführte Verarbeitung, wie sie im Ausgangsverfahren in Rede steht, als Zulässigkeitsgrund Art. 7 Buchst. f der Richtlinie in Betracht.

74 Nach dieser Bestimmung ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, insbesondere ihr Recht auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die gemäß Art. 1 Abs. 1 der Richtlinie geschützt sind, überwiegen. Die Anwendung von Art. 7 Buchst. f der Richtlinie 95/46 erfordert also eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen, in deren Rahmen die Bedeutung der Rechte der betroffenen Person, die sich aus den Art. 7 und 8 der Charta ergeben, zu berücksichtigen ist (vgl. Urteil ASNEF und FECEMD, EU:C:2011:777, Rn. 38 und 40).

75 Ob eine Verarbeitung den Bestimmungen von Art. 6 und Art. 7 Buchst. f der Richtlinie 95/46 entspricht, kann im Rahmen eines Antrags gemäß Art. 12 Buchst. b der Richtlinie geprüft werden; unter bestimmten Voraussetzungen kann die betroffene Person darüber hinaus aber auch ihr Widerspruchsrecht gemäß Art. 14 Abs. 1 Buchst. a der Richtlinie ausüben.

76 Nach dem genannten Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 erkennen die Mitgliedstaaten das Recht der betroffenen Person an, zumindest in den Fällen von Art. 7 Buchst. e und f der Richtlinie jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen Widerspruch einlegen zu können, dass sie betreffende Daten verarbeitet werden, wobei dies nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung gilt. Bei der im Rahmen von Art. 14 Abs. 1 Buchst. a der Richtlinie vorzunehmenden Abwägung lassen sich somit spezieller alle Umstände der konkreten Situation der betroffenen Person berücksichtigen. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen.

77 Anträge gemäß Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 können von der betroffenen Person unmittelbar an den für die Verarbeitung Verantwortlichen gerichtet werden, der dann sorgfältig ihre Begründetheit zu prüfen und die Verarbeitung der betreffenden Daten gegebenenfalls zu beenden hat. Gibt der für die Verarbeitung Verantwortliche den Anträgen nicht statt, kann sich die betroffene Person an die Kontrollstelle oder das zuständige Gericht wenden, damit diese die erforderlichen Überprüfungen vornehmen und den für die Verarbeitung Verantwortlichen entsprechend anweisen, bestimmte Maßnahmen zu ergreifen.

78 In diesem Zusammenhang ist darauf hinzuweisen, dass sich nach Art. 28 Abs. 3 und 4 der Richtlinie 95/46 jede Person zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden kann und jede Kontrollstelle über Untersuchungsbefugnisse und wirksame Einwirkungsbefugnisse verfügt, aufgrund deren sie u. a. die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung personenbezogener Daten anordnen kann.

79 Wird die Kontrollstelle oder das zuständige Gericht mit einem Antrag wie dem des Ausgangsverfahrens befasst, sind die Bestimmungen der Richtlinie 95/46 über die Rechte der betroffenen Person im Licht der vorstehenden Erwägungen auszulegen und anzuwenden.

80 Wie bereits in den Rn. 36 bis 38 des vorliegenden Urteils ausgeführt, kann eine von einem Suchmaschinenbetreiber ausgeführte Verarbeitung personenbezogener Daten wie die im Ausgangsverfahren in Rede stehende die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt wird, da diese Verarbeitung es jedem Internetnutzer ermöglicht, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können, und somit ein mehr oder weniger detailliertes Profil der Person zu erstellen. Zudem wird die Wirkung des Eingriffs in die genannten Rechte der betroffenen Person noch durch die bedeutende Rolle des Internets und der Suchmaschinen in der modernen Gesellschaft gesteigert, die den in einer Ergebnisliste enthaltenen Informationen Ubiquität verleihen (vgl. in diesem Sinne Urteil eDate Advertising u. a., C‑509/09 und C‑161/10, EU:C:2011:685, Rn. 45).

81 Wegen seiner potenziellen Schwere kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden. Da sich die Entfernung von Links aus der Ergebnisliste aber je nach der Information, um die es sich handelt, auf das berechtigte Interesse von potenziell am Zugang zu der Information interessierten Internetnutzern auswirken kann, ist in Situationen wie der des Ausgangsverfahrens ein angemessener Ausgleich u. a. zwischen diesem Interesse und den Grundrechten der betroffenen Person aus den Art. 7 und 8 der Charta zu finden. Zwar überwiegen die durch diese Artikel geschützten Rechte der betroffenen Person im Allgemeinen gegenüber dem Interesse der Internetnutzer; der Ausgleich kann in besonders gelagerten Fällen aber von der Art der betreffenden Information, von deren Sensibilität für das Privatleben der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information abhängen, das u. a. je nach der Rolle, die die Person im öffentlichen Leben spielt, variieren kann.

82 Nach der Beurteilung der Anwendungsvoraussetzungen von Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46, die die Kontrollstelle oder das zuständige Gericht vorzunehmen haben, wenn sie mit einem Antrag wie dem des Ausgangsverfahrens befasst werden, können sie den Suchmaschinenbetreiber anweisen, aus der Liste mit den Ergebnissen einer anhand des Namens einer Person durchgeführten Suche Links zu von Dritten veröffentlichten Seiten mit Informationen über diese Person zu entfernen, ohne dass eine solche Anordnung voraussetzt, dass der Name und die Informationen vorher oder gleichzeitig vom Herausgeber der Internetseite, auf der sie veröffentlicht worden sind, freiwillig oder auf Anordnung der Kontrollstelle oder des Gerichts von dieser Seite entfernt werden.

83 Wie bereits in den Rn. 35 bis 38 des vorliegenden Urteils ausgeführt, hat der Suchmaschinenbetreiber, da die im Rahmen der Tätigkeit einer Suchmaschine ausgeführte Datenverarbeitung sich von der unterscheidet, die von den Herausgebern von Websites ausgeführt worden ist, zusätzlich zu dieser erfolgt und die Grundrechte der betroffenen Person zusätzlich beeinträchtigt, als für die Verarbeitung Verantwortlicher in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen, dass die Verarbeitung den Anforderungen der Richtlinie 95/46 genügt, so dass die von dieser vorgesehenen Garantien ihre volle Wirkung entfalten können.

84 Insoweit ist darauf hinzuweisen, dass, da auf einer Website veröffentlichte Informationen leicht auf anderen Websites wiedergegeben werden können und die für die Veröffentlichung Verantwortlichen nicht immer dem Unionsrecht unterliegen, ein wirksamer und umfassender Schutz der betroffenen Personen nicht erreicht werden könnte, wenn diese vorher oder parallel bei den Herausgebern der Websites die Löschung der sie betreffenden Informationen erwirken müssten.

85 Außerdem kann die vom Herausgeber einer Website in Form der Veröffentlichung von Informationen zu einer natürlichen Person ausgeführte Verarbeitung gegebenenfalls „allein zu journalistischen … Zwecken“ erfolgen, so dass für sie nach Art. 9 der Richtlinie 95/46 Ausnahmen von den Erfordernissen der Richtlinie gelten, während dies bei einer vom Betreiber einer Suchmaschine ausgeführten Verarbeitung nicht der Fall ist. Mithin ist nicht auszuschließen, dass die betroffene Person unter bestimmten Umständen die Rechte gemäß Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 gegen den Suchmaschinenbetreiber, aber nicht gegen den Herausgeber der Website geltend machen kann.

86 Schließlich ist festzustellen, dass der Zulässigkeitsgrund gemäß Art. 7 der Richtlinie 95/46 für die Veröffentlichung personenbezogener Daten auf einer Website nicht unbedingt derselbe ist wie für die Tätigkeit der Suchmaschinen; selbst wenn dies der Fall ist, kann die nach Art. 7 Buchst. f und Art. 14 Abs. 1 Buchst. a der Richtlinie vorzunehmende Interessenabwägung je nachdem, ob es sich um die vom Suchmaschinenbetreiber oder die von dem Herausgeber der Internetseite ausgeführte Verarbeitung handelt, verschieden ausfallen, da sowohl die berechtigten Interessen, die die Verarbeitungen rechtfertigen, verschieden sein können als auch die Folgen, die die Verarbeitungen für die betroffene Person, insbesondere für ihr Privatleben, haben, nicht zwangsläufig dieselben sind.

87 Die Aufnahme einer Internetseite und der darin über eine Person enthaltenen Informationen in die Liste mit den Ergebnissen einer anhand des Namens der betreffenden Person durchgeführten Suche kann die Zugänglichkeit der Informationen für Internetnutzer, die eine Suche zu der Person durchführen, nämlich erheblich erleichtern und eine entscheidende Rolle bei der Verbreitung der Informationen spielen. Sie kann mithin einen stärkeren Eingriff in das Grundrecht auf Achtung des Privatlebens der betroffenen Person darstellen als die Veröffentlichung durch den Herausgeber der Internetseite.

88 Somit ist auf Frage 2 Buchst. c und d zu antworten, dass Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen sind, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu

von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.

Zu Frage 3 (Umfang der durch die Richtlinie 95/46 garantierten Rechte der betroffenen Person)

89 Mit Frage 3 möchte das vorlegende Gericht wissen, ob Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen sind, dass die betroffene Person vom Suchmaschinenbetreiber verlangen kann, von der Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, Links zu von Dritten rechtmäßig veröffentlichten Internetseiten mit wahrheitsgemäßen Informationen über sie zu entfernen, weil diese Informationen ihr schaden können oder weil sie möchte, dass sie nach einer gewissen Zeit „vergessen“ werden.

90 Nach Auffassung von Google Spain, Google Inc., der griechischen, der österreichischen und der polnischen Regierung sowie der Kommission ist diese Frage zu verneinen. Google Spain, Google Inc., die polnische Regierung und die Kommission machen insoweit geltend, Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 gewährten den betroffenen Personen nur unter der Voraussetzung Rechte, dass die betreffende Verarbeitung nicht den Bestimmungen der Richtlinie entspreche, oder aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen, und nicht bereits, weil die Verarbeitung ihnen ihrer Auffassung nach schaden könne oder sie möchten, dass die Daten, die Gegenstand der Verarbeitung seien, dem Vergessen anheimfallen. Nach Auffassung der griechischen und der österreichischen Regierung hat sich die betroffene Person an den Herausgeber der Website zu wenden.

91 Herr Costeja González sowie die spanische und die italienische Regierung vertreten die Auffassung, die betroffene Person könne der Indexierung der sie betreffenden personenbezogenen Daten durch eine Suchmaschine widersprechen, wenn die Verbreitung der Daten mit Hilfe der Suchmaschine ihr schade und ihre Grundrechte auf Schutz personenbezogener Daten und Achtung des Privatlebens, die das „Recht auf Vergessenwerden“ umfassten, gegenüber den berechtigten Interessen des Suchmaschinenbetreibers und dem allgemeinen Interesse an der Informationsfreiheit überwögen.

92 Zu Art. 12 Buchst. b der Richtlinie 95/46, der voraussetzt, dass die Verarbeitung personenbezogener Daten nicht den Bestimmungen der Richtlinie entspricht, ist festzustellen, dass die Verarbeitung, wie bereits in Rn. 72 des vorliegenden Urteils ausgeführt, den Bestimmungen der Richtlinie nicht nur nicht entsprechen kann, weil die Daten sachlich unrichtig sind, sondern u. a. auch, weil sie nicht den Zwecken der Verarbeitung entsprechen, dafür nicht erheblich sind oder darüber hinausgehen, nicht auf den neuesten Stand gebracht sind oder länger als erforderlich aufbewahrt werden, es sei denn ihre Aufbewahrung ist für historische, statistische oder wissenschaftliche Zwecke erforderlich.

93 Aus diesen in Art. 6 Abs. 1 Buchst. c bis e der Richtlinie 95/46 enthaltenen Anforderungen ergibt sich, dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind. Das ist insbesondere der Fall, wenn sie diesen Zwecken in Anbetracht der verstrichenen Zeit nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen.

94 Wird somit auf einen Antrag der betroffenen Person gemäß Art. 12 Buchst. b der Richtlinie 95/46 festgestellt, dass die Einbeziehung von Links zu von Dritten rechtmäßig veröffentlichten Internetseiten, die wahrheitsgemäße Informationen zu ihrer Person enthalten, in die Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, zum gegenwärtigen Zeitpunkt nicht mit Art. 6 Abs. 1 Buchst. c bis e der Richtlinie vereinbar ist, weil sich herausstellt, dass die Informationen in Anbetracht aller Umstände des Einzelfalls den Zwecken der in Rede stehenden Verarbeitung durch den Suchmaschinenbetreiber nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen, müssen die betreffenden Informationen und Links der Ergebnisliste gelöscht werden.

95 Zu den Anträgen gemäß Art. 12 Buchst. b der Richtlinie 95/46 wegen Nichtbeachtung der Voraussetzungen des Art. 7 Buchst. f der Richtlinie und den Anträgen gemäß Art. 14 Abs. 1 Buchst. a der Richtlinie ist festzustellen, dass jede Verarbeitung personenbezogener Daten während der gesamten Dauer ihrer Ausführung nach Art. 7 zulässig sein muss.

96 Somit ist im Rahmen der Beurteilung solcher Anträge, die gegen eine Verarbeitung wie die im Ausgangsverfahren in Rede stehende gerichtet sind, u. a. zu prüfen, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an

eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird. Die Feststellung eines solchen Rechts setzt nicht voraus, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht.

97 Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, ist, wie sich insbesondere aus Rn. 81 des vorliegenden Urteils ergibt, davon auszugehen, dass diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden, überwiegen. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist.

98 In einer Situation wie der im Ausgangsverfahren in Rede stehenden, in der es darum geht, dass in der Ergebnisliste, die der Internetnutzer erhält, wenn er mit Google Search eine Suche anhand des Namens der betroffenen Person durchführt, Links zu Seiten des Onlinearchivs einer Tageszeitung angezeigt werden, die Anzeigen enthalten, die sich unter Nennung des Namens der betroffenen Person auf die Versteigerung eines Grundstücks im Zusammenhang mit einer wegen Forderungen der Sozialversicherung erfolgten Pfändung beziehen, ist davon auszugehen, dass die betroffene Person wegen der Sensibilität der in diesen Anzeigen enthaltenen Informationen für ihr Privatleben und weil die ursprüngliche Veröffentlichung der Anzeigen 16 Jahre zurückliegt, ein Recht darauf hat, dass diese Informationen nicht mehr durch eine solche Ergebnisliste mit ihrem Namen verknüpft werden. Da im vorliegenden Fall offenbar keine besonderen Gründe vorliegen, die ein überwiegendes Interesse der Öffentlichkeit daran rechtfertigten, im Rahmen einer Suche anhand des Namens der betroffenen Person Zugang zu den genannten Informationen zu erhalten – was zu prüfen jedoch Sache des vorlegenden Gerichts ist –, kann die Person nach Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 die Entfernung der Links aus der Ergebnisliste verlangen.

99 Somit ist auf Frage 3 zu antworten, dass Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahin auszulegen sind, dass im Rahmen der Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u. a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am Zugang zu der Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist. […]

**5) EuGH C-363/14 - Europäisches Parlament**

*a) Sachverhalt*

1 Mit seiner Klage beantragt das Europäische Parlament die Nichtigerklärung des Durchführungsbeschlusses 2014/269/EU des Rates vom 6. Mai 2014 zur Änderung des Beschlusses 2009/935/JI hinsichtlich der Liste der Drittstaaten und dritten Organisationen, mit denen Europol Abkommen schließt (ABl. L 138, S. 104, im Folgenden: angefochtener Beschluss). […]

*b) Begründung*

[…]Zur Klage

16 Das Parlament macht in seinen Schriftsätzen drei Klagegründe geltend, und zwar erstens eine sich aus der fehlenden Initiative eines Mitgliedstaats oder der Kommission sowie der Fehlerhaftigkeit des durchgeführten Verfahrens der fakultativen Anhörung des Parlaments ergebende Verletzung wesentlicher Formvorschriften, zweitens die Wahl einer aufgehobenen oder rechtswidrigen Rechtsgrundlage und drittens die Wahl einer Rechts-

grundlage für Durchführungsmaßnahmen zum Erlass eines in den Bereich der Gesetzgebung fallenden Beschlusses.

17 Da die Rechtsgrundlage für das beim Erlass des Rechtsakts zu befolgende Verfahren maßgebend ist (Urteile Parlament/Rat, C‑130/10, EU:C:2012:472, Rn. 80, und Parlament/Rat, C‑658/11, EU:C:2014:2025, Rn. 57), sind als Erstes der zweite und der dritte Klagegrund zu prüfen, mit denen die Wahl einer aufgehobenen oder rechtswidrigen Rechtsgrundlage bzw. die Wahl einer Rechtsgrundlage für Durchführungsmaßnahmen zum Erlass eines in den Bereich der Gesetzgebung fallenden Beschlusses gerügt wird.

Zum zweiten und zum dritten Klagegrund: Wahl einer aufgehobenen oder rechtswidrigen Rechtsgrundlage bzw. Wahl einer Rechtsgrundlage für Durchführungsmaßnahmen zum Erlass eines in den Bereich der Gesetzgebung fallenden Beschlusses

Zum ersten Teil des zweiten Klagegrundes: Wahl einer aufgehobenen Rechtsgrundlage

– Vorbringen der Parteien

18 Das Parlament macht geltend, dass weder Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses noch die Art. 5 und 6 des Beschlusses 2009/934 als echte Rechtsgrundlagen angesehen werden könnten.

19 Diese Bestimmungen beschränkten sich nämlich auf eine implizite Bezugnahme auf Art. 34 Abs. 2 Buchst. c EU, der die einzig mögliche Rechtsgrundlage für den Erlass einer Maßnahme wie des angefochtenen Beschlusses im Rahmen der ehemaligen „dritten Säule“ gewesen sei.

20 Folglich sei die vom Rat verwendete Rechtsgrundlage Art. 34 Abs. 2 Buchst. c EU. Da dieser Artikel jedoch durch den Vertrag von Lissabon aufgehoben worden sei, könne er nicht mehr als Rechtsgrundlage für den Erlass neuer Rechtsakte herangezogen werden.

21 Der Rat erläutert, dass er den angefochtenen Beschluss auf der Grundlage von Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses erlassen habe. Die Art. 5 und 6 des Beschlusses 2009/934 seien als ergänzende Rechtsgrundlagen angeführt worden. Auch Ungarn ist der Ansicht, dass Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses eine ausreichende Rechtsgrundlage darstelle und dass es daher nicht erforderlich sei, für den Erlass des angefochtenen Beschlusses auf das Primärrecht Bezug zu nehmen.

– Würdigung durch den Gerichtshof

22 Zur Beurteilung der Begründetheit des ersten Teils des zweiten Klagegrundes ist die Rechtsgrundlage zu bestimmen, auf der der angefochtene Beschluss erlassen worden ist.

23 Hierzu ist festzustellen, dass dieser Beschluss nicht auf Art. 34 EU Bezug nimmt und dass seine Bezugsvermerke ausdrücklich auf Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses sowie auf die Art. 5 und 6 des Beschlusses 2009/934 verweisen.

24 In Anbetracht des Wortlauts des angefochtenen Beschlusses, der grundsätzlich die Rechtsgrundlage, auf die er gestützt ist, anführen muss, damit die Begründungspflicht erfüllt ist (vgl. in diesem Sinne Urteile Kommission/Rat, C‑370/07, EU:C:2009:590, Rn. 39 und 55, Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 29, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 19), kann daher nicht angenommen werden, dass dieser Beschluss auf Art. 34 EU beruht.

25 Im Übrigen lässt auch kein anderer Bestandteil des angefochtenen Beschlusses erkennen, dass der Rat die Absicht gehabt hätte, Art. 34 EU als Rechtsgrundlage für diesen Beschluss zu verwenden.

26 Vor allem ist die Annahme, dass Art. 34 Abs. 2 Buchst. c EU die einzig mögliche Rechtsgrundlage für den Erlass einer Maßnahme wie des angefochtenen Beschlusses darstellte, selbst wenn sie zutrifft, in diesem Zusammenhang unerheblich, da die ausdrückliche Entscheidung des Rates, in dem angefochtenen Beschluss nicht diese Bestimmung, sondern Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses sowie die Art. 5 und 6 des Beschlusses 2009/934 zu nennen, eindeutig zum Ausdruck bringt, dass der angefochtene Beschluss auf die zuletzt genannten Bestimmungen als solche gestützt ist (vgl. entsprechend Urteil Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 21).

27 Hierzu ist festzustellen, dass die Art. 5 und 6 des Beschlusses 2009/934 zwar nicht die Änderung der in Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses genannten Liste (im Folgenden: Liste) betreffen und daher nicht als Rechtsgrundlage für den angefochtenen Beschluss dienen konnten, dass die Nennung dieser Artikel in den Bezugsvermerken des Beschlusses aber in jedem Fall allenfalls einen rein formalen Fehler darstellt, da sie sich weder auf den Inhalt des angefochtenen Beschlusses noch auf das Verfahren zu dessen Erlass ausgewirkt hat (vgl. in diesem Sinne Urteil Vereinigtes Königreich/Rat, C‑81/13, EU:C:2014:2449, Rn. 65 bis 67).

28 Aus alledem folgt, dass die Aufhebung von Art. 34 EU durch den Vertrag von Lissabon dem angefochtenen Beschluss nicht seine Rechtsgrundlage entzieht.

29 Angesichts dessen ist der erste Teil des zweiten Klagegrundes als unbegründet zurückzuweisen.

Zum zweiten Teil des zweiten Klagegrundes und zum dritten Klagegrund: Wahl einer rechtswidrigen Rechtsgrundlage bzw. Wahl einer Rechtsgrundlage für Durchführungsmaßnahmen zum Erlass eines in den Bereich der Gesetzgebung fallenden Beschlusses

– Vorbringen der Verfahrensbeteiligten

30 Nach Auffassung des Parlaments stellt Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses, falls diese Bestimmung als Rechtsgrundlage des angefochtenen Beschlusses anzusehen sei, eine rechtswidrige abgeleitete Rechtsgrundlage dar, auf die dieser Beschluss nicht rechtswirksam gestützt werden könne.

31 Aus der Rechtsprechung des Gerichtshofs ergebe sich nämlich, dass die Schaffung einer abgeleiteten Rechtsgrundlage, die die Modalitäten für den Erlass eines Rechtsakts erleichtere, nicht mit den Verträgen vereinbar sei. Dies treffe auf Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses zu, da diese Bestimmung den Erlass der Durchführungsmaßnahmen dieses Beschlusses entgegen Art. 34 Abs. 2 Buchst. c EU nicht von der vorhergehenden Initiative eines Mitgliedstaats oder der Kommission abhängig mache.

32 Außerdem sei Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses infolge des Inkrafttretens des Vertrags von Lissabon unanwendbar geworden und enthalte eine rechtswidrige Abweichung von dem durch diesen Vertrag für den Erlass neuer Rechtsakte eingeführten Verfahren. Eine solche Abweichung werde durch Art. 9 des Protokolls (Nr. 36) über die Übergangsbestimmungen (im Folgenden: Protokoll über die Übergangsbestimmungen) nicht gestattet. Aus dieser Vorschrift ergebe sich lediglich, dass die Rechtsakte der ehemaligen „dritten Säule“ durch das Inkrafttreten dieses Vertrags nicht automatisch aufgehoben würden.

33 Im Übrigen macht das Parlament geltend, dass die Liste einen wesentlichen Aspekt des fraglichen Bereichs darstelle und daher Teil des Gesetzgebungsakts sein müsse. Sie sei zumindest als normatives Element anzusehen und müsse Gegenstand eines delegierten Rechtsakts im Sinne von Art. 290 AEUV – und nicht eines Durchführungsrechtsakts im Sinne von Art. 291 AEUV – sein.

34 Hierbei stützt sich das Parlament auf drei Erwägungen. Erstens lege der Europol-Beschluss nicht die Bedingungen fest, die erfüllt sein müssten, damit ein Staat in die Liste aufgenommen werde. Zweitens habe eine solche Aufnahme erhebliche Auswirkungen, und zwar auch auf die Grundrechte der Bürger. Drittens erfordere sie politische Entscheidungen, die in die eigene Zuständigkeit des Unionsgesetzgebers fielen.

35 Daraus folge, dass das gewählte Verfahren und die gewählte Rechtsgrundlage fehlerhaft gewesen seien, da der angefochtene Beschluss erlassen worden sei, als wäre er eine Durchführungsmaßnahme.

36 Der Rat ist der Ansicht, dass das Vorbringen des Parlaments zum einen zur Eigenschaft von Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses als abgeleiteter Rechtsgrundlage und zum anderen zu dem Umstand, dass die Änderung der Liste einen wesentlichen Aspekt des fraglichen Bereichs darstelle, als eine Einrede der Rechtswidrigkeit gegen diese Bestimmung zu betrachten seien.

37 Der Rat bestreitet die Zulässigkeit dieser Rechtswidrigkeitseinrede. Nach Art. 10 Abs. 1 des Protokolls über die Übergangsbestimmungen seien die Befugnisse des Gerichtshofs bezüglich des Europol-Beschlusses bis zum 1. Dezember 2014 diejenigen geblieben, die vor dem Inkrafttreten des Vertrags von Lissabon bestanden hätten. Der damals anwendbare Art. 35 Abs. 6 EU habe jedoch für das Parlament nicht die Möglichkeit vorgesehen, eine Nichtigkeitsklage gegen einen im Rahmen der früheren „dritten Säule“ erlassenen Rechtsakt wie den angefochtenen Beschluss zu erheben. Aus der damaligen sachlichen Unzuständigkeit des Gerichtshofs in diesem Bereich folge, dass die vom Parlament erhobene Einrede der Rechtswidrigkeit für unzulässig zu erklären sei.

38 Hilfsweise trägt der Rat, unterstützt durch Ungarn, vor, dass Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses zum Zeitpunkt des Erlasses dieses Beschlusses mit dem EU-Vertrag vereinbar gewesen sei. Diese Bestimmung beschränke sich nämlich darauf, die Anwendung des Verfahrens vorzusehen, das in Art. 34 Abs. 2 Buchst. c EU festgelegt sei. Dieser mache den Erlass einer Maßnahme wie des angefochtenen Beschlusses nicht notwendigerweise von der Initiative eines Mitgliedstaats oder der Kommission abhängig.

39 Der Rat und die Tschechische Republik sind ferner der Auffassung, dass eine Änderung der Liste keineswegs einen wesentlichen Aspekt des durch den Europol-Beschluss geregelten Bereichs betreffe.

40 Im Hinblick auf die Wirkungen des Inkrafttretens des Vertrags von Lissabon machen der Rat, die Tschechische Republik und Ungarn geltend, dass die vom Parlament vorgeschlagene Auslegung von Art. 9 des Protokolls über die Übergangsbestimmungen jede Möglichkeit paralysiere, die in den Rechtsakten der früheren „dritten Säule“ vorgesehenen Durchführungsmaßnahmen zu erlassen, was genau die Situation sei, die die Verfasser der Verträge hätten vermeiden wollen.

– Würdigung durch den Gerichtshof

41 Nach ständiger Rechtsprechung des Gerichtshofs muss die Wahl der Rechtsgrundlage eines Unionsrechtsakts auf objektiven und gerichtlich nachprüfbaren Umständen beruhen, zu denen das Ziel und der Inhalt des Rechtsakts gehören (Urteil Kommission/Parlament und Rat, C‑43/12, EU:C:2014:298, Rn. 29 und die dort angeführte Rechtsprechung).

42 In dieser Hinsicht ist hervorzuheben, dass zwischen den Parteien zum Verhältnis zwischen Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses und dem Ziel oder dem Inhalt des angefochtenen Beschlusses keine Uneinigkeit besteht. Allerdings stellt das Parlament die Rechtmäßigkeit dieser Bestimmung in Abrede, indem es geltend macht, dass sie die Modalitäten für den Erlass einer Maßnahme wie des angefochtenen Beschlusses im Vergleich zu dem in den Verträgen hierfür vorgesehenen Verfahren erleichtere.

43 Nach der Rechtsprechung des Gerichtshofs können jedoch – da die Grundsätze über die Willensbildung der Unionsorgane in den Verträgen festgelegt sind und nicht zur Disposition der Mitgliedstaaten oder der Organe selbst stehen – allein die Verträge ein Organ in besonderen Fällen dazu ermächtigen, ein von ihnen geschaffenes Entscheidungsverfahren zu ändern. Würde daher einem Organ die Möglichkeit zur Schaffung abgeleiteter Rechtsgrundlagen gegeben, die den Erlass von Gesetzgebungsakten oder Durchführungsmaßnahmen ermöglichen, sei es im Sinne einer Verschärfung oder einer Erleichterung der Modalitäten des Erlasses eines Rechtsakts, so liefe dies darauf hinaus, ihm eine Rechtsetzungsbefugnis zu verleihen, die über das in den Verträgen vorgesehene Maß hinausginge (vgl. in diesem Sinne Urteile Parlament/Rat, C‑133/06, EU:C:2008:257, Rn. 54 bis 56, Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 42 und 43, sowie Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 32 und 33).

44 In diesem Zusammenhang ist erstens das Vorbringen des Parlaments zu prüfen, wonach die Rechtsgrundlage und das Verfahren, die für den Erlass des angefochtenen Beschlusses gewählt worden seien, deshalb fehlerhaft seien, weil dieser einen wesentlichen Aspekt des geregelten Bereichs betreffe, der nur durch einen Gesetzgebungsakt geregelt werden könne.

45 Da das in Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses vorgesehene Verfahren zur Änderung der Liste nicht dem im Primärrecht für den Erlass von Gesetzgebungsakten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vorgesehenen entspricht, ist dieses Vorbringen dahin zu verstehen, dass damit geltend gemacht wird, Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses sei rechtswidrig, weil er den Erlass eines Rechtsakts, der einen wesentlichen Aspekt des geregelten Bereichs betreffe, in einem flexibleren als dem im Primärrecht hierfür vorgesehenen Verfahren ermögliche.

46 Nach ständiger Rechtsprechung des Gerichtshofs ist der Erlass der wesentlichen Vorschriften einer Materie wie der in der vorliegenden Rechtssache fraglichen der Zuständigkeit des Unionsgesetzgebers vorbehalten; diese Bestimmungen sind in der Grundregelung zu erlassen. Daraus folgt, dass Bestimmungen, die wesentliche Aspekte einer Grundregelung festlegen und deren Erlass politische Entscheidungen erfordert, die in die eigene Zuständigkeit des Unionsgesetzgebers fallen, weder Gegenstand einer solchen Befugnisübertragung sein noch in Durchführungsrechtsakte aufgenommen werden können (vgl. in diesem Sinne Urteil Parlament/Rat, C‑355/10, EU:C:2012:516, Rn. 64 bis 66).

47 Die Bestimmung der Aspekte einer Materie, die als wesentlich einzustufen sind, muss sich nach objektiven Gesichtspunkten richten, die Gegenstand einer gerichtlichen Kontrolle sein können, und verlangt, die

Merkmale und die Besonderheiten des betreffenden Sachgebiets zu berücksichtigen (vgl. in diesem Sinne Urteil Parlament/Rat, C‑355/10, EU:C:2012:516, Rn. 67 und 68).

48 Im vorliegenden Fall ergibt sich aus Art. 3 des Europol-Beschlusses, dass es das Ziel von Europol ist, die Tätigkeit der zuständigen Behörden der Mitgliedstaaten sowie deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität zu unterstützen und zu verstärken, wenn zwei oder mehr Mitgliedstaaten betroffen sind.

49 In diesem Zusammenhang stellt die Aufnahme von Beziehungen zwischen Europol und Drittstaaten eine mit den Tätigkeiten von Europol zusammenhängende Tätigkeit dar, da die Zusammenarbeit mit diesen Staaten in Anwendung von Art. 23 Abs. 1 des Europol-Beschlusses im Übrigen nur hergestellt und unterhalten werden kann, soweit dies für die Erfüllung der Aufgaben von Europol erforderlich ist.

50 Zudem hat der Unionsgesetzgeber den Grundsatz der Herstellung und Aufrechterhaltung solcher Beziehungen verankert, das mit diesen Beziehungen zu verfolgende Ziel festgelegt und den Rahmen abgesteckt, in dem sich diese Beziehungen halten müssen.

51 Selbst wenn daher ein Beschluss zur Änderung der Liste bestimmte Schiedsverfahren mit technischer und politischer Dimension einschließt, kann nicht angenommen werden, dass ein solcher Beschluss politische Entscheidungen erfordert, die in die eigene Zuständigkeit des Unionsgesetzgebers fallen.

52 Das Vorbringen des Parlaments, die Änderung der Liste könne erhebliche Auswirkungen auf die Grundrechte der Bürger haben, kann hieran nichts ändern.

53 Zwar ist zum einen darauf hinzuweisen, dass die Übermittlung personenbezogener Daten, die die in Anwendung von Art. 23 des Europol-Beschlusses geschlossenen Abkommen zulassen können, einen Eingriff in die Grundrechte der betroffenen Personen darstellen kann, und zum anderen, dass bestimmte dieser Eingriffe so erheblich sein können, dass der Unionsgesetzgeber tätig werden muss (vgl. in diesem Sinne Urteil Parlament/Rat, C‑355/10, EU:C:2012:516, Rn. 77).

54 Der Grundsatz der Übermittlung personenbezogener Daten an bestimmte Drittstaaten und der Rahmen, in dem diese Übermittlung zu erfolgen hat, sind jedoch vom Gesetzgeber selbst festgelegt worden, da nach Art. 23 Abs. 6 Buchst. b des Europol-Beschlusses und Art. 5 Abs. 4 des Beschlusses 2009/934 insbesondere festzustellen ist, dass der betreffende Drittstaat ein angemessenes Datenschutzniveau gewährleistet.

55 Jedenfalls erlaubt die Aufnahme eines Drittstaats in die Liste als solche keine Übermittlung der personenbezogenen Daten an diesen. Aus Art. 23 Abs. 2, 4 und 6 des Europol-Beschlusses ergibt sich nämlich, dass eine solche Übermittlung erst nach dem Abschluss eines Abkommens zwischen Europol und diesem Staat möglich ist, das speziell die Übermittlung solcher Daten zulässt. Insoweit ist darauf hinzuweisen, dass aus Art. 23 Abs. 2 dieses Beschlusses in Verbindung mit den Art. 5 und 6 des Beschlusses 2009/934 und Art. 1 des Beschlusses 2009/935 hervorgeht, dass die Aushandlung und der Abschluss eines solchen Abkommens – nach der Aufnahme des betreffenden Drittstaats in die Liste – aufeinanderfolgende Beschlüsse des Verwaltungsrats von Europol und des Rates einschließt, wobei es Ersterem freisteht, den Direktor von Europol nicht zu ermächtigen, Verhandlungen mit dem betreffenden Drittstaat aufzunehmen, diese Verhandlungen auf den Abschluss eines Abkommens zu richten, das den Austausch personenbezogener Daten nicht zulässt, oder den vom Direktor ausgehandelten Entwurf des Abkommens nicht endgültig zu billigen, und es Zweiterem freisteht, den von Europol übermittelten Entwurf nicht zu billigen.

56 Zum Vorbringen des Parlaments, der Europol-Beschluss lege nicht die Bedingungen fest, die erfüllt sein müssten, damit ein Drittstaat in die Liste aufgenommen werde, ist festzustellen, dass die Voraussetzungen für eine solche Aufnahme in Art. 23 Abs. 1 dieses Beschlusses hinreichend genau bestimmt sind.

57 Aus alledem folgt, dass die Änderung der Liste kein wesentlicher Aspekt des durch den Europol-Beschluss geregelten Bereichs ist und es dem Unionsgesetzgeber daher freistand, vorzusehen, dass sie durch einen Durchführungsrechtsakt vorgenommen werden kann.

58 Daher ist zweitens das Vorbringen des Parlaments zu prüfen, wonach Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses insoweit rechtswidrig sei, als er den Erlass von Maßnahmen zur Durchführung dieses Beschlusses ohne vorhergehende Initiative eines Mitgliedstaats oder der Kommission zulasse.

59 Da die Rechtmäßigkeit eines Unionsrechtsakts anhand der Sach- und Rechtslage zum Zeitpunkt seines Erlasses zu beurteilen ist, ist die Rechtmäßigkeit von Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses in diesem Zusammenhang anhand der Bestimmungen zu beurteilen, die zum Zeitpunkt des Erlasses dieses Beschlusses die Durchführung der allgemeinen Rechtsakte im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen regelten, d. h. anhand der Art. 34 Abs. 2 Buchst. c EU und 39 Abs. 1 EU (vgl. entsprechend Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 45, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 35).

60 Aus diesen Bestimmungen ergibt sich, dass der Rat mit qualifizierter Mehrheit nach Anhörung des Parlaments die Maßnahmen annimmt, die zur Durchführung der im Rahmen des Titels zur polizeilichen und justiziellen Zusammenarbeit in Strafsachen erlassenen Beschlüsse erforderlich sind.

61 Zwischen den Verfahrensbeteiligten ist jedoch streitig, wie die in Art. 34 Abs. 2 Buchst. c EU festgelegten Regeln im Hinblick auf die Frage auszulegen ist, ob der Erlass dieser Durchführungsmaßnahmen eine vorhergehende Initiative eines Mitgliedstaats oder der Kommission erfordert.

62 Insoweit ist darauf hinzuweisen, dass diese Bestimmung zwischen Beschlüssen, die der Rat einstimmig erlassen kann, und den zu deren Durchführung auf Unionsebene erforderlichen Maßnahmen unterscheidet, die der Rat mit qualifizierter Mehrheit erlässt.

63 In diesem Zusammenhang ist die Wendung „auf Initiative eines jeden Mitgliedstaats oder der Kommission“ in Anbetracht der Syntax der Sätze, die diese Bestimmung bilden, so zu verstehen, dass sie sich nur auf die grundlegenden Maßnahmen bezieht, die der Rat einstimmig erlassen kann.

64 Aus dem Wortlaut dieser Bestimmung geht demnach hervor, dass sie dahin auszulegen ist, dass eine Initiative eines Mitgliedstaats oder der Kommission für den Erlass von Durchführungsmaßnahmen wie dem angefochtenen Beschluss nicht erforderlich ist.

65 Diese Auslegung wird durch den Zusammenhang bestätigt, in den sich Art. 34 Abs. 2 Buchst. c der EU einfügt und der bei dessen Auslegung zu berücksichtigen ist (vgl. in diesem Sinne Urteil M’Bodj, C‑542/13, EU:C:2014:2452, Rn. 34 und die dort angeführte Rechtsprechung).

66 Was die nach Inkrafttreten des Vertrags von Lissabon speziell für die polizeiliche und justizielle Zusammenarbeit in Strafsachen geltenden Bestimmungen betrifft, erfordern die Art. 76 AEUV und 291 AEUV die Initiative eines Mitgliedstaats oder der Kommission nämlich nur für den Erlass von Gesetzgebungsakten, nicht aber für den Erlass von Durchführungsmaßnahmen.

67 Folglich ist das Vorbringen des Parlaments zurückzuweisen, wonach davon auszugehen sei, dass der Europol-Beschluss, da sein Art. 26 Abs. 1 Buchst. a den Erlass von Maßnahmen zur Durchführung dieses Beschlusses ohne vorhergehende Initiative eines Mitgliedstaats oder der Kommission zulasse, Modalitäten für den Erlass dieser Maßnahmen festlege, die im Vergleich zu dem im EU-Vertrag hierfür vorgesehenen Verfahren erleichtert seien.

68 Hinsichtlich des Vorbringens des Parlaments zur Unvereinbarkeit von Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses mit den nach Inkrafttreten des Vertrags von Lissabon anwendbaren Verfahrensvorschriften ist jedenfalls darauf hinzuweisen, dass das Protokoll über die Übergangsbestimmungen Vorschriften speziell zu den rechtlichen Regelungen enthält, die nach Inkrafttreten dieses Vertrags auf die vor diesem Zeitpunkt auf der Grundlage des EU-Vertrags erlassenen Rechtsakte anwendbar sind (vgl. in diesem Sinne Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 51, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 41).

69 So sieht Art. 9 dieses Protokolls vor, dass diese Rechtsakte so lange Rechtswirkung behalten, bis sie in Anwendung der Verträge aufgehoben, für nichtig erklärt oder geändert werden.

70 Der Gerichtshof hat jedoch entschieden, dass dieser Artikel dahin auszulegen ist, dass eine Bestimmung eines vor Inkrafttreten des Vertrags von Lissabon ordnungsgemäß auf der Grundlage des EU-Vertrags ergangenen Rechtsakts, die Modalitäten für den Erlass von Durchführungsmaßnahmen zu diesem Rechtsakt vorsieht, weiterhin ihre Rechtswirkungen entfaltet, solange sie nicht aufgehoben, für nichtig erklärt oder geändert worden ist, und den Erlass dieser Maßnahmen in Anwendung des von ihr definierten Verfahrens ermöglicht (Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 57, sowie Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 47).

71 Da Art. 290 AEUV nicht anwendbar ist, kann Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses daher nicht mit dieser Bestimmung des AEU‑Vertrags unvereinbar sein.

72 Ebenso wenig kann das Vorbringen des Parlaments, mit dem es dartun möchte, dass Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses im Vergleich zu dem durch den AEU-Vertrag hierfür vorgesehenen Verfahren verschärfte oder erleichterte Modalitäten für den Erlass von Durchführungsmaßnahmen vorsieht, den Gerichtshof zu der Feststellung veranlassen, dass diese Bestimmung eine rechtswidrige abgeleitete Rechtsgrundlage darstellt, deren Anwendung im Wege der Einrede ausgeschlossen werden müsste (vgl. entsprechend Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 58, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 48).

73 Unter diesen Umständen sind der zweite Teil des zweiten Klagegrundes und der dritte Klagegrund, ohne dass über ihre Zulässigkeit entschieden zu werden braucht, daher als unbegründet zurückzuweisen (vgl. in diesem Sinne Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 59, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 49 und die dort angeführte Rechtsprechung), so dass diese Klagegründe vollumfänglich zurückzuweisen sind.

Erster Klagegrund: Verletzung wesentlicher Formvorschriften

Vorbringen der Verfahrensbeteiligten

74 Das Parlament trägt vor, dass der angefochtene Beschluss, falls die vor dem Vertrag von Lissabon geltende Regelung im vorliegenden Fall anwendbar bleibe, gemäß Art. 34 Abs. 2 Buchst. c EU in Verbindung mit Art. 39 Abs. 1 EU auf Initiative eines Mitgliedstaats oder der Kommission und nach Anhörung des Parlaments zu erlassen sei.

75 Zum einen sei der angefochtene Beschluss aber nicht auf Initiative eines Mitgliedstaats oder der Kommission erlassen worden. Zum anderen habe die Anhörung des Parlaments durch den Rat nicht den Anforderungen von Art. 39 Abs. 1 EU und Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses entsprochen, da sie nach Ansicht des Rates nur fakultativ gewesen sei.

76 Der Rat ist dagegen der Auffassung, dass weder der Europol-Beschluss noch Art. 34 Abs. 2 Buchst. c EU, Art. 291 Abs. 2 AEUV oder Art. 76 AEUV es erforderten, dass ein Rechtsakt wie der angefochtene Beschluss auf Initiative eines Mitgliedstaats oder der Kommission erlassen würde.

77 Der Rat sei aufgrund der Aufhebung von Art. 39 EU durch den Vertrag von Lissabon nicht mehr verpflichtet, das Parlament anzuhören. Die Auferlegung einer solchen Verpflichtung würde im Übrigen darauf hinauslaufen, dem Verfahren nach Art. 291 AEUV einen dort nicht vorgesehenen Bestandteil hinzuzufügen, und damit das durch den Vertrag von Lissabon geschaffene institutionelle Gleichgewicht in Frage stellen.

78 Ungarn macht geltend, der Rat sei der in Art. 26 Abs. 1 des Europol-Beschlusses vorgeschriebenen Anhörungspflicht mit dem Instrument der freiwilligen Anhörung, das er eingesetzt habe, nachgekommen.

Würdigung durch den Gerichtshof

79 Was erstens den Erlass des angefochtenen Beschlusses ohne vorhergehende Initiative eines Mitgliedstaats oder der Kommission angeht, ist festzustellen, dass Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses eine solche Initiative nicht vorsieht. Aus dieser Bestimmung in Verbindung mit Art. 2 Abs. 2 des Beschlusses 2009/935 geht vielmehr hervor, dass es der Verwaltungsrat von Europol ist, der die Aufnahme eines Drittstaats in die Liste vorzuschlagen hat.

80 Ferner ergibt sich aus den Ausführungen in den Rn. 62 bis 66 des vorliegenden Urteils, dass Art. 34 Abs. 2 Buchst. c EU auch nicht vorschrieb, dass Durchführungsmaßnahmen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf Initiative eines Mitgliedstaats oder der Kommission zu erlassen sind.

81 Unter diesen Umständen stellt es keine Verletzung einer wesentlichen Formvorschrift dar, wenn dem Erlass des angefochtenen Beschlusses keine Initiative eines Mitgliedstaats oder der Kommission vorausging.

82 Was zweitens die Bedingungen betrifft, unter denen das Parlament angehört wurde, stellt die ordnungsgemäße Anhörung des Parlaments in den durch die anwendbaren Regelungen des Unionsrechts vorgesehenen Fällen ein wesentliches Formerfordernis dar, dessen Missachtung die Nichtigkeit der betroffenen Handlung zur

Folge hat (Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 63, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 53 und die dort angeführte Rechtsprechung).

83 Da sich aus der Würdigung des zweiten und des dritten Klagegrundes ergibt, dass der Rat den angefochtenen Beschluss rechtswirksam auf Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses stützen konnte, ist daher zu prüfen, ob das Parlament gemäß dieser Bestimmung vor dem Erlass eines Rechtsakts anzuhören war.

84 Schon nach dem Wortlaut dieser Bestimmung war der Rat gehalten, vor einer Änderung der Liste das Parlament anzuhören.

85 Entgegen dem Vorbringen des Rates kann die Aufhebung von Art. 39 Abs. 1 EU durch den Vertrag von Lissabon diese Pflicht zur Anhörung des Parlaments nicht in Frage stellen, da diese in Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses ausdrücklich vorgesehen ist.

86 Ebenso wenig von Bedeutung ist der Umstand, dass Art. 291 AEUV keine Verpflichtung zur Anhörung des Parlaments vorsieht. Denn die Verpflichtung, das Parlament anzuhören, stellt eine der Rechtswirkungen des Europol-Beschlusses dar, die gemäß Art. 9 des Protokolls über die Übergangsbestimmungen nach Inkrafttreten des Vertrags von Lissabon fortbesteht (vgl. entsprechend Urteile Parlament/Rat, C‑317/13 und C‑679/13, EU:C:2015:223, Rn. 68, und Parlament/Rat, C‑540/13, EU:C:2015:224, Rn. 58).

87 Im vorliegenden Fall steht fest, dass der angefochtene Beschluss vom Rat nach Anhörung des Parlaments erlassen wurde.

88 Das Parlament macht jedoch geltend, der Rat habe dadurch, dass er diese Anhörung in der Meinung durchgeführt habe, dass er nicht dazu verpflichtet sei, eine wesentliche Formvorschrift verletzt.

89 Insoweit ist festzustellen, dass nicht behauptet und erst recht nicht nachgewiesen worden ist, dass der vom Rat hinsichtlich des Rahmens, in dem die Anhörung des Parlaments erfolgen musste, begangene Fehler in der Praxis dazu geführt hätte, dass der dem Parlament in dem Verfahren zum Erlass des angefochtenen Beschlusses eingeräumte Platz eingeschränkt oder der Inhalt dieses Beschlusses berührt worden wäre.

90 Insbesondere konnte das Parlament dem Rat vor dem Erlass dieses Beschlusses seinen Standpunkt darlegen. Im Übrigen ergibt sich aus dem Wortlaut der Stellungnahme, die das Parlament in diesem Verfahren abgegeben hat, und seinen Erläuterungen in der mündlichen Verhandlung, dass es, als es diese Stellungnahme annahm, davon ausging, dass es vom Rat gemäß der in Art. 26 Abs. 1 Buchst. a des Europol-Beschlusses genannten Anhörungspflicht angehört worden sei.

91 Unter diesen Umständen ist nicht erwiesen, dass der vom Rat begangene Fehler die wirksame Beteiligung des Parlaments an dem fraglichen Verfahren verhindert oder zu einer Beeinträchtigung der Bedingungen geführt hat, unter denen das Parlament seine Funktionen ausübt (vgl. in diesem Sinne Urteile Parlament/Rat, C‑392/95, EU:C:1997:289, Rn. 14, und Parlament/Rat, C‑658/11, EU:C:2014:2025, Rn. 81).

92 Diese Schlussfolgerung wird nicht durch die Ausführungen des Gerichtshofs im Urteil Parlament/Rat (C‑316/91, EU:C:1994:76) in Frage gestellt.

93 Der Gerichtshof hat in diesem Urteil zwar festgestellt, dass die fehlerhafte Wahl einer Rechtsgrundlage, die die Anhörung des Parlaments nicht vorsieht, die Befugnis des Parlaments – die in dem Recht liegt, angehört zu werden, wenn das Primärrecht dies vorsieht – selbst dann verletzen kann, wenn eine fakultative Anhörung stattgefunden hat (Urteil Parlament/Rat, C‑316/91, EU:C:1994:76, Rn. 14).

94 Diese Feststellung hat der Gerichtshof in diesem Urteil jedoch nur im Hinblick auf die Beurteilung der Zulässigkeit einer vom Parlament gegen einen Rechtsakt des Rates erhobenen Klage getroffen, ohne sich zu der Frage zu äußern, ob ein dem Rat bei der Auslegung der anwendbaren Rechtsgrundlage hinsichtlich des zwingenden Charakters der Anhörung des Parlaments unterlaufener Fehler als solcher – unabhängig von seinen konkreten Auswirkungen auf die wirksame Beteiligung des Parlaments an einem bestimmten Verfahren oder auf die Bedingungen, unter denen das Parlament seine Funktionen ausübt –eine Verletzung einer wesentlichen Formvorschrift darstellt.

95 Die Lösung, zu der der Gerichtshof in der Rechtssache gelangt ist, in der dieses Urteil ergangen ist, beruhte zudem teilweise darauf, dass der die behauptete Rechtsgrundlage betreffende Fehler zum Ausschluss der Anwendung einer Bestimmung führte, nach der das Parlament die Anwendung des Konzertierungsverfahrens bean-

tragen konnte (Urteil Parlament/Rat, C‑316/91, EU:C:1994:7, Rn. 18), was in der vorliegenden Rechtssache nicht der Fall ist.

96 Der Gerichtshof hat außerdem entschieden, dass die fehlerhafte Ersetzung einer Rechtsgrundlage, die die Anhörung des Parlaments nicht vorsieht, durch eine Rechtsgrundlage, die eine solche Anhörung gebietet, einen rein formalen Fehler darstellt (Urteil Kommission/Rat, 165/87, EU:C:1988:458, Rn. 20). Daher ist der Umstand, dass der Rat über den Rechtsrahmen geirrt hat, in dem er das Parlament anhört, nicht geeignet, sich auf den Inhalt des am Ende des betreffenden Verfahrens ergangenen Beschlusses auszuwirken.

97 Nach alledem ist der erste Klagegrund insgesamt zurückzuweisen.

98 Da keiner der vom Parlament geltend gemachten Klagegründe durchgreift, ist die Klage abzuweisen. […]

**6) EuGH C-518/07 - Europäische Kommission**

*a) Sachverhalt*

Die Richtlinie (RL) 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verpflichtet die Mitgliedstaaten, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (Art. 1 RL 95/46). Gemäß Art. 28 RL („Kontrollstelle") sehen die Mitgliedstaaten vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen, und dass diese Stellen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland wird die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit überwacht, die Verarbeitung solcher Daten durch öffentliche Stellen der Länder vom jeweiligen Landesdatenschutzbeauftragten. Alle diese Datenschutzbeauftragten sind nur gegenüber ihrem jeweiligen Parlament rechenschaftspflichtig und unterliegen in aller Regel keinerlei Aufsicht, Weisungen oder sonstigem Einfluss durch die von ihnen zu kontrollierenden öffentlichen Stellen. Dagegen ist die Stellung der mit der Kontrolle der Datenverarbeitung des nichtöffentlichen Bereichs beauftragten Stellen von Land zu Land unterschiedlich ausgestaltet. Den Gesetzen der Länder ist jedoch gemeinsam, dass diese Kontrollstellen ausdrücklich einer staatlichen Aufsicht unterworfen sind. In Letzterem sah die Kommission einen Verstoß gegen die Vorgabe der Unabhängigkeit des Art. 28 I UA 2 der RL. Während der Generalanwalt dies verneinte, gab der EuGH der Klage statt.
(Zusammenfassung nach JuS 2010, 556, beck-online)

Im vorliegenden Rechtsstreit geht es um die gegensätzlichen Auffassungen der Kommission, die vom EDSB unterstützt wird, und der Bundesrepublik Deutschland hinsichtlich der Wendung „in völliger Unabhängigkeit" in Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 und der Wahrnehmung der Aufgaben der Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

15 Nach Auffassung der Kommission und des EDSB, die von einer weiten Auslegung der Wendung „in völliger Unabhängigkeit" ausgehen, ist das Erfordernis, dass die Kontrollstellen ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen, dahin auszulegen, dass eine Kontrollstelle jeglicher Einflussnahme, sei es durch sonstige Behörden, sei es von außerhalb der Staatsverwaltung, entzogen sein müsse. Die staatliche Aufsicht, der die mit der Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich beauftragten Stellen in Deutschland unterworfen seien, verstoße daher gegen dieses Erfordernis.

16 Die Bundesrepublik Deutschland vertritt dagegen eine engere Auslegung der Wendung „in völliger Unabhängigkeit". Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 verlange eine funktionale Unabhängigkeit der Kontrollstellen in dem Sinne, dass sie von dem ihrer Kontrolle unterstellten nichtöffentlichen Bereich unabhängig sein müssten und keinen sachfremden Einflüssen unterliegen dürften. Die staatliche Aufsicht in den Bundesländern stelle keinen sachfremden Einfluss dar, sondern einen verwaltungsinternen Mechanismus der Kontrolle durch Stellen innerhalb desselben Verwaltungsapparats, die in derselben Weise wie die Kontrollstellen den Zielvorgaben der Richtlinie 95/46 verpflichtet seien.

*b) Leitsatz*

1. Die Bundesrepublik Deutschland hat gegen ihre Verpflichtungen aus Art. 28 I Unterabs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verstoßen, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen und öffentlich-rechtliche Wett-

bewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben "in völliger Unabhängigkeit" wahrnehmen, falsch umgesetzt hat. (amtlicher Leitsatz)
(EuGH Urt. v. 9.3.2010 – C-518/07, BeckRS 2010, 90304, beck-online)

*c) Begründung*

[…]Zur Tragweite des Erfordernisses der Unabhängigkeit der Kontrollstellen

17 Die Beurteilung der Begründetheit der vorliegenden Klage hängt davon ab, welche Tragweite das Unabhängigkeitserfordernis des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 hat, und somit von der Auslegung dieser Bestimmung. In diesem Zusammenhang sind deren Wortlaut sowie die Ziele und die Systematik der Richtlinie 95/46 heranzuziehen.

18 Was erstens den Wortlaut von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 angeht, ist angesichts des Fehlens einer Definition in der Richtlinie auf den gewöhnlichen Sinn der Wendung „in völliger Unabhängigkeit“ abzustellen. In Bezug auf öffentliche Stellen bezeichnet der Begriff „Unabhängigkeit“ in der Regel eine Stellung, in der gewährleistet ist, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann.

19 Entgegen dem Standpunkt der Bundesrepublik Deutschland deutet nichts darauf hin, dass das Unabhängigkeitserfordernis allein das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen beträfe. Im Gegenteil wird der Begriff „Unabhängigkeit“ durch das Adjektiv „völlig“ verstärkt, was eine Entscheidungsgewalt impliziert, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei sie unmittelbar oder mittelbar, entzogen ist.

20 Zweitens geht in Bezug auf die Ziele der Richtlinie 95/46 insbesondere aus deren Erwägungsgründen 3, 7 und 8 hervor, dass sie durch die Harmonisierung der nationalen Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in erster Linie den freien Verkehr dieser Daten zwischen Mitgliedstaaten gewährleisten soll (vgl. in diesem Sinne Urteil vom 20. Mai 2003, Österreichischer Rundfunk u. a., C‑465/00, C‑138/01 und C‑139/01, Slg. 2003, I‑4989, Randnrn. 39 und 70), der für die Errichtung und das Funktionieren des Binnenmarkts nach Art. 14 Abs. 2 EG erforderlich ist.

21 Der freie Verkehr personenbezogener Daten kann jedoch das Recht auf Privatsphäre beeinträchtigen, wie es u. a. in Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (vgl. in diesem Sinne Urteile des EGMR vom 16. Februar 2000, Amann/Schweiz, Recueil des arrêts et décisions 2000-II, §§ 69 und 80, und vom 4. Mai 2000, Rotaru/Rumänien, Recueil des arrêts et décisions 2000-V, §§ 43 und 46) und durch die allgemeinen Grundsätze des Gemeinschaftsrechts anerkannt ist.

22 Deshalb und wie insbesondere aus ihrem zehnten Erwägungsgrund und Art. 1 hervorgeht, hat die Richtlinie 95/46 außerdem zum Ziel, den durch die bestehenden nationalen Rechtsvorschriften garantierten Schutz nicht zu verringern, sondern vielmehr in der Gemeinschaft bei der Verarbeitung personenbezogener Daten ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten zu gewährleisten (vgl. in diesem Sinne Urteile Österreichischer Rundfunk u. a., Randnr. 70, sowie vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C‑73/07, Slg. 2008, I‑9831, Randnr. 52).

23 Die in Art. 28 der Richtlinie 95/46 vorgesehenen Kontrollstellen sind somit die Hüter dieser Grundrechte und Grundfreiheiten, und ihre Einrichtung in den Mitgliedstaaten gilt, wie es im 62. Erwägungsgrund der Richtlinie heißt, als ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.

24 Um diesen Schutz zu gewährleisten, müssen die Kontrollstellen zum einen die Achtung des Grundrechts auf Privatsphäre und zum anderen die Interessen, die den freien Verkehr personenbezogener Daten verlangen, miteinander ins Gleichgewicht bringen. Im Übrigen sind die verschiedenen nationalen Kontrollstellen nach Art. 28 Abs. 6 der Richtlinie 95/46 zu gegenseitiger Zusammenarbeit aufgerufen und können gegebenenfalls von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

25 Die Gewährleistung der Unabhängigkeit der nationalen Kontrollstellen soll die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen und ist im Licht dieses Zwecks auszulegen. Sie wurde eingeführt, um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen selbst oder ihren Bevollmächtigten eine besondere Stellung zu verleihen. Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Ein-

flussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen.

26 Drittens ist die Richtlinie 95/46 hinsichtlich ihrer Systematik als Gegenstück zu Art. 286 EG und der Verordnung Nr. 45/2001 zu sehen. Diese betreffen die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft sowie den freien Verkehr dieser Daten. Die Richtlinie verfolgt diese Ziele ebenfalls, aber in Bezug auf die Verarbeitung solcher Daten in den Mitgliedstaaten.

27 So wie Kontrollstellen auf nationaler Ebene bestehen, ist auch auf der Ebene der Union eine Kontrollstelle damit beauftragt, die Anwendung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen, nämlich der EDSB. Nach Art. 44 Abs. 1 der Verordnung Nr. 45/2001 übt dieser sein Amt in völliger Unabhängigkeit aus. In Abs. 2 desselben Artikels wird zur Erläuterung dieses Begriffs der Unabhängigkeit hinzugefügt, dass der EDSB in Ausübung seines Amtes niemanden um Weisung ersucht und keine Weisungen entgegennimmt.

28 Angesichts dessen, dass Art. 44 der Verordnung Nr. 45/2001 und Art. 28 der Richtlinie 95/46 dasselbe allgemeine Konzept zugrunde liegt, sind beide Bestimmungen homogen auszulegen, so dass nicht nur die Unabhängigkeit des EDSB, sondern auch die der nationalen Stellen impliziert, dass sie bei der Wahrnehmung ihrer Aufgaben keinerlei Weisungen unterliegen.

29 Ausgehend vom Wortlaut von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 sowie von den Zielen und der Systematik dieser Richtlinie ist eine klare Auslegung der genannten Bestimmung möglich. Folglich ist es nicht erforderlich, die Entstehungsgeschichte dieser Richtlinie heranzuziehen oder auf die einander widersprechenden Ausführungen der Kommission und der Bundesrepublik Deutschland dazu einzugehen.

30 Nach alledem ist Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 dahin auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen.

Zur staatlichen Aufsicht

31 Sodann ist zu prüfen, ob die staatliche Aufsicht, der in Deutschland die Kontrollstellen unterworfen sind, die die Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich überwachen, mit dem so beschriebenen Unabhängigkeitserfordernis vereinbar ist.

32 Hierzu ist festzustellen, dass die staatliche Aufsicht gleich welcher Art es der Regierung des betroffenen Landes oder einer Stelle der ihr untergeordneten Verwaltung grundsätzlich ermöglicht, auf Entscheidungen der Kontrollstellen unmittelbar oder mittelbar Einfluss zu nehmen bzw. diese Entscheidungen aufzuheben und zu ersetzen.

33 Es trifft zwar, wie die Bundesrepublik Deutschland geltend macht, a priori zu, dass die staatliche Aufsicht nur sicherstellen soll, dass das Handeln der Kontrollstellen den geltenden nationalen und gemeinschaftsrechtlichen Bestimmungen entspricht, und demnach nicht darauf abzielt, diese Stellen dazu zu zwingen, politische Zielsetzungen zu verfolgen, die dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den Grundrechten zuwiderlaufen.

34 Es lässt sich aber nicht ausschließen, dass die Aufsichtsstellen, die Teil der allgemeinen Staatsverwaltung und damit der Regierung des jeweiligen Landes unterstellt sind, nicht zu objektivem Vorgehen in der Lage sind, wenn sie die Vorschriften über die Verarbeitung personenbezogener Daten auslegen und anwenden.

35 Die Regierung des betroffenen Landes hat nämlich, wie der EDSB in seinen Erklärungen hervorhebt, möglicherweise ein Interesse an der Nichteinhaltung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, wenn es um die Verarbeitung solcher Daten im nichtöffentlichen Bereich geht. Sie kann selbst involvierte Partei dieser Verarbeitung sein, wenn sie davon betroffen ist oder sein könnte, z. B. im Fall einer Kooperation von öffentlichen und privaten Stellen oder im Rahmen öffentlicher Aufträge an den privaten Bereich. Außerdem könnte sie ein besonderes Interesse haben, wenn sie für bestimmte ihrer Aufgaben, insbesondere zu Zwecken der Finanzverwaltung oder der Strafverfolgung, Zugang zu Daten-

banken benötigt oder ein solcher Zugang einfach nur sachdienlich ist. Im Übrigen könnte diese Regierung auch geneigt sein, wirtschaftlichen Interessen den Vorrang zu geben, wenn es um die Anwendung der genannten Vorschriften durch bestimmte Unternehmen geht, die für das Land oder die Region wirtschaftlich von Bedeutung sind.

36 Hinzu kommt, dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte es, wie die Kommission ausführt, einen „vorauseilenden Gehorsam“ der Kontrollstellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstellen geben. Zum anderen erfordert die Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben sind.

37 Nach alledem ist festzustellen, dass die staatliche Aufsicht, der die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen in Deutschland unterworfen sind, nicht mit dem Unabhängigkeitserfordernis, wie es in Randnr. 30 des vorliegenden Urteils beschrieben ist, vereinbar ist.

Zu den von der Bundesrepublik Deutschland angeführten Grundsätzen des Gemeinschaftsrechts

38 Nach Auffassung der Bundesrepublik Deutschland würde es gegen mehrere Grundsätze des Gemeinschaftsrechts verstoßen, das Unabhängigkeitserfordernis des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 so auszulegen, dass der Mitgliedstaat gezwungen wäre, sein bewährtes und effektives System der Aufsicht über die Kontrollstellen hinsichtlich der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich aufzugeben.

39 Erstens stehe insbesondere das Demokratieprinzip einer weiten Auslegung dieses Unabhängigkeitserfordernisses entgegen.

40 Dieses Prinzip, das nicht nur in der deutschen Verfassung, sondern auch in Art. 6 Abs. 1 EU verankert sei, verlange eine Weisungsgebundenheit der Verwaltung gegenüber der Regierung, die ihrerseits dem Parlament verantwortlich sei. So müssten Eingriffe in die Rechte der Bürger und Unternehmen der Rechtsaufsicht des zuständigen Ministers unterliegen. Da die Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gemäß Art. 28 Abs. 3 der Richtlinie 95/46 über bestimmte Eingriffsbefugnisse gegenüber Bürgern und dem nichtöffentlichen Bereich verfügten, sei eine erweiterte Rechtmäßigkeitskontrolle ihres Handelns über Rechts- oder Fachaufsichtsinstrumente dringend geboten.

41 Hierzu ist festzustellen, dass der Grundsatz der Demokratie zur Gemeinschaftsrechtsordnung gehört und in Art. 6 Abs. 1 EU ausdrücklich als Grundlage der Europäischen Union niedergelegt ist. Als den Mitgliedstaaten gemeinsamer Grundsatz ist er daher bei der Auslegung eines sekundärrechtlichen Aktes wie Art. 28 der Richtlinie 95/46 zu berücksichtigen.

42 Dieser Grundsatz bedeutet nicht, dass es außerhalb des klassischen hierarchischen Verwaltungsaufbaus keine öffentlichen Stellen geben kann, die von der Regierung mehr oder weniger unabhängig sind. Das Bestehen und die Bedingungen für das Funktionieren solcher Stellen sind in den Mitgliedstaaten durch Gesetz und in einigen Mitgliedstaaten sogar in der Verfassung geregelt, und diese Stellen sind an das Gesetz gebunden und unterliegen der Kontrolle durch die zuständigen Gerichte. Solche unabhängigen öffentlichen Stellen, wie es sie im Übrigen auch im deutschen Rechtssystem gibt, haben häufig Regulierungsfunktion oder nehmen Aufgaben wahr, die der politischen Einflussnahme entzogen sein müssen, bleiben dabei aber an das Gesetz gebunden und der Kontrolle durch die zuständigen Gerichte unterworfen. Eben dies ist bei den Aufgaben der Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten der Fall.

43 Gewiss kommt ein Fehlen jeglichen parlamentarischen Einflusses auf diese Stellen nicht in Betracht. Die Richtlinie 95/46 schreibt jedoch den Mitgliedstaaten keineswegs vor, dem Parlament jede Einflussmöglichkeit vorzuenthalten.

44 So kann zum einen das Leitungspersonal der Kontrollstellen vom Parlament oder der Regierung bestellt werden. Zum anderen kann der Gesetzgeber die Kompetenzen der Kontrollstellen festlegen.

45 Außerdem kann der Gesetzgeber die Kontrollstellen verpflichten, dem Parlament Rechenschaft über ihre Tätigkeiten abzulegen. Insoweit lässt sich eine Parallele zu Art. 28 Abs. 5 der Richtlinie 95/46 ziehen, wonach jede Kontrollstelle regelmäßig einen Bericht über ihre Tätigkeit vorlegt, der veröffentlicht wird.

46 Nach alledem ist der Umstand, dass den Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich eine von der allgemeinen Staatsverwaltung unabhängige Stellung zukommt, für sich allein noch nicht geeignet, diesen Stellen die demokratische Legitimation zu nehmen.

47 Zweitens verpflichtet der von der Bundesrepublik Deutschland ebenfalls angeführte, in Art. 5 Abs. 1 EG verankerte Grundsatz der begrenzten Einzelermächtigung die Gemeinschaft, nur innerhalb der Grenzen der ihr im EG-Vertrag zugewiesenen Befugnisse und gesetzten Ziele tätig zu werden.

48 Die Bundesrepublik Deutschland macht insoweit geltend, die Unabhängigkeit der Kontrollstellen von den übergeordneten Verwaltungsstellen könne nicht auf der Grundlage von Art. 100a EG-Vertrag, auf den die Richtlinie 95/46 gestützt sei, verlangt werden.

49 Diese Bestimmung ermächtigt den Gemeinschaftsgesetzgeber zum Erlass von Maßnahmen zur Verbesserung der Bedingungen für die Errichtung und das Funktionieren des Binnenmarkts, wobei die entsprechenden Maßnahmen tatsächlich dieses Ziel verfolgen und dazu beitragen müssen, Hemmnisse für die mit dem EG-Vertrag garantierten wirtschaftlichen Freiheiten zu beseitigen (vgl. in diesem Sinne u. a. Urteile vom 5. Oktober 2000, Deutschland/Parlament und Rat, C‑376/98, Slg. 2000, I‑8419, Randnrn. 83, 84 und 95, vom 10. Dezember 2002, British American Tobacco [Investments] und Imperial Tobacco, C‑491/01, Slg. 2002, I‑11453, Randnr. 60, sowie vom 2. Mai 2006, Parlament/Rat, C‑436/03, Slg. 2006, I‑3733, Randnr. 38).

50 Wie bereits dargelegt, ist die Unabhängigkeit der Kontrollstellen in dem Sinne, dass sie jeglicher äußeren Einflussnahme entzogen sein müssen, die ihre Entscheidungen steuern könnte, ein im Hinblick auf die Ziele der Richtlinie 95/46 wesentliches Element. Sie ist erforderlich, um in allen Mitgliedstaaten ein gleich hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu schaffen, und trägt so zum freien Datenverkehr bei, der für die Errichtung und das Funktionieren des Binnenmarkts erforderlich ist.

51 Nach alledem geht eine weite Auslegung des Erfordernisses der Unabhängigkeit der Kontrollstellen nicht über die Grenzen der Befugnisse hinaus, die der Gemeinschaft nach Art. 100a EG-Vertrag, der die Rechtsgrundlage der Richtlinie 95/46 bildet, zugewiesen werden.

52 Drittens beruft sich die Bundesrepublik Deutschland auf die in Art. 5 Abs. 2 und 3 EG verankerten Grundsätze der Subsidiarität und der Verhältnismäßigkeit sowie auf den Grundsatz der loyalen Zusammenarbeit zwischen den Mitgliedstaaten und den Gemeinschaftsorganen nach Art. 10 EG.

53 Sie verweist insbesondere auf Nr. 7 des durch den Vertrag von Amsterdam dem EU-Vertrag und dem EG-Vertrag beigefügten Protokolls über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, wonach bewährte nationale Regelungen sowie Struktur und Funktionsweise der Rechtssysteme der Mitgliedstaaten unter Einhaltung der gemeinschaftlichen Rechtsvorschriften geachtet werden sollten.

54 Es verstoße gegen dieses Erfordernis, wenn die Bundesrepublik Deutschland gezwungen werde, ein ihrer Rechtsordnung fremdes System zu übernehmen und damit ein effektives, seit fast 30 Jahren bewährtes Kontrollsystem aufzugeben, das weit über den nationalen Bereich hinaus richtungsweisend für die Datenschutzgesetzgebung gewesen sei.

55 Diesem Vorbringen ist nicht zu folgen. Wie in den Randnrn. 21 bis 25 sowie 50 des vorliegenden Urteils ausgeführt, geht die Auslegung des Unabhängigkeitserfordernisses des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 in dem Sinne, dass dieses Erfordernis einer staatlichen Aufsicht entgegensteht, nicht über das hinaus, was zur Erreichung der Ziele des EG-Vertrags erforderlich ist.

56 In Anbetracht aller vorstehenden Erwägungen ist festzustellen, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, falsch umgesetzt hat. […]

### 7) EuGH C-203/15, C-689/15 - Home Department

*a) Sachverhalt*

Das Urteil betrifft die Auslegung von Art. 15 I der RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002 L 201, 37) in der durch die RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 (ABl. 2009 L 337, 11) geänderten Fassung (im Folgenden: RL 2002/58) im Licht der Art. 7 und 8 sowie des Art. 52 I der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta). Es ergeht im Rahmen von zwei Rechtsstreitigkeiten. In der ersten streitet die Tele2 Sverige AB (im Folgenden: Tele2 Sverige) mit der Post- och telestyrelsen (schwedische Überwachungsbehörde für Post und Telekommunikation; im Folgenden: PTS) über eine Anordnung der PTS gegenüber Tele2 Sverige zur Vorratsspeicherung von Verkehrsdaten und von Standortdaten ihrer Teilnehmer und registrierten Nutzer (Rs. C-203/15). In der zweiten Rechtssache streiten Herr Tom Watson, Herr Peter Brice und Herr Geoffrey Lewis mit dem britischen Secretary of State for the Home Department (Innenminister, Vereinigtes Königreich Großbritannien und Nordirland) über die Vereinbarkeit des Data Retention and Investigatory Powers Act 2014 (Gesetz von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen; im Folgenden: DRIPA) mit dem Unionsrecht (Rs. C-698/15). Rs. C-203/15 Am 9.4.2014 teilte Tele2 Sverige, ein in Schweden ansässiger Betreiber elektronischer Kommunikationsdienste, der PTS mit, dass sie infolge der Ungültigerklärung der RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der RL 2002/58/EG (ABl. 2006 L 105, 54; im Folgenden: RL 2006/24) durch das Urteil in der Rs. C-293/12 ua – Digital Rights Ireland ua (EuGH, ECLI:EU:C:2014:238 = NJW 2014, 2169; im Folgenden: Urteil Digital Rights) ab dem 14.4.2014 die vom schwedischen Gesetz Nr. 2003:389 über die elektronische Kommunikation (im Folgenden: LEK) erfassten elektronischen Kommunikationsdaten nicht mehr auf Vorrat speichern und die bis dahin gespeicherten Daten löschen werde. Am 15.4.2014 beschwerte sich die Rikspolisstyrels (Reichspolizeidirektion, Schweden) bei der PTS darüber, dass Tele2 Sverige ihr die betreffenden Daten nicht mehr mitteile. Am 29.4.2014 beauftragte der Justitieminister (Minister der Justiz, Schweden) einen Sondergutachter damit, die einschlägige schwedische Regelung im Hinblick auf das Urteil Digital Rights zu prüfen. In einem Bericht vom 13.6.2014 (im Folgenden: Bericht von 2014) gelangte der Sondergutachter zu dem Schluss, dass die nationale Regelung über die Vorratsdatenspeicherung in den §§ 16–16 f LEK weder gegen das Unionsrecht noch gegen die am 4.11.1950 in Rom unterzeichnete EMRK verstoße. Nach Auffassung des Sondergutachters kann das Urteil Digital Rights nicht dahin ausgelegt werden, dass es einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung grundsätzlich entgegenstehe. Aufgrund dessen teilte die PTS am 19.6.2014 Tele2 Sverige mit, dass sie gegen ihre Pflichten aus der nationalen Regelung verstoße, indem sie die unter das LEK fallenden Daten nicht für Zwecke der Kriminalitätsbekämpfung für sechs Monate auf Vorrat speichere. Mit Verfügung vom 27.6.2014 gab die PTS ihr auf, diese Daten spätestens ab dem 25.7.2014 auf Vorrat zu speichern. 718 Gegen diese Verfügung erhob Tele2 Sverige Klage beim Förvaltningsrätt i Stockholm (Verwaltungsgericht Stockholm, Schweden), die mit Urteil vom 13.10.2014 abgewiesen worden war, woraufhin Tele2 Sverige Berufung beim vorlegenden Gericht einlegte. Nach Ansicht des vorlegenden Gerichts ist die Vereinbarkeit der schwedischen Regelung mit dem Unionsrecht anhand von Art. 15 I der RL 2002/58 zu beurteilen. Dem vorlegenden Gericht stellt sich jedoch die Frage, ob eine allgemeine und unterschiedslose Pflicht zur Vorratsspeicherung elektronischer Kommunikationsdaten, wie sie im Ausgangsverfahren in Rede steht, mit Rücksicht auf das Urteil Digital Rights mit Art. 15 I der RL 2002/58, im Licht der Art. 7 und 8 sowie des Art. 52 I der Charta betrachtet, vereinbar ist. Im Hinblick auf die insoweit divergierenden Ansichten der Parteien sei es angebracht, dass der EuGH in eindeutiger Weise darüber befinde, ob – wie Tele2 Sverige meine – die allgemeine und unterschiedslose Vorratsspeicherung elektronischer Kommunikationsdaten als solche mit den Art. 7 und 8 sowie Art. 52 I der Charta unvereinbar sei oder aber ob, wie sich aus dem Bericht von 2014 ergebe, die Vereinbarkeit einer solchen Vorratsdatenspeicherung nach den Bestimmungen über den Zugang zu den Daten, über ihren Schutz, über ihre Sicherheit sowie über die Dauer ihrer Speicherung beurteilt werden müsse. Unter diesen Umständen hat der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) das Verfahren ausgesetzt und dem EuGH seine Fragen zur Vorabentscheidung vorgelegt. Rs. C-698/15 Herr Watson, Herr Brice und Herr Lewis erhoben beim High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Hoher Gerichtshof [England und Wales], Abteilung Queen's Bench, Vereinigtes Königreich) jeweils Klage auf Überprüfung der Rechtmäßigkeit von Section 1 des DRIPA und machten insbesondere geltend, dass diese Section mit den Art. 7 und 8 der Charta sowie mit Art. 8 EMRK unvereinbar sei. Mit Urteil vom 17.7.2015 stellte der High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) fest, dass das Urteil Digital Rights „verbindliche unionsrechtliche Voraussetzungen" für die Regelungen der Mitgliedstaaten über die Vorratsspeicherung von Kommunikationsdaten und den Zugang zu solchen Daten festlege. Da der EuGH in diesem Urteil angenommen habe, dass die RL 2006/24 mit dem Grundsatz der Verhältnismäßigkeit unvereinbar sei, lasse sich eine nationale Regelung gleichen Inhalts wie diese Richtlinie ebenfalls nicht mit dem Verhältnismäßigkeitsgrundsatz vereinba-

ren. Aus der dem Urteil Digital Rights zugrunde liegenden Logik ergebe sich, dass Rechtsvorschriften, mit denen eine allgemeine Regelung für die Vorratsspeicherung von Kommunikationsdaten geschaffen werde, gegen die in den Art. 7 und 8 der Charta gewährleisteten Rechte verstoße, sofern diese Rechtsvorschriften nicht durch eine im nationalen Recht festgelegte Regelung über den Zugang zu den Daten ergänzt werde, die ausreichende Garantien für die Wahrung dieser Rechte vorsehe. Section 1 des DRIPA sei folglich nicht mit den Art. 7 und 8 der Charta vereinbar, da sie keine klaren und präzisen Regeln für den Zugang zu den auf Vorrat gespeicherten Daten und über deren Nutzung aufstelle und den Zugang zu diesen Daten nicht von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig mache. Der Minister des Innern legte gegen dieses Urteil Rechtsmittel beim Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) ein. Das vorlegende Gericht ging in der Vorlageentscheidung und in seinem im Rahmen des Rechtsmittelverfahrens erlassenen Urteil vom 20.11.2015, mit dem es beschlossen hat, das vorliegende Vorabentscheidungsersuchen an den EuGH zu richten, davon aus, dass die nationalen Vorschriften über die Vorratsdatenspeicherung zwangsläufig unter Art. 15 I der RL 2002/58 fielen und daher die sich aus der Charta ergebenden Erfordernisse beachten müssten. Allerdings habe nach Art. 1 III der Richtlinie der Unionsgesetzgeber die Regeln für den Zugang zu den auf Vorrat gespeicherten Daten nicht harmonisiert. Hinsichtlich der Auswirkungen des Urteils Digital Rights auf die im Ausgangsverfahren aufgeworfenen Fragen weist das vorlegende Gericht darauf hin, dass der EuGH in der Rechtssache, die zu diesem Urteil geführt habe, mit der Gültigkeit der RL 2006/24 und nicht mit der Gültigkeit einer nationalen Regelung befasst gewesen sei. Daher hat der Court of Appeal (England & Wales) (Civil Division) das Verfahren ausgesetzt und dem EuGH seine Fragen zur Vorabentscheidung vorgelegt.
(Zusammenfassung nach NJW 2017, 717, beck-online)

*b) Leitsätze*

**1.**Art. 15 I der RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 I der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.
**2.**Art. 15 I der RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 I der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.
**3.**Die zweite Vorlagefrage des Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) ist unzulässig.
(NJW 2017, 717, beck-online)

*c) Begründung*

[…]Zur ersten Frage in der Rechtssache C‑203/15

62 Mit der ersten Frage in der Rechtssache C‑203/15 möchte der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung wie der im Ausgangsverfahren streitigen entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

63 Diese Frage geht u. a. darauf zurück, dass die Richtlinie 2006/24, die mit der im Ausgangsverfahren in Rede stehenden nationalen Regelung umgesetzt werden sollte, mit dem Urteil Digital Rights für ungültig erklärt wurde, die Parteien aber uneins sind über die Tragweite dieses Urteils und seine Auswirkungen auf die nationale Regelung, die für die Vorratsspeicherung von Verkehrs- und Standortdaten sowie für den Zugang der nationalen Behörden zu diesen Daten gilt.

64 Zunächst ist zu prüfen, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende in den Anwendungsbereich des Unionsrechts fällt.

Zum Geltungsbereich der Richtlinie 2002/58

65 Die Mitgliedstaaten, die beim Gerichtshof schriftliche Erklärungen eingereicht haben, vertreten unterschiedliche Standpunkte zu der Frage, ob und inwieweit nationale Regelungen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie den Zugang der nationalen Behörden zu diesen Daten für Zwecke der Kriminalitätsbekämpfung in den Geltungsbereich der Richtlinie 2002/58 fallen. Während namentlich die belgische, die dänische, die deutsche und die estnische Regierung, Irland und die niederländische Regierung sich dafür ausgesprochen haben, diese Frage zu bejahen, hat die tschechische Regierung vorgeschlagen, sie zu verneinen, weil alleiniger Zweck dieser Regelungen die Kriminalitätsbekämpfung sei. Die Regierung des Vereinigten Königreichs macht geltend, dass in den Geltungsbereich dieser Richtlinie nur Regelungen über die Vorratsdatenspeicherung fielen, nicht aber Regelungen über den Zugang zu den gespeicherten Daten durch die nationalen Strafverfolgungsbehörden.

66 Die Kommission schließlich hat zwar in ihren schriftlichen Erklärungen, die sie beim Gerichtshof in der Rechtssache C‑203/15 eingereicht hat, die Ansicht vertreten, dass die im Ausgangsverfahren streitige nationale Regelung in den Geltungsbereich der Richtlinie 2002/58 falle. In ihren schriftlichen Erklärungen in der Rechtssache C‑698/15 hingegen hat sie vorgetragen, dass nur nationale Vorschriften über die Vorratsspeicherung von Daten, nicht aber solche über den Zugang der nationalen Behörden zu diesen Daten in den Geltungsbereich der Richtlinie fielen. Diese letztgenannten Vorschriften müssten gleichwohl berücksichtigt werden, um zu beurteilen, ob eine nationale Regelung über die Vorratsdatenspeicherung durch Betreiber elektronischer Kommunikationsdienste einen unverhältnismäßigen Eingriff in die durch die Art. 7 und 8 der Charta gewährleisteten Grundrechte darstelle.

67 Insoweit ist darauf hinzuweisen, dass für die Bestimmung der Reichweite des Geltungsbereichs der Richtlinie 2002/58 insbesondere deren Systematik zu berücksichtigen ist.

68 Die Richtlinie 2002/58 sieht nach ihrem Art. 1 Abs. 1 u. a. die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation zu gewährleisten.

69 Art. 1 Abs. 3 dieser Richtlinie schließt von ihrem Geltungsbereich die „Tätigkeiten des Staates“ in den dort genannten Bereichen aus, d. h. namentlich die Tätigkeiten des Staates im strafrechtlichen Bereich sowie Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates, einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt (vgl. entsprechend, zu Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, Urteile vom 6. November 2003, Lindqvist, C‑101/01, EU:C:2003:596, Rn. 43, sowie vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C‑73/07, EU:C:2008:727, Rn. 41).

70 Nach Art. 3 der Richtlinie 2002/58 gilt diese für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt.

71 Nach Art. 15 Abs. 1 der Richtlinie 2002/58 können die Mitgliedstaaten unter den angegebenen Voraussetzungen „Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken“. Art. 15 Abs. 1 Satz 2 der Richtlinie nennt als Beispiel für Vorschriften, die so von den Mitgliedstaaten erlassen werden können, Vorschriften, die „vorsehen, dass Daten … aufbewahrt werden“.

72 Zwar beziehen sich die Rechtsvorschriften, um die es in Art. 15 Abs. 1 der Richtlinie 2002/58 geht, auf spezifische Tätigkeiten der Staaten oder der staatlichen Stellen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C‑275/06, EU:C:2008:54, Rn. 51). Zudem decken sich die Zweckbestimmungen, denen die Rechtsvorschriften nach dieser Bestimmung entsprechen müssen – Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit sowie Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen –, im Wesentlichen mit den Zielen, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden.

73 In Anbetracht der Systematik der Richtlinie 2002/58 erlauben jedoch die in der vorstehenden Randnummer dieses Urteils genannten Gesichtspunkte nicht den Schluss, dass die Rechtsvorschriften im Sinne des Art. 15 Abs. 1 dieser Richtlinie von deren Geltungsbereich ausgeschlossen sind, da dieser Bestimmung damit jede praktische Wirksamkeit genommen würde. Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften, wie Vorschriften über die Aufbewahrung von Daten für Zwecke der Kriminalitätsbekämpfung, in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden.

74 Außerdem regeln die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften – zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste. Demnach ist Art. 15 Abs. 1 in Verbindung mit Art. 3 der Richtlinie 2002/58 dahin auszulegen, dass diese Rechtsvorschriften in den Geltungsbereich dieser Richtlinie fallen.

75 In ihren Geltungsbereich fällt insbesondere eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten auf Vorrat zu speichern, da damit zwangsläufig eine Verarbeitung personenbezogener Daten durch die Betreiber verbunden ist.

76 Ebenfalls in ihren Geltungsbereich fällt eine Rechtsvorschrift, die, wie im Ausgangsverfahren, den Zugang der nationalen Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft.

77 Der in Art. 5 Abs. 1 der Richtlinie 2002/58 garantierte Schutz der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten gilt nämlich für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob es sich um private Personen oder Einrichtungen oder um staatliche Einrichtungen handelt. Wie ihr 21. Erwägungsgrund bestätigt, soll die Richtlinie 2002/58 jeden unerlaubten Zugang zu Nachrichten einschließlich zu „mit ihnen verbundenen Daten“ verhindern, um die Vertraulichkeit elektronischer Kommunikationen zu schützen.

78 Daher betrifft eine Rechtsvorschrift, mit der ein Mitgliedstaat den Betreibern elektronischer Kommunikationsdienste auf der Grundlage von Art. 15 Abs. 1 der Richtlinie 2002/58 zu den in dieser Bestimmung genannten Zwecken vorschreibt, den nationalen Behörden unter in der betreffenden Rechtsvorschrift vorgesehenen Voraussetzungen den Zugang zu den von ihnen gespeicherten Daten zu gewähren, die Verarbeitung personenbezogener Daten durch die Betreiber, und eine solche Verarbeitung fällt in den Geltungsbereich dieser Richtlinie.

79 Grundsätzlich setzt eine nationale Regelung über die Vorratsdatenspeicherung, da diese allein zu dem Zweck erfolgt, die Daten gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, zwangsläufig voraus, dass es Bestimmungen über den Zugang dieser Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten gibt.

80 Diese Auslegung wird durch Art. 15 Abs. 1b der Richtlinie 2002/58 gestützt, wonach die Betreiber nach den gemäß Art. 15 Abs. 1 der Richtlinie eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer einrichten.

81 Nach alledem fällt eine nationale Regelung, wie sie in den Ausgangsverfahren der Rechtssachen C‑203/15 und C‑698/15 in Rede steht, in den Geltungsbereich der Richtlinie 2002/58.

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Hinblick auf die Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta

82 Nach Art. 1 Abs. 2 der Richtlinie 2002/58 stellen ihre Bestimmungen eine „Detaillierung und Ergänzung“ der Richtlinie 95/46 dar. Wie in ihrem zweiten Erwägungsgrund zum Ausdruck gebracht wird, soll mit der Richtlinie 2002/58 gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM[2000] 385 endgültig), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber beabsichtigte, „sicher[zu]stellen, dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt“.

83 Zu diesem Zweck enthält die Richtlinie 2002/58 spezielle Vorschriften, die – wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt – die Nutzer elektronischer Kommunikationsdienste vor den sich aus den neuen Technologien und den zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung von Daten ergebenden Risiken für personenbezogene Daten und die Privatsphäre schützen sollen.

84 Insbesondere sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch ihre innerstaatlichen Vorschriften sicherzustellen haben.

85 Der mit der Richtlinie 2002/58 eingeführte Grundsatz der Vertraulichkeit von Kommunikationen bedeutet u. a., dass – wie aus Art. 5 Abs. 1 Satz 2 der Richtlinie hervorgeht – es jeder anderen Person als dem Nutzer grundsätzlich untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern. Ausgenommen sind lediglich die gemäß Art. 15 Abs. 1 dieser Richtlinie gesetzlich dazu ermächtigten Personen sowie die für die Weiterleitung einer Nachricht erforderliche technische Speicherung (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C‑275/06, EU:C:2008:54, Rn. 47).

86 Wie die Erwägungsgründe 22 und 26 der Richtlinie 2002/58 bestätigen, dürfen Verkehrsdaten nach Art. 6 der Richtlinie nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums verarbeitet und gespeichert werden (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C‑275/06, EU:C:2008:54, Rn. 47 und 48). Was speziell die Gebührenabrechnung für die Dienste betrifft, ist diese Verarbeitung nur bis zum Ende des Zeitraums zulässig, in dem die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie 2002/58 nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben.

87 Die Tragweite der Bestimmungen der Art. 5, 6 und 9 Abs. 1 der Richtlinie 2002/58, die die Vertraulichkeit von Kommunikationen und der damit verbundenen Daten gewährleisten und Missbrauchsrisiken verringern sollen, beurteilt sich außerdem unter Berücksichtigung des 30. Erwägungsgrundes der Richtlinie, wonach „[d]ie Systeme für die Bereitstellung elektronischer Kommunikationsnetze und ‑dienste … so konzipiert werden [sollten], dass so wenig personenbezogene Daten wie möglich benötigt werden“.

88 Zwar erlaubt Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten und den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten vorzusehen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C‑275/06, EU:C:2008:54, Rn. 50).

89 Gleichwohl ist Art. 15 Abs. 1 der Richtlinie 2002/58, da er den Mitgliedstaaten erlaubt, die Tragweite der grundsätzlichen Verpflichtung, die Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten zu gewährleisten, einzuschränken, nach der ständigen Rechtsprechung des Gerichtshofs eng auszulegen (vgl. entsprechend Urteil vom 22. November 2012, Probst, C‑119/12, EU:C:2012:748, Rn. 23). Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Verpflichtung und insbesondere von dem in Art. 5 der Richtlinie 2002/58 vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden.

90 Insoweit ist darauf hinzuweisen, dass Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vorsieht, dass die in dieser Bestimmung genannten Rechtsvorschriften, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichen, „die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen“ zum Ziel haben müssen oder einen der anderen Zwecke verfolgen müssen, die in Art. 13 Abs. 1 der Richtlinie 95/46, auf den Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 verweist, genannt sind (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C‑275/06, EU:C:2008:54, Rn. 53). Hierbei handelt es sich um eine abschließende Aufzählung der Zwecke, wie aus Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Art. 15 Abs. 1 Satz 1 dieser Richtlinie „aufgeführten Gründen“ gerechtfertigt sein müssen. Die Mitgliedstaaten dürfen demnach solche Vorschriften nicht zu anderen als den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen.

91 Außerdem müssen nach Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 „[a]lle in [Art. 15 Abs. 1 dieser Richtlinie] genannten Maßnahmen … den allgemeinen Grundsätzen des [Unions]rechts einschließlich den in Artikel 6 Absätze 1 und 2 [EU] niedergelegten Grundsätzen entsprechen“, zu denen die allgemeinen Grundsätze und die Grundrechte gehören, die nunmehr durch die Charta gewährleistet werden. Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit im Licht der von der Charta garantierten Grundrechte ausgelegt werden (vgl. entsprechend, zur Richtlinie 95/46, Urteile vom 20. Mai 2003, Österreichischer Rundfunk u. a., C‑465/00, C‑138/01 und C‑139/01, EU:C:2003:294, Rn. 68, vom 13. Mai 2014, Google Spain und Google, C‑131/12, EU:C:2014:317, Rn. 68, sowie vom 6. Oktober 2015, Schrems, C‑362/14, EU:C:2015:650, Rn. 38).

92 In diesem Zusammenhang ist hervorzuheben, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung, wie sie im Ausgangsverfahren in Rede steht, auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um diese gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der in den Vorlagefragen ausdrücklich erwähnten Art. 7 und 8 der Charta, sondern auch die Einhaltung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung betreffen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 25 und 70).

93 Folglich muss die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Grundrechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Grundrechts auf Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt (vgl. in diesem Sinne Urteil vom 6. Oktober 2015, Schrems, C‑362/14, EU:C:2015:650, Rn. 39 und die dort angeführte Rechtsprechung), bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 berücksichtigt werden. Das Gleiche gilt in Anbetracht der besonderen Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukommt, für das Recht auf freie Meinungsäußerung. Dieses in Art. 11 der Charta gewährleistete Grundrecht stellt eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft dar, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteile vom 12. Juni 2003, Schmidberger, C‑112/00, EU:C:2003:333, Rn. 79, und vom 6. September 2011, Patriciello, C‑163/10, EU:C:2011:543, Rn. 31).

94 Insoweit ist darauf hinzuweisen, dass nach Art. 52 Abs. 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und Wesensgehalt dieser Rechte und Freiheiten achten muss. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Urteil vom 15. Februar 2016, N., C‑601/15 PPU, EU:C:2016:84, Rn. 50).

95 Was den letztgenannten Gesichtspunkt betrifft, sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Zwecke „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist. Im elften Erwägungsgrund dieser Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss. Was speziell die Vorratsspeicherung von Daten betrifft, verlangt Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58, dass diese nur „während einer begrenzten Zeit“ und „aus den“ in Art. 15 Abs. 1 Satz 1 der Richtlinie aufgeführten Gründen erfolgen darf.

96 Dass der Grundsatz der Verhältnismäßigkeit zu beachten ist, ergibt sich ebenfalls aus der ständigen Rechtsprechung des Gerichtshofs, wonach der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (Urteile vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C‑73/07, EU:C:2008:727, Rn. 56, vom 9. November 2010, Volker und Markus Schecke und Eifert, C‑92/09 und C‑93/09, EU:C:2010:662, Rn. 77, Digital Rights, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C‑362/14, EU:C:2015:650, Rn. 92).

97 Hinsichtlich der Frage, ob eine nationale Regelung wie die in der Rechtssache C‑203/15 in Rede stehende diesen Voraussetzungen genügt, ist festzustellen, dass sie eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht und die Betreiber elektronischer Kommunikationsdienste verpflichtet, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Wie aus der Vorlageentscheidung hervorgeht, entsprechen die von dieser Regelung erfassten Datenkategorien im Wesentlichen denen, deren Vorratsspeicherung nach der Richtlinie 2006/24 vorgesehen war.

98 Die Daten, die somit von den Betreibern elektronischer Kommunikationsdienste auf Vorrat zu speichern sind, ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte. Zu diesen Daten gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand. Ferner ist ihnen zu entnehmen, wie häufig der Teilnehmer oder registrierte Benutzer in einem bestimmten Zeitraum mit bestimmten Personen kommuniziert hat (vgl. entsprechend, in Bezug auf die Richtlinie 2006/24, Urteil Digital Rights, Rn. 26).

99 Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 27). Diese Daten ermöglichen insbesondere – wie der Generalanwalt in den Nrn. 253, 254 und 257 bis 259 seiner Schlussanträge ausgeführt hat – die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

100 Der mit einer solchen Regelung verbundene Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte ist von großem Ausmaß und als besonders schwerwiegend anzusehen. Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 37).

101 Auch wenn eine solche Regelung nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubt und folglich nicht den Wesensgehalt der vorgenannten Grundrechte antastet (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 39), könnte die Vorratsspeicherung der Verkehrs- und Standortdaten jedoch Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel haben (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 28).

102 In Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 60).

103 Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 51).

104 Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

105 Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).

106 Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

107 Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

108 Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

109 Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

110 Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

111 Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

112 In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C‑203/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

Zur zweiten Frage in der Rechtssache C‑203/15 und zur ersten Frage in der Rechtssache C‑698/15

113 Vorab ist darauf hinzuweisen, dass der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) die zweite Frage in der Rechtssache C‑203/15 nur für den Fall gestellt hat, dass die erste Frage in dieser Rechtssache verneint wird. Diese zweite Frage ist jedoch unabhängig davon, ob eine Vorratsspeicherung von Daten in dem in den Rn. 108 bis 111 des vorliegenden Urteils in Betracht gezogenen Sinne allgemein oder gezielt erfolgt. Daher sind die zweite Frage in der Rechtssache C‑203/15 und die erste Frage in der Rechtssache C‑698/15, die

unabhängig vom Umfang der den Betreibern elektronischer Kommunikationsdienste auferlegten Pflicht zur Vorratsspeicherung von Daten gestellt ist, gemeinsam zu beantworten.

114 Mit der zweiten Frage in der Rechtssache C‑203/15 und der ersten Frage in der Rechtssache C‑698/15 möchten die vorlegenden Gerichte wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, zum Gegenstand hat, ohne diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne ihn einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne das Erfordernis vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

115 Hinsichtlich der Zwecke, die eine vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweichende nationale Regelung rechtfertigen können, ist darauf hinzuweisen, dass, da die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zwecke – wie in den Rn. 90 und 102 des vorliegenden Urteils festgestellt – abschließend ist, der Zugang zu den auf Vorrat gespeicherten Daten tatsächlich strikt einem dieser Zwecke dienen muss. Da außerdem der mit der Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs in die Grundrechte stehen muss, vermag folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung schwerer Straftaten einen solchen Zugang zu den auf Vorrat gespeicherten Daten zu rechtfertigen.

116 Was die Einhaltung des Grundsatzes der Verhältnismäßigkeit anbelangt, muss eine nationale Regelung über die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den auf Vorrat gespeicherten Daten zu gewähren haben, nach den in den Rn. 95 und 96 des vorliegenden Urteils getroffenen Feststellungen sicherstellen, dass ein solcher Zugang nur innerhalb der Schranken des absolut Notwendigen stattfindet.

117 Da zudem die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften nach dem elften Erwägungsgrund der Richtlinie „angemessenen Garantien … entsprechen“ müssen, muss eine solche Rechtsvorschrift – wie sich aus der in Rn. 109 des vorliegenden Urteils angeführten Rechtsprechung ergibt – klare und präzise Regeln aufstellen, in denen angegeben ist, unter welchen Umständen und unter welchen Voraussetzungen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren haben. Außerdem muss eine derartige Vorschrift im innerstaatlichen Recht verbindlich sein.

118 Es ist zwar Sache des nationalen Rechts, die Voraussetzungen festzulegen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden den Zugang zu den auf Vorrat gespeicherten Daten gewähren müssen, damit gewährleistet ist, dass dieser Zugang auf das absolut Notwendige beschränkt ist. Die betreffende nationale Regelung darf sich jedoch nicht darauf beschränken, dass der Zugang einem der in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Zwecke zu entsprechen hat, auch wenn es sich dabei um die Bekämpfung schwerer Straftaten handelt. Denn eine solche nationale Regelung muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten festlegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 61).

119 Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten unabhängig davon, ob irgendein – zumindest mittelbarer – Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich die betreffende nationale Regelung bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten von Teilnehmern oder registrierten Nutzern zu gewähren ist, auf objektive Kriterien stützen. Insoweit darf im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein (vgl. entsprechend Urteil des Europäischen Gerichtshofs für Menschenrechte vom 4. Dezember 2015, Zakharov/Russland, CE:ECHR:2015:1204JUD004714306, Rn. 260). Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.

120 Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich

– außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 62; vgl. auch entsprechend, zu Art. 8 EMRK, Urteil des Europäischen Gerichtshofs für Menschenrechte vom 12. Januar 2016, Szabó und Vissy/Ungarn CE:ECHR:2016:0112JUD003713814, Rn. 77 und 80).

121 Außerdem ist es wichtig, dass die zuständigen nationalen Behörden, denen Zugang zu den auf Vorrat gespeicherten Daten gewährt worden ist, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzen, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann. Diese Information ist nämlich der Sache nach erforderlich, damit die betroffenen Personen u. a. das Recht auf Einlegung eines Rechtsbehelfs ausüben können, das in Art. 15 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 22 der Richtlinie 95/46 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist (vgl. entsprechend Urteile vom 7. Mai 2009, Rijkeboer, C‑553/07, EU:C:2009:293, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C‑362/14, EU:C:2015:650, Rn. 95).

122 Bezüglich der Vorschriften zur Sicherheit und zum Schutz der von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten ist festzustellen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten nicht erlaubt, von Art. 4 Abs. 1 und Art. 4 Abs. 1a der Richtlinie abzuweichen. Nach diesen Bestimmungen haben die Betreiber geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang geschützt sind. Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 66 bis 68).

123 Jedenfalls müssen die Mitgliedstaaten gewährleisten, dass die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle überwacht wird, da eine solche Überwachung in Art. 8 Abs. 3 der Charta ausdrücklich gefordert wird und nach ständiger Rechtsprechung des Gerichtshofs ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten ist. Anderenfalls würde den Personen, deren personenbezogene Daten gespeichert wurden, das durch Art. 8 Abs. 1 und 3 der Charta garantierte Recht vorenthalten, sich zum Schutz ihrer Daten mit einer Eingabe an die nationalen Kontrollstellen zu wenden (vgl. in diesem Sinne Urteile Digital Rights, Rn. 68, und vom 6. Oktober 2015, Schrems, C‑362/14, EU:C:2015:650, Rn. 41 und 58).

124 Es ist Sache der vorlegenden Gerichte, zu prüfen, ob und inwieweit die in den Ausgangsverfahren in Rede stehenden nationalen Regelungen die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta ergebenden Erfordernisse beachten, wie sie in den Rn. 115 bis 123 des vorliegenden Urteils ausdrücklich benannt sind, sowohl was den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten als auch was den Schutz dieser Daten und das Sicherheitsniveau betrifft.

125 Aufgrund all dessen ist auf die zweite Frage in der Rechtssache C‑203/15 und die erste Frage in der Rechtssache C‑698/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

Zur zweiten Frage in der Rechtssache C‑698/15

126 Mit der zweiten Frage in der Rechtssache C‑698/15 möchte der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen]) wissen, ob der Gerichtshof im

Urteil Digital Rights die Art. 7 und 8 der Charta in einem Sinne ausgelegt hat, der über den hinausgeht, der Art. 8 EMRK vom Europäischen Gerichtshof für Menschenrechte gegeben wurde.

127 Zunächst ist darauf hinzuweisen, dass die in der EMRK anerkannten Grundrechte zwar, wie Art. 6 Abs. 3 EUV bestätigt, als allgemeine Grundsätze Teil des Unionsrechts sind, die EMRK jedoch, solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument darstellt, das förmlich in die Unionsrechtsordnung übernommen wurde (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C‑601/15 PPU, EU:C:2016:84, Rn. 45 und die dort angeführte Rechtsprechung).

128 Daher ist die Richtlinie 2002/58, um die es vorliegend geht, einzig und allein anhand der durch die Charta garantierten Grundrechte auszulegen (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C‑601/15 PPU, EU:C:2016:84, Rn. 46 und die dort angeführte Rechtsprechung).

129 Außerdem heißt es in den Erläuterungen zu Art. 52 der Charta, dass mit ihrem Art. 52 Abs. 3 die notwendige Kohärenz zwischen der Charta und der EMRK geschaffen werden soll, „ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird“ (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C‑601/15 PPU, EU:C:2016:84, Rn. 47). Insbesondere steht, wie aus Art. 52 Abs. 3 Satz 2 der Charta hervorgeht, Art. 52 Abs. 3 Satz 1 der Charta dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK. Zudem betrifft Art. 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht, für das es in der EMRK keine Entsprechung gibt.

130 Nach ständiger Rechtsprechung des Gerichtshofs liegt die Rechtfertigung für ein Vorabentscheidungsersuchen jedoch nicht in der Abgabe von Gutachten zu allgemeinen oder hypothetischen Fragen, sondern darin, dass das Ersuchen für die tatsächliche Entscheidung eines Rechtsstreits über das Unionsrecht erforderlich ist (vgl. in diesem Sinne Urteile vom 24. April 2012, Kamberaj, C‑571/10, EU:C:2012:233, Rn. 41, vom 26. Februar 2013, Åkerberg Fransson, C‑617/10, EU:C:2013:105, Rn. 42, sowie vom 27. Februar 2014, Pohotovosť, C‑470/12, EU:C:2014:101, Rn. 29).

131 Im vorliegenden Fall ist in Anbetracht der insbesondere in den Rn. 128 und 129 des vorliegenden Urteils enthaltenen Erwägungen die Frage, ob der in den Art. 7 und 8 der Charta verliehene Schutz über den in Art. 8 EMRK garantierten hinausgeht, nicht geeignet, die Auslegung der Richtlinie 2002/58 im Licht der Charta, um die es in der Rechtssache C‑698/15 im Ausgangsverfahren geht, zu beeinflussen.

132 Es ist somit nicht ersichtlich, dass die Antwort auf die zweite Frage in der Rechtssache C‑698/15 Hinweise zur Auslegung des Unionsrechts liefern könnte, die für die Entscheidung des betreffenden Rechtsstreits im Hinblick auf das Unionsrecht erforderlich sind.

133 Folglich ist die zweite Frage in der Rechtssache C‑698/15 unzulässig. […]

**8) EuGH Gutachten 1/15**

*I. Gutachtenantrag*

1 Der Gutachtenantrag, den das Europäische Parlament beim Gerichtshof gestellt hat, lautet:
„Ist das geplante Abkommen [zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen] mit den Bestimmungen der Verträge (Artikel 16 AEUV) und der Charta der Grundrechte der Europäischen Union (Artikel 7, Artikel 8 und Artikel 52 Absatz 1) in Bezug auf das Recht natürlicher Personen auf den Schutz personenbezogener Daten vereinbar?
Sind Artikel 82 Absatz 1 [Unterabsatz 2] Buchstabe d und Artikel 87 Absatz 2 Buchstabe a AEUV die geeignete Rechtsgrundlage für den Rechtsakt des Rates [der Europäischen Union] über den Abschluss des geplanten Abkommens, oder muss sich dieser Rechtsakt auf Artikel 16 AEUV gründen?“
2 Als Anlagen zu seinem Gutachtenantrag hat das Parlament beim Gerichtshof u. a. folgende Dokumente eingereicht:
– den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (im Folgenden: geplantes Abkommen),
– den Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen im Namen der Union (im Folgenden: Entwurf eines Beschlusses des Rates über den Abschluss des geplanten Abkommens) und
– das Schreiben vom 7. Juli 2014, mit dem der Rat das Parlament um Zustimmung zu dem Entwurf des Beschlusses ersucht hat.

*II. Rechtlicher Rahmen*

A. Abkommen von Chicago

3 Das am 7. Dezember 1944 in Chicago unterzeichnete Abkommen über die Internationale Zivilluftfahrt (*United Nations Treaty Series*, Band 15, Nr. 102, im Folgenden: Abkommen von Chicago) ist von Kanada und sämtlichen Mitgliedstaaten der Europäischen Union ratifiziert worden. Die Europäische Union selbst ist allerdings nicht Vertragsstaat des Abkommens.

4 Art. 13 des Abkommens von Chicago lautet:

„Die Gesetze und Vorschriften eines Vertragsstaats über den Ein- und Ausflug von Fluggästen, Besatzungen oder Fracht eines Luftfahrzeugs nach oder aus seinem Hoheitsgebiet, wie z. B. Einreise-, Abfertigungs-, Einwanderungs-, Pass-, Zoll- und Quarantänevorschriften, sind durch oder in Bezug auf die Fluggäste, Besatzungen oder Fracht bei dem Ein- und Ausflug sowie während des Aufenthalts im Hoheitsgebiet dieses Staates zu befolgen."

5 Durch das Abkommen von Chicago wurde die Internationale Zivilluftfahrt-Organisation (ICAO) geschaffen. Eine ihrer Aufgaben ist nach Art. 44 des Abkommens die Entwicklung der Grundsätze und der Technik der internationalen Luftfahrt.

B. Protokoll (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts

6 Art. 1 des Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts (ABl. 2010, C 83, S. 295, im Folgenden: Protokoll Nr. 21) bestimmt:

„Vorbehaltlich des Artikels 3 beteiligen sich das Vereinigte Königreich und Irland nicht an der Annahme von Maßnahmen durch den Rat, die nach dem Dritten Teil Titel V des Vertrags über die Arbeitsweise der Europäischen Union vorgeschlagen werden. Für Beschlüsse des Rates, die einstimmig angenommen werden müssen, ist die Zustimmung der Mitglieder des Rates mit Ausnahme der Vertreter der Regierungen des Vereinigten Königreichs und Irlands erforderlich.

…"

7 Art. 3 Abs. 1 des Protokolls lautet:

„Das Vereinigte Königreich oder Irland kann dem Präsidenten des Rates innerhalb von drei Monaten nach der Vorlage eines Vorschlags oder einer Initiative nach dem Dritten Teil Titel V des Vertrags über die Arbeitsweise der Europäischen Union beim Rat schriftlich mitteilen, dass es sich an der Annahme und Anwendung der betreffenden Maßnahme beteiligen möchte, was dem betreffenden Staat daraufhin gestattet ist."

C. Protokoll (Nr. 22) über die Position Dänemarks

8 In den Abs. 3 bis 5 der Präambel des Protokolls (Nr. 22) über die Position Dänemarks (ABl. 2010, C 83, S. 299, im Folgenden: Protokoll Nr. 22) heißt es, dass die Hohen Vertragsparteien über die Bestimmungen des Protokolls übereingekommen sind

„IN DEM BEWUSSTSEIN, dass Dänemarks Beteiligung an wichtigen Bereichen der Zusammenarbeit in der Union erheblich eingeschränkt wird, wenn die auf den Beschluss von Edinburgh zurückgehende Rechtsregelung im Rahmen der Verträge fortgesetzt wird, und dass es im Interesse der Union liegt, die uneingeschränkte Anwendung des Besitzstands im Raum der Freiheit, der Sicherheit und des Rechts zu gewährleisten,

IN DEM WUNSCH, aufgrund dessen einen Rechtsrahmen festzulegen, der Dänemark die Option bieten wird, sich am Erlass von Maßnahmen zu beteiligen, die auf der Grundlage des Dritten Teils Titel V des Vertrags über die Arbeitsweise der Europäischen Union vorgeschlagen werden, und die Absicht Dänemarks begrüßend, wenn möglich von dieser Option im Einklang mit seinen verfassungsrechtlichen Vorschriften Gebrauch zu machen,

IN ANBETRACHT DESSEN, dass Dänemark die anderen Mitgliedstaaten nicht daran hindern wird, ihre Zusammenarbeit in Bezug auf Maßnahmen, die für Dänemark nicht bindend sind, weiter auszubauen".

9 Art. 1 des Protokolls lautet:

„Dänemark beteiligt sich nicht an der Annahme von Maßnahmen durch den Rat, die nach dem Dritten Teil Titel V des Vertrags über die Arbeitsweise der Europäischen Union vorgeschlagen werden. Für Beschlüsse des Rates, die einstimmig angenommen werden müssen, ist die Zustimmung der Mitglieder des Rates mit Ausnahme des Vertreters der Regierung Dänemarks erforderlich.

Für die Zwecke dieses Artikels bestimmt sich die qualifizierte Mehrheit nach Artikel 238 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union."

10 Art. 2 des Protokolls lautet:

„Vorschriften des Dritten Teils Titel V des Vertrags über die Arbeitsweise der Europäischen Union, nach jenem Titel beschlossene Maßnahmen, Vorschriften internationaler Übereinkünfte, die von der Union nach jenem Titel geschlossen werden, sowie Entscheidungen des Gerichtshofs der Europäischen Union, in denen solche Vorschriften oder Maßnahmen oder nach jenem Titel geänderte oder änderbare Maßnahmen ausgelegt werden, sind für Dänemark nicht bindend oder anwendbar. Diese Vorschriften, Maßnahmen oder Entscheidungen berühren in keiner Weise die Zuständigkeiten, Rechte und Pflichten Dänemarks; ebenso wenig berühren diese Vorschriften, Maßnahmen oder Entscheidungen in irgendeiner Weise den Besitzstand der Gemeinschaft oder der Union oder sind sie Teil des Unionsrechts, soweit sie auf Dänemark Anwendung finden. Insbesondere sind Rechtsakte der

Union auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, die vor dem Inkrafttreten des Vertrags von Lissabon angenommen wurden und die geändert werden, für Dänemark ohne die Änderungen weiterhin bindend und anwendbar."

11 Art. 2a des Protokolls lautet:

„Artikel 2 dieses Protokolls gilt auch für die auf der Grundlage des Artikels 16 des Vertrags über die Arbeitsweise der Europäischen Union festgelegten Vorschriften über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 des genannten Vertrags fallen."

D. Richtlinie 95/46/EG

12 Art. 25 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31) bestimmt:

„(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

…

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

…"

E. Richtlinie 2004/82/EG

13 Art. 3 Abs. 1 und 2 der Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (ABl. 2004, L 261, S. 24), lautet:

„(1) Die Mitgliedstaaten unternehmen die erforderlichen Schritte, um die Beförderungsunternehmen zu verpflichten, auf Anfrage der mit der Durchführung der Personenkontrollen an den Außengrenzen beauftragten Behörden bei Abschluss des Check-in die Angaben über die Personen zu übermitteln, die sie zu einer zugelassenen Grenzübergangsstelle befördern werden, über die diese Personen in das Hoheitsgebiet eines Mitgliedstaats einreisen werden.

(2) Zu diesen Angaben zählen:

– die Nummer und die Art des mitgeführten Reisedokuments,
– die Staatsangehörigkeit,
– der vollständige Name,
– das Geburtsdatum,
– die Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten,
– die Beförderungs-Codenummer,
– die Abreise- und Ankunftszeit,
– die Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,
– der ursprüngliche Abreiseort."

*III. Vorgeschichte des geplanten Abkommens*

14 Am 18. Juli 2005 erließ der Rat den Beschluss 2006/230/EG über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und der Regierung Kanadas über die Verarbeitung von API/PNR-Daten (ABl. 2006, L 82, S. 14), mit dem er dieses Abkommen (im Folgenden: Abkommen von 2006) genehmigte. Nach seiner Präambel wurde das Abkommen geschlossen „gestützt auf die von der Regierung Kanadas erlassene Vorschrift, nach der die Fluggesellschaften, die Personen nach Kanada befördern, zur Übermittlung von erweiterten Fluggastdaten (Advanced Passenger Information) und Fluggastdatensätzen (Passenger Name Records) (im Folgenden ‚API/PNR-Daten' genannt) an die zuständigen kanadischen Behörden verpflichtet sind, soweit diese Fluggesellschaften solche Daten erfassen und in computergestützten Buchungs- sowie Abfertigungssystemen speichern".

15 Nach Art. 1 Abs. 1 des Abkommens von 2006 „wird gewährleistet, dass die Weitergabe von API/PNR-Daten zu Personen auf abkommensrelevanten Flügen unter uneingeschränkter Achtung grundlegender Rechte

und Freiheiten, insbesondere des Rechts auf Privatsphäre, erfolgt“. In Art. 3 Abs. 1 sind die Vertragsparteien übereingekommen, „dass die API/PNR-Daten zu Personen auf abkommensrelevanten Flügen im Einklang mit den Verpflichtungen der zuständigen Behörde verarbeitet werden, die die API/PNR-Daten erhält“. Zuständige Behörde Kanadas war nach Anhang I des Abkommens die Canada Border Services Agency (CBSA).

16 Auf der Grundlage dieser Verpflichtungen erließ die Kommission der Europäischen Gemeinschaften am 6. September 2005 die Entscheidung 2006/253/EG über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche der Canada Border Services Agency übermittelt werden (ABl. 2006, L 91, S. 49). In Art. 1 dieser Entscheidung wurde „[i]m Hinblick auf Artikel 25 Absatz 2 der Richtlinie [95/46] … festgestellt, dass die [CBSA] auf der Grundlage der als Anhang [der Entscheidung] angefügten Verpflichtungserklärung [der CBSA zu ihrem PNR-Programm] einen angemessenen Schutz bietet für PNR-Daten über Flüge nach Kanada, die aus der Gemeinschaft übermittelt werden“. Art. 7 der Entscheidung sah vor, dass ihre Geltungsdauer „3 Jahre und 6 Monate nach dem Tag ihrer Bekanntmachung [endet], es sei denn, sie wird nach dem Verfahren des Artikels 31 Absatz 2 der Richtlinie [95/46] verlängert“. Eine solche Verlängerung ist nicht erfolgt.

17 Die Geltungsdauer des Abkommens von 2006 war nach dessen Art. 5 Abs. 1 und 2 an die der Entscheidung 2006/253 geknüpft, so dass sie im September 2009 endete.

18 Am 5. Mai 2010 nahm das Parlament eine Entschließung zum Start der Verhandlungen über Abkommen über Fluggastdatensätze mit den USA, Australien und Kanada (ABl. 2011, C 81 E, S. 70) an. In Rn. 7 der Entschließung forderte es „einen kohärenten Ansatz in Bezug auf die Nutzung von Fluggastdatensätzen für Strafverfolgungs- und Sicherheitszwecke, wobei Abkommen mit Drittstaaten auf einheitlichen Grundsätzen beruhen sollten“, und forderte „die Kommission auf, … einen Vorschlag für ein solches einheitliches Modell und ein[en] Entwurf für ein Mandat für die Verhandlungen mit Drittstaaten vorzulegen“. In Rn. 9 der Entschließung werden die Mindestanforderungen für die Verwendung von Fluggastdatensätzen in Drittstaaten genannt.

19 Am 2. Dezember 2010 erließ der Rat einen Beschluss mit einer Verhandlungsrichtlinie; darin wurde die Kommission ermächtigt, im Namen der Union Verhandlungen mit Kanada über ein Abkommen über die Übermittlung und Verwendung von Fluggastdatensätzen (im Folgenden: PNR-Daten) zu Zwecken der Verhütung und Bekämpfung von Terrorismus und anderer grenzübergreifender schwerer Kriminalität aufzunehmen.

20 Nach Abschluss der Verhandlungen mit Kanada wurde das geplante Abkommen am 6. Mai 2013 paraphiert. Am 18. Juli 2013 nahm die Kommission einen Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (COM[2013] 528 final, im Folgenden: Vorschlag für einen Beschluss des Rates über den Abschluss des geplanten Abkommens) und einen Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (COM[2013] 529 final) an.

21 In der Begründung des Vorschlags für einen Beschluss des Rates über den Abschluss des geplanten Abkommens heißt es:

„Die [CBSA] ist nach kanadischem Recht ermächtigt, bei Verkehrsflügen nach oder aus Kanada vor Ankunft der Fluggäste bzw. vor ihrem Abflug von Fluggesellschaften elektronischen Zugang zu den Fluggastdatensätzen (Passenger Name Records – PNR) zu verlangen. Dabei stützen sich die kanadischen Behörden auf Section 107.1 des Customs Act, die Passenger Information (Customs) Regulations, Paragraph 148(1)(d) des Immigration and Refugee Protection Act und Regulation 269 der Immigration and Refugee Protection Regulations.

Diese Rechtsvorschriften sollen vor der Ankunft eines Flugs den elektronischen Zugriff auf PNR-Daten ermöglichen und es somit der [CBSA] erheblich erleichtern, die Fluggäste vor ihrer Ankunft einer effizienten und wirksamen Risikobewertung zu unterziehen und Bona-fide-Reisenden Erleichterungen zu gewähren, um für mehr Sicherheit in Kanada zu sorgen. Die Europäische Union arbeitet mit Kanada bei der Bekämpfung von Terrorismus und anderer grenzübergreifender schwerer Kriminalität zusammen und betrachtet die Übermittlung von PNR-Daten an Kanada als Beitrag zur Förderung der polizeilichen und justiziellen Zusammenarbeit auf internationaler Ebene. Hierzu sollen analytische Informationen, die von Kanada erlangte PNR-Daten enthalten, mit den zuständigen Polizei- und Justizbehörden der Mitgliedstaaten sowie mit Europol und Eurojust im Rahmen ihres jeweiligen Mandats ausgetauscht werden.

…

Die Fluggesellschaften sind verpflichtet, der [CBSA] Zugriff auf bestimmte PNR-Daten zu gewähren, die mit den computergestützten Buchungs- und Abfertigungssystemen der Fluggesellschaften erhoben und darin gespeichert werden.

Nach den EU-Datenschutzbestimmungen ist es europäischen und anderen Fluggesellschaften, die Ziele außerhalb der [Union] anfliegen, untersagt, PNR-Daten an Drittländer zu übermitteln, die keinen angemessenen Schutz personenbezogener Daten bieten, weil sie keine geeigneten Schutzvorkehrungen treffen. Angesichts der Notwendigkeit und Bedeutung der Verwendung von PNR-Daten bei der Bekämpfung von Terrorismus und anderer grenzübergreifender schwerer Kriminalität muss eine Lösung gefunden werden, die eine Rechtsgrundlage für die Übermittlung von PNR-Daten aus der EU an Kanada bietet und gleichzeitig den Fluggesellschaften Rechtssicherheit gibt. Außerdem sollte diese Lösung in der gesamten Europäischen Union einheitlich angewandt

werden, um Rechtssicherheit für Fluggesellschaften zu schaffen und das Recht des Einzelnen auf Schutz seiner Daten sowie auf physische Sicherheit zu gewährleisten.
…“

22 Am 30. September 2013 nahm der Europäische Datenschutzbeauftragte (EDSB) zu diesen Vorschlägen für Beschlüsse Stellung. Der vollständige Text der Stellungnahme ist auf der Website des EDSB abrufbar. Eine Zusammenfassung wurde im *Amtsblatt der Europäischen Union* (ABl. 2014, C 51, S. 12) veröffentlicht.

23 Am 5. Dezember 2013 erließ der Rat den Beschluss über die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen. Am selben Tag entschied er, zu seinem Entwurf des Beschlusses über den Abschluss des geplanten Abkommens die Zustimmung des Parlaments einzuholen.

24 Das geplante Abkommen wurde am 25. Juni 2014 unterzeichnet.

25 Mit Schreiben vom 7. Juli 2014 ersuchte der Rat das Parlament darum, dem Entwurf seines Beschlusses über den Abschluss des geplanten Abkommens zuzustimmen.

26 Am 25. November 2014 nahm das Parlament die Entschließung zur Einholung eines Gutachtens des Gerichtshofs über die Vereinbarkeit des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen mit den Verträgen (ABl. 2016, C 289, S. 2) an.

### *IV. Entwurf eines Beschlusses des Rates über den Abschluss des geplanten Abkommens*

27 Im Entwurf eines Beschlusses des Rates über den Abschluss des geplanten Abkommens sind als Rechtsgrundlagen des Beschlusses Art. 82 Abs. 1 Unterabs. 2 Buchst. d und Art. 87 Abs. 2 Buchst. a in Verbindung mit Art. 218 Abs. 6 Buchst. a AEUV angegeben.

28 In den Erwägungsgründen 5 und 6 des Entwurfs heißt es:

„(5) Gemäß Artikel 3 des … Protokolls [(Nr. 21)] … haben [das Vereinigte Königreich und Irland] mitgeteilt, dass sie sich an der Annahme dieses Beschlusses beteiligen möchten.

(6) Gemäß den Artikeln 1 und 2 des … Protokolls [(Nr. 22)] … beteiligt sich Dänemark nicht an der Annahme dieses Beschlusses und ist weder durch diesen Beschluss gebunden noch zu seiner Anwendung verpflichtet.“

29 Art. 1 des Entwurfs lautet:

„Das Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen wird im Namen der Union genehmigt.

Der Wortlaut des Abkommens ist diesem Beschluss beigefügt.“

### *V. Das geplante Abkommen*

30 Das geplante Abkommen lautet:

„KANADA

und

DIE EUROPÄISCHE UNION,

im Folgenden die ‚Parteien‘ genannt

IN DEM BEMÜHEN, zum Schutz ihrer demokratischen Gesellschaften und gemeinsamen Werte mit Blick auf die Förderung der Sicherheit und der Rechtsstaatlichkeit Terrorismus und Straftaten mit terroristischem Hintergrund sowie andere grenzübergreifende schwere Kriminalität zu verhindern, zu bekämpfen, zu unterbinden und zu beseitigen,

IN ANERKENNUNG der Bedeutung der Verhinderung, Bekämpfung, Unterbindung und Beseitigung von Terrorismus und Straftaten mit terroristischem Hintergrund sowie anderer grenzübergreifender schwerer Kriminalität bei gleichzeitiger Wahrung der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Schutz der Privatsphäre und des Rechts auf Datenschutz,

IN DEM BEMÜHEN, die Zusammenarbeit zwischen den Parteien im Geiste der Partnerschaft zwischen Kanada und der Europäischen Union auszubauen und weiter voranzubringen,

IN DEM BEWUSSTSEIN, dass der Austausch von Informationen ein wesentlicher Faktor bei der Bekämpfung von Terrorismus und damit verknüpften Straftaten sowie anderer grenzübergreifender schwerer Kriminalität ist und dass die Verwendung von Fluggastdatensätzen (Passenger Name Record, im Folgenden ‚PNR-Daten‘) in diesem Zusammenhang von maßgeblicher Bedeutung für die Verfolgung der genannten Ziele ist,

IN DEM BEWUSSTSEIN, dass zur Gewährleistung der öffentlichen Sicherheit und zu Strafverfolgungszwecken Regeln für die Übermittlung von PNR-Daten durch die Fluggesellschaften an Kanada festgelegt werden sollten,

IN ANERKENNUNG DESSEN, dass die Parteien durch gemeinsame Werte in Bezug auf Datenschutz und Schutz der Privatsphäre verbunden sind, die sich in ihrem jeweiligen Recht widerspiegeln,

EINGEDENK des Artikels 6 des Vertrags über die Europäische Union, in dem sich die Europäische Union zur Achtung der Grundrechte verpflichtet, des Artikels 16 des Vertrags über die Arbeitsweise der Europäischen Union über das Recht auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, der Grundsätze der Verhältnismäßigkeit und der Notwendigkeit hinsichtlich des Rechts auf Achtung des Privat- und Famili-

enlebens, der Achtung der Privatsphäre und des Schutzes personenbezogener Daten gemäß Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union, Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108 des Europarats [unterzeichnet in Straßburg am 28. Januar 1981] und Zusatzprotokoll Nr. 181 [unterzeichnet in Straßburg am 8. November 2001]),
UNTER BERÜCKSICHTIGUNG der einschlägigen Bestimmungen der Canadian Charter of Rights and Freedoms (Kanadische Charta der Rechte und Freiheiten) und der kanadischen Rechtsvorschriften zum Schutz der Privatsphäre,
IN ANBETRACHT der Zusage der Europäischen Union, dafür Sorge zu tragen, dass die Fluggesellschaften nicht daran gehindert werden, bei der Übermittlung von PNR-Daten aus der Europäischen Union an Kanada gemäß diesem Abkommen dem kanadischen Recht zu entsprechen,
IN BESTÄTIGUNG der erfolgreichen gemeinsamen Überprüfung des Abkommens zwischen den Parteien von 2006 über die Übermittlung von PNR-Daten im Jahr 2008,
IN ANERKENNUNG DESSEN, dass dieses Abkommen nicht für erweiterte Fluggastdaten (Advance Passenger Information) gelten soll, die zum Zweck der Grenzkontrolle von den Fluggesellschaften erhoben und an Kanada übermittelt werden,
IN ANERKENNUNG DESSEN, dass dieses Abkommen Kanada nicht daran hindert, in Ausnahmefällen weiterhin Informationen von Fluggesellschaften zu verarbeiten, wenn dies zur Eindämmung einer unmittelbaren und ernsten Gefahr für den Luftverkehr oder die nationale Sicherheit unter Beachtung der im kanadischen Recht festgelegten strengen Beschränkungen und in jedem Fall ohne Überschreitung der in diesem Abkommen vorgesehenen Beschränkungen notwendig ist,
ANGESICHTS des Interesses der Parteien und der Mitgliedstaaten der Europäischen Union an einem Austausch von Informationen über das Verfahren der Übermittlung von PNR-Daten sowie über die Weitergabe von PNR-Daten außerhalb Kanadas gemäß den einschlägigen Artikeln dieses Abkommens sowie angesichts des Interesses der Europäischen Union an der Einbeziehung dieses Aspekts in das in diesem Abkommen vorgesehene Konsultations- und Überprüfungsverfahren,
UNTER HINWEIS DARAUF, dass die Parteien die Möglichkeit und Notwendigkeit eines ähnlichen Abkommens für die Verarbeitung von PNR-Daten im Seeverkehr prüfen können,
UNTER HINWEIS AUF die Verpflichtung Kanadas sicherzustellen, dass die zuständige kanadische Behörde PNR-Daten zum Zweck der Verhinderung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität unter strikter Einhaltung der in dem Abkommen enthaltenen Garantien für den Schutz der Privatsphäre und den Schutz personenbezogener Daten verarbeitet,
IN ANBETRACHT der Bedeutung, die dem Austausch von PNR-Daten und einschlägigen analytischen Informationen, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, zwischen Kanada und den zuständigen Polizei- und Justizbehörden der Mitgliedstaaten der Europäischen Union, Europol und Eurojust als Mittel zur Stärkung der internationalen polizeilichen und justiziellen Zusammenarbeit zukommt,
UNTER BEKRÄFTIGUNG, dass dieses Abkommen keinen Präzedenzfall für weitere Vereinbarungen zwischen Kanada und der Europäischen Union oder zwischen einer der Parteien und einer anderen Partei über die Verarbeitung und Übermittlung von PNR-Daten oder über den Datenschutz darstellt,
UNTER BERÜCKSICHTIGUNG der beiderseitigen Verpflichtung der Parteien zur Anwendung und Weiterentwicklung internationaler Normen für die Verarbeitung von PNR-Daten –
SIND WIE FOLGT ÜBEREINGEKOMMEN:

ALLGEMEINE BESTIMMUNGEN

ARTIKEL 1

Gegenstand des Abkommens

In diesem Abkommen legen die Parteien fest, unter welchen Bedingungen Fluggastdatensätze (PNR-Daten) zur Gewährleistung der öffentlichen Sicherheit zu übermitteln und zu verwenden [sind] und wie sie geschützt werden.

ARTIKEL 2

Begriffsbestimmungen

Für die Zwecke dieses Abkommens bezeichnet der Begriff:

a) ‚Fluggesellschaft' ein kommerzielles Transportunternehmen, das Luftfahrzeuge zur Beförderung von Fluggästen zwischen Kanada und der Europäischen Union einsetzt;

b) ‚Fluggastdatensätze' (‚PNR-Daten') die Datensätze, die für jeden von einem oder für einen Fluggast gebuchten Flug von einer Fluggesellschaft erfasst werden und für die Verarbeitung und Überprüfung der Buchungen erforderlich sind. PNR-Daten im Sinne dieses Abkommens sind die im Anhang des Abkommens aufgeführten Elemente;

c) ‚Verarbeitung' jeden mit oder ohne automatisierte Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit PNR-Daten wie das Erheben, das Erfassen, die Organisation, die Aufbewahrung, die Anpassung oder Änderung, das Aufrufen, das Auslesen, das Abfragen, die Verwendung, den Transfer, die

Verbreitung, die Weitergabe oder jede andere Form der Bereitstellung, die Verknüpfung oder Kombination sowie das Sperren, Unkenntlichmachen, Löschen oder Vernichten;

d) ‚zuständige kanadische Behörde' die für den Erhalt und die Verarbeitung von PNR-Daten im Rahmen dieses Abkommens verantwortliche kanadische Behörde;

e) ‚sensible Daten' jegliche Informationen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Informationen über Gesundheit oder Sexualleben einer Person.

ARTIKEL 3

Verwendung von PNR-Daten

(1) Kanada stellt sicher, dass die zuständige kanadische Behörde die auf der Grundlage dieses Abkommens erhaltenen PNR-Daten nur zum Zweck der Verhinderung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität verarbeitet.

(2) Für die Zwecke dieses Abkommens umfasst der Begriff ‚terroristische Straftat':

a) eine politischen, religiösen oder ideologischen Zwecken oder Zielen dienende oder politisch, religiös oder ideologisch begründete Handlung oder Unterlassung, mit der beabsichtigt wird, die Allgemeinheit hinsichtlich ihrer Sicherheit, einschließlich ihrer wirtschaftlichen Sicherheit, einzuschüchtern oder eine Person, eine Regierung oder eine inländische oder internationale Organisation zu einer Handlung oder Unterlassung zu zwingen, und mit der vorsätzlich

i) der Tod oder eine schwere Körperverletzung verursacht wird,

ii) das Leben einer Einzelperson gefährdet wird,

iii) die Gesundheit oder Sicherheit der Allgemeinheit erheblich gefährdet wird,

iv) beträchtliche Sachschäden verursacht werden, die wahrscheinlich zu den unter den Ziffern i bis iii genannten Schäden führen, oder

v) eine schwerwiegende Beeinträchtigung oder Störung eines Dienstes, einer Einrichtung oder eines Systems von maßgeblicher Bedeutung verursacht wird, die nicht infolge einer legalen oder illegalen Interessenvertretung, Protestkundgebung, Arbeitsverweigerung oder -niederlegung wie Streik eintritt, mit der keiner der unter den Ziffern i bis iii genannten Schäden beabsichtigt wird, oder

b) Handlungen, die in anwendbaren internationalen Übereinkünften und Protokollen zur Terrorismusbekämpfung als Straftat gelten und als solche definiert sind, oder

c) die wissentliche Beteiligung oder Mitwirkung an einer Maßnahme zur Stärkung der Fähigkeit einer terroristischen Einheit, eine unter den Buchstaben a oder b genannte Handlung oder Unterlassung zu erleichtern oder durchzuführen, oder die Anweisung einer Person, Gruppe oder Organisation zur Durchführung einer solchen Maßnahme oder

d) die Begehung einer strafbaren Handlung, wobei die die Straftat darstellende Handlung oder Unterlassung zugunsten, unter der Leitung oder in Verbindung mit einer terroristischen Einheit erfolgt, oder

e) die Sammlung von Vermögenswerten oder die Aufforderung einer Person, Gruppe oder Organisation, Vermögenswerte oder finanzielle oder andere damit zusammenhängende Dienstleistungen zum Zweck der Durchführung einer Handlung oder Unterlassung gemäß den Buchstaben a oder b bereitzustellen, die Bereitstellung oder Zugänglichmachung solcher Vermögenswerte oder Dienstleistungen oder die Verwendung oder den Besitz von Vermögenswerten zum Zweck der Durchführung einer Handlung oder Unterlassung gemäß den Buchstaben a oder b oder

f) den Versuch oder die Androhung einer Handlung oder Unterlassung gemäß den Buchstaben a oder b, die Verabredung zur Begehung oder Unterlassung einer solchen Handlung, die Beihilfe zu einer solchen Handlung oder Unterlassung, diesbezügliche Anweisungen oder eine diesbezügliche Beratung oder die nachträgliche Mittäterschaft oder die Bereitstellung von Unterschlupf oder Verstecken, um einer terroristischen Einheit die Erleichterung oder Durchführung einer Handlung oder Unterlassung gemäß den Buchstaben a oder b zu ermöglichen.

g) Für die Zwecke dieses Absatzes bezeichnet der Begriff ‚terroristische Einheit':

i) eine Person, Gruppe oder Organisation, deren Zweck oder Tätigkeit unter anderem darin besteht, eine unter den Buchstaben a oder b genannte Handlung oder Unterlassung zu erleichtern oder durchzuführen, oder

ii) eine Person, Gruppe oder Organisation, die wissentlich im Auftrag, unter der Leitung oder in Verbindung mit einer unter Ziffer i genannten Person, Gruppe oder Organisation handelt.

(3) Als grenzübergreifende schwere Kriminalität gilt jede Straftat, die nach kanadischem Recht in Kanada mit einer Freiheitsstrafe im Höchstmaß von mindestens vier Jahren oder mit einer schwereren Strafe geahndet wird, wenn die Straftat grenzübergreifenden Charakter hat.

Für die Zwecke dieses Abkommens gilt eine Straftat als grenzübergreifend, wenn sie

a) in mehr als einem Land verübt wird,

b) in einem Land verübt wird, aber ein Großteil ihrer Vorbereitung, Planung, Lenkung oder Überwachung in einem anderen Land stattfindet,

c) in einem Land im Rahmen einer organisierten kriminellen Vereinigung verübt wird, die kriminellen Handlungen in mehr als einem Land nachgeht,

d) in einem Land verübt wird, aber beträchtliche Auswirkungen in einem anderen Land hat oder

e) in einem Land verübt wird und sich der Straftäter in einem anderen Land aufhält oder dorthin ausreisen will.

(4) In Ausnahmefällen kann die zuständige kanadische Behörde PNR-Daten zum Schutz lebenswichtiger Interessen von Einzelpersonen verarbeiten, zum Beispiel wenn

a) Gefahr für Leib und Leben besteht oder

b) die Gesundheit der Allgemeinheit erheblich gefährdet ist, vor allem im Sinne international anerkannter Normen.

(5) Außerdem kann Kanada im Einzelfall PNR-Daten verarbeiten, damit

a) die Aufsicht oder Rechenschaftspflicht der öffentlichen Verwaltung gewährleistet ist oder

b) einer Vorladung, einem erlassenen Haftbefehl oder einer gerichtlichen Verfügung Folge geleistet werden kann.

ARTIKEL 4

Gewährleistung der Bereitstellung von PNR-Daten

(1) Die Europäische Union sorgt dafür, dass Fluggesellschaften nicht daran gehindert werden, der zuständigen kanadischen Behörde auf der Grundlage dieses Abkommens PNR-Daten zu übermitteln.

(2) Kanada verlangt von den Fluggesellschaften keine PNR-Datenelemente, die die Fluggesellschaften nicht bereits für Buchungszwecke erhoben oder gespeichert haben.

(3) Kanada löscht bei Erhalt alle auf der Grundlage dieses Abkommens von Fluggesellschaften übermittelten Daten, wenn die betreffenden Datenelemente nicht im Anhang aufgeführt sind.

(4) Die Parteien sorgen dafür, dass Fluggesellschaften der zuständigen kanadischen Behörde durch bevollmächtigte Agenturen, die im Namen und unter der Verantwortung der Fluggesellschaften handeln, für die Zwecke dieses Abkommens und unter den darin festgelegten Bedingungen PNR-Daten übermitteln können.

ARTIKEL 5

Angemessenheit

Vorbehaltlich der Einhaltung dieses Abkommens wird davon ausgegangen, dass die zuständige kanadische Behörde bei der Verarbeitung und Verwendung von PNR-Daten einen angemessenen Schutz im Sinne der einschlägigen Datenschutzvorschriften der Europäischen Union gewährleistet. Es wird davon ausgegangen, dass Fluggesellschaften, die Kanada auf der Grundlage dieses Abkommens PNR-Daten übermitteln, die rechtlichen Anforderungen in der Europäischen Union bezüglich der Übermittlung von PNR-Daten aus der Europäischen Union an Kanada erfüllen.

ARTIKEL 6

Polizeiliche und justizielle Zusammenarbeit

(1) Kanada tauscht zum frühestmöglichen Zeitpunkt sachdienliche analytische Informationen, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, mit Europol oder Eurojust im Rahmen ihres jeweiligen Mandats oder mit der Polizei- oder Justizbehörde eines Mitgliedstaats der Europäischen Union aus. Kanada sorgt dafür, dass diese Informationen im Einklang mit den Abkommen und unter Vereinbarungen zwischen Kanada und Europol, Eurojust oder diesem Mitgliedstaat auf dem Gebiet der Strafverfolgung oder des Informationsaustauschs ausgetauscht werden.

(2) Kanada tauscht auf Ersuchen von Europol oder Eurojust im Rahmen ihres jeweiligen Mandats oder auf Ersuchen der Polizei- oder Justizbehörde eines Mitgliedstaats der Europäischen Union in konkreten Fällen PNR-Daten oder analytische Informationen aus, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, um eine terroristische Straftat oder grenzübergreifende schwere Kriminalität in der Europäischen Union zu verhindern, aufzudecken, zu untersuchen oder strafrechtlich zu verfolgen. Kanada stellt diese Informationen im Einklang mit den Abkommen und Vereinbarungen zwischen Kanada und Europol, Eurojust oder diesem Mitgliedstaat auf dem Gebiet der Strafverfolgung, der justiziellen Zusammenarbeit oder des Informationsaustauschs zur Verfügung.

GARANTIEN FÜR DIE VERARBEITUNG VON PNR-DATEN

ARTIKEL 7

Nichtdiskriminierung

Kanada sorgt dafür, dass die auf die Verarbeitung von PNR-Daten anwendbaren Garantien für alle Fluggäste gleichermaßen gelten und keinen Fluggast unrechtmäßig diskriminieren.

ARTIKEL 8

Verwendung sensibler Daten

(1) Enthalten die PNR-Daten eines Fluggastes sensible Daten, so sorgt Kanada dafür, dass die zuständige kanadische Behörde die sensiblen Daten mit Hilfe automatisierter Systeme unkenntlich macht. Kanada sorgt dafür, dass die zuständige kanadische Behörde diese Daten nicht weiter verarbeitet, außer nach Maßgabe der Absätze 3, 4 und 5.

(2) Kanada übermittelt der Europäischen Kommission eine Liste mit Codes und Begriffen zur Auffindung sensibler Daten, die Kanada unkenntlich machen muss. Kanada übermittelt diese Liste binnen 90 Tagen nach Inkrafttreten dieses Abkommens.

(3) Im Einzelfall kann Kanada ausnahmsweise sensible Daten verarbeiten, wenn die Verarbeitung unerlässlich ist, da Gefahr für Leib und Leben einer Einzelperson besteht.

(4) Kanada sorgt dafür, dass sensible Daten im Einklang mit Absatz 3 ausschließlich unter strengen verfahrensrechtlichen Vorgaben verarbeitet werden, darunter Folgende:
a) Die Verarbeitung sensibler Daten wird vom Leiter der zuständigen kanadischen Behörde genehmigt;
b) sensible Daten werden nur von einem eigens und persönlich hierzu befugten Bediensteten verarbeitet und
c) nach Aufhebung der Unkenntlichmachung werden sensible Daten nicht mit Hilfe automatisierter Systeme verarbeitet.
(5) Kanada löscht sensible Daten spätestens 15 Tage nach Erhalt, es sei denn, Kanada speichert die Daten gemäß Artikel 16 Absatz 5.
(6) Verarbeitet die zuständige kanadische Behörde im Einklang mit den Absätzen 3, 4 und 5 sensible Daten, die eine Einzelperson betreffen, die Bürger eines Mitgliedstaats der Europäischen Union ist, sorgt Kanada dafür, dass die zuständige kanadische Behörde die Behörden dieses Mitgliedstaats zum frühestmöglichen Zeitpunkt von der Verarbeitung in Kenntnis setzt. Kanada übermittelt die entsprechende Mitteilung im Einklang mit den Abkommen und Vereinbarungen zwischen Kanada und diesem Mitgliedstaat auf dem Gebiet der Strafverfolgung oder des Informationsaustauschs.

ARTIKEL 9

Datensicherheit und -integrität

(1) Kanada ergreift regulatorische, verfahrensrechtliche oder technische Maßnahmen, um zu verhindern, dass versehentlich, unrechtmäßig oder ohne Befugnis auf PNR-Daten zugegriffen wird, solche Daten versehentlich, unrechtmäßig oder ohne Befugnis verarbeitet werden oder verloren gehen.
(2) Kanada gewährleistet, dass die Einhaltung der Vorschriften überprüft wird, und sorgt für den Schutz, die Sicherheit, die Vertraulichkeit und die Integrität der Daten. Kanada
a) wendet Verschlüsselungs-, Genehmigungs- und Dokumentierungsverfahren auf die PNR-Daten an,
b) beschränkt den Zugriff auf PNR-Daten auf befugte Bedienstete,
c) bewahrt PNR-Daten in einer gesicherten physischen Umgebung auf, die durch Zugangskontrollen geschützt ist, und
d) legt ein Verfahren fest, mit dem sichergestellt wird, dass Abfragen von PNR-Daten nach Maßgabe des Artikels 3 erfolgen.
(3) Wird auf die PNR-Daten einer Einzelperson ohne Befugnis zugegriffen oder werden diese ohne Befugnis weitergegeben, ergreift Kanada Maßnahmen zur Benachrichtigung der betreffenden Person und zur Minderung des Schadensrisikos sowie Abhilfemaßnahmen.
(4) Kanada sorgt dafür, dass die zuständige kanadische Behörde die Europäische Kommission unverzüglich über wesentliche Vorfälle informiert, in denen versehentlich, unrechtmäßig oder ohne Befugnis auf PNR-Daten zugegriffen wurde oder in denen solche Daten versehentlich, unrechtmäßig oder ohne Befugnis verarbeitet wurden oder verloren gegangen sind.
(5) Kanada sorgt dafür, dass bei jedem Verstoß gegen die Datensicherheit, insbesondere solchen Verstößen, die die versehentliche oder unrechtmäßige Vernichtung, den versehentlichen Verlust, die Änderung, die unbefugte Weitergabe, den unbefugten Zugriff oder eine unrechtmäßige Form der Verarbeitung zur Folge haben, wirksame und abschreckende Korrekturmaßnahmen ergriffen werden, zu denen auch Strafen gehören können.

ARTIKEL 10

Aufsicht

(1) Die Einhaltung der Datenschutzgarantien bei der Verarbeitung von PNR-Daten im Rahmen dieses Abkommens wird von einer unabhängigen Behörde oder einer durch administrative Mittel eingerichteten Stelle, die ihre Aufgaben unparteiisch wahrnimmt und nachweislich unabhängig Entscheidungen trifft (im Folgenden ‚Aufsichtsbehörde'), beaufsichtigt. Kanada sorgt dafür, dass die Aufsichtsbehörde befugt ist, die Einhaltung der Vorschriften bezüglich der Erhebung, Verwendung, Weitergabe, Speicherung oder Vernichtung von PNR-Daten zu überprüfen. Die Aufsichtsbehörde kann entsprechende Überprüfungen und Untersuchungen durchführen, über die Ergebnisse Bericht erstatten und der zuständigen kanadischen Behörde Empfehlungen unterbreiten. Kanada sorgt dafür, dass die Aufsichtsbehörde befugt ist, bei Zuwiderhandlungen im Zusammenhang mit diesem Abkommen gegebenenfalls eine strafrechtliche Verfolgung einleiten oder Disziplinarmaßnahmen verhängen zu lassen.
(2) Kanada sorgt dafür, dass die Aufsichtsbehörde dafür Sorge trägt, dass Beschwerden bezüglich Verstößen gegen das Abkommen entgegengenommen, untersucht und beantwortet und angemessene Abhilfemaßnahmen ergriffen werden.

ARTIKEL 11

Transparenz

(1) Kanada sorgt dafür, dass die zuständige kanadische Behörde folgende Informationen auf ihrer Website bereitstellt:
a) ein Verzeichnis der Rechtsvorschriften, die die Erhebung von PNR-Daten gestatten;
b) aus welchem Grund PNR-Daten erhoben werden;
c) wie die PNR-Daten geschützt werden;
d) auf welche Weise und inwieweit die PNR-Daten weitergegeben werden dürfen;

e) Angaben dazu, wie Daten eingesehen und berichtigt werden können, zur Möglichkeit, einen Bestreitungsvermerk anbringen zu lassen, und zu Rechtsbehelfen und
f) Kontaktangaben für Anfragen.
(2) Zur Förderung der Transparenz arbeiten die Parteien mit interessierten Parteien wie der Luftverkehrsbranche zusammen, vorzugsweise zum Zeitpunkt der Buchung, und stellen Fluggästen folgende Informationen zur Verfügung:
a) Gründe für die Erhebung von PNR-Daten,
b) Verwendung von PNR-Daten,
c) Verfahren für die Beantragung von Auskunft über PNR-Daten und
d) Verfahren für die Beantragung der Berichtigung von PNR-Daten.
ARTIKEL 12
Zugang von Einzelpersonen
(1) Kanada sorgt dafür, dass jede Einzelperson Zugang zu ihren PNR-Daten hat.
(2) Kanada sorgt dafür, dass die zuständige kanadische Behörde innerhalb einer angemessenen Frist
a) der Einzelperson eine Kopie ihrer PNR-Daten zur Verfügung stellt, wenn diese schriftlich Auskunft über ihre PNR-Daten beantragt hat;
b) jeden Antrag schriftlich beantwortet;
c) der Einzelperson Zugang zu den erfassten Informationen gewährt und bestätigt, dass die PNR-Daten der Einzelperson offengelegt wurden, wenn diese eine solche Bestätigung wünscht;
d) die rechtlichen oder tatsächlichen Gründe für die Verweigerung des Zugangs zu den PNR-Daten der Einzelperson erläutert;
e) die Einzelperson entsprechend informiert, wenn keine PNR-Daten existieren;
f) die Einzelperson über die Möglichkeit der Einlegung einer Beschwerde und über das Beschwerdeverfahren informiert.
(3) Kanada kann jede Offenlegung von Informationen angemessenen rechtlichen Anforderungen und Beschränkungen unterwerfen, darunter Beschränkungen, die zur Verhinderung, Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung von Straftaten oder zum Schutz der öffentlichen oder nationalen Sicherheit unter gebührender Beachtung des berechtigten Interesses der betroffenen Person erforderlich sind.
ARTIKEL 13
Recht von Einzelpersonen auf Berichtigung oder Anbringung eines Bestreitungsvermerks
(1) Kanada sorgt dafür, dass jede Einzelperson die Berichtigung ihrer PNR-Daten beantragen kann.
(2) Kanada sorgt dafür, dass die zuständige kanadische Behörde alle schriftlichen Anträge auf Berichtigung prüft und innerhalb einer angemessenen Frist
a) die PNR-Daten berichtigt und die Einzelperson von der Berichtigung in Kenntnis setzt oder
b) die Berichtigung ganz oder teilweise ablehnt und
i) den PNR-Daten einen Bestreitungsvermerk beifügt, dem zu entnehmen ist, welche beantragten Berichtigungen abgelehnt wurden,
ii) die Einzelperson davon in Kenntnis setzt, dass
i. der Berichtigungsantrag abgelehnt wurde, und die rechtlichen oder tatsächlichen Gründe für die Ablehnung erläutert,
ii. der Bestreitungsvermerk gemäß Ziffer i den PNR-Daten beigefügt wurde und
c) die Einzelperson über die Möglichkeit, eine Beschwerde einzulegen, und über das Beschwerdeverfahren informiert.
ARTIKEL 14
Verwaltungsrechtliche und gerichtliche Rechtsbehelfe
(1) Kanada sorgt dafür, dass eine unabhängige Behörde oder eine durch administrative Mittel eingerichtete Stelle, die ihre Aufgaben unparteiisch wahrnimmt und nachweislich unabhängig Entscheidungen trifft, Beschwerden von Einzelpersonen betreffend ihren Antrag auf Auskunft über ihre PNR-Daten, Berichtigung dieser Daten oder Anbringung eines Bestreitungsvermerks entgegennimmt, prüft und beantwortet. Kanada sorgt dafür, dass die betreffende Behörde den Beschwerdeführer über die Möglichkeiten der Einlegung eines gerichtlichen Rechtsbehelfs gemäß Absatz 2 informiert.
(2) Kanada sorgt dafür, dass jede Person, die der Auffassung ist, dass ihre Rechte durch eine Entscheidung oder Maßnahme in Bezug auf ihre PNR-Daten verletzt wurden, Anspruch hat auf einen wirksamen gerichtlichen Rechtsbehelf nach kanadischem Recht im Hinblick auf eine gerichtliche Überprüfung oder auf eine andere Wiedergutmachung, wozu auch Schadenersatzzahlungen gehören können.
ARTIKEL 15
Entscheidungen auf der Grundlage der automatisierten Verarbeitung
Kanada trifft Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten.
ARTIKEL 16
Speicherung von PNR-Daten
(1) Kanada speichert PNR-Daten höchstens fünf Jahre ab dem Tag, an dem es sie erhalten hat.

(2) Kanada beschränkt den Datenzugriff auf eine begrenzte Anzahl von durch Kanada eigens hierzu befugten Bediensteten.
(3) 30 Tage nach Erhalt der PNR-Daten nimmt Kanada eine Anonymisierung durch Unkenntlichmachung der Namen sämtlicher Fluggäste vor.
Zwei Jahre nach Erhalt der PNR-Daten nimmt Kanada eine weitere Anonymisierung durch Unkenntlichmachung folgender Informationen vor:
a) andere Namen im PNR-Datensatz sowie Anzahl der in dem Datensatz erfassten Reisenden,
b) sämtliche verfügbaren Kontaktangaben, einschließlich Informationen zur Identifizierung des Dateneingebers,
c) allgemeine Eintragungen, unter anderem Other Supplementary Information (OSI), Special Service Information (SSI) und Special Service Request (SSR) Information, sofern sie Angaben enthalten, anhand deren eine natürliche Person identifiziert werden kann, und
d) etwaige für Buchungszwecke erhobene Daten zur Advance Passenger Information (API), sofern sie Angaben enthalten, anhand deren eine natürliche Person identifiziert werden kann.
(4) Kanada darf die Unkenntlichmachung von PNR-Daten nur aufheben, wenn aufgrund der verfügbaren Informationen Untersuchungen nach Maßgabe des Artikels 3 durchgeführt werden müssen, und zwar
a) von 30 Tagen bis zwei Jahren nach dem erstmaligen Erhalt nur durch eine begrenzte Anzahl eigens hierzu befugter Bediensteter und
b) von zwei bis fünf Jahren nach dem erstmaligen Erhalt nur mit vorheriger Genehmigung des Leiters der zuständigen kanadischen Behörde oder eines vom Leiter eigens hiermit beauftragten hohen Beamten.
(5) Unbeschadet des Absatzes 1 gilt:
a) Kanada darf PNR-Daten speichern, die bis zum Abschluss einer besonderen Maßnahme, Überprüfung, Untersuchung, Vollzugsmaßnahme, eines Gerichtsverfahrens, einer strafrechtlichen Verfolgung oder der Vollstreckung von Strafen erforderlich sind;
b) Kanada darf die PNR-Daten, auf die Buchstabe a Bezug nimmt, während weiterer zwei Jahre nur speichern, um die Rechenschaftspflicht oder Aufsicht der öffentlichen Verwaltung zu gewährleisten, sodass sie dem [Fluggast] offengelegt werden können, sollte dieser dies beantragen.
(6) Kanada vernichtet die PNR-Daten bei Ablauf von deren Speicherfrist.
ARTIKEL 17
Protokollierung und Dokumentierung der Verarbeitung von PNR-Daten
Kanada protokolliert und dokumentiert die gesamte Verarbeitung von PNR-Daten. Kanada verwendet Protokolle oder Dokumentierungen ausschließlich
a) zu Zwecken der Selbstüberwachung und der Überprüfung der Rechtmäßigkeit der Datenverarbeitung,
b) zur Gewährleistung einer angemessenen Datenintegrität,
c) zur Gewährleistung der Sicherheit der Datenverarbeitung und
d) zur Gewährleistung der Aufsicht und Rechenschaftspflicht der öffentlichen Verwaltung.
ARTIKEL 18
Weitergabe innerhalb Kanadas
(1) Kanada sorgt dafür, dass die zuständige kanadische Behörde PNR-Daten an andere [Behörden] in Kanada nur weitergibt, wenn folgende Bedingungen erfüllt sind:
a) die PNR-Daten werden an [Behörden] weitergegeben, deren Aufgaben einen direkten Bezug zum Anwendungsbereich des Artikels 3 aufweisen,
b) die PNR-Daten werden nur fallweise weitergegeben,
c) unter den betreffenden Umständen ist die Weitergabe zu den in Artikel 3 genannten Zwecken notwendig,
d) es werden nur die unbedingt erforderlichen PNR-Daten weitergegeben,
e) die [Behörde], die die PNR-Daten erhält, gewährleistet einen den in diesem Abkommen beschriebenen Garantien entsprechenden Schutz und
f) die [Behörde], die die PNR-Daten erhält, gibt diese nur dann an eine andere Stelle weiter, wenn die Weitergabe von der zuständigen kanadischen Behörde unter Einhaltung der in diesem Absatz festgelegten Bedingungen genehmigt wurde.
(2) Werden analytische Informationen übermittelt, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, sind die in diesem Artikel festgelegten Garantien für diese Daten einzuhalten.
ARTIKEL 19
Weitergabe außerhalb Kanadas
(1) Kanada sorgt dafür, dass die zuständige kanadische Behörde PNR-Daten an [Behörden] in anderen Ländern als den Mitgliedstaaten der EU nur weitergibt, wenn folgende Bedingungen erfüllt sind:
a) die PNR-Daten werden an [Behörden] weitergegeben, deren Aufgaben einen direkten Bezug zum Anwendungsbereich des Artikels 3 aufweisen;
b) die PNR-Daten werden nur fallweise weitergegeben;
c) die PNR-Daten werden nur weitergegeben, wenn dies zu den in Artikel 3 genannten Zwecken notwendig ist;
d) es werden nur die unbedingt erforderlichen PNR-Daten weitergegeben;

e) die zuständige kanadische Behörde ist davon überzeugt, dass
i) die ausländische Behörde, die die PNR-Daten erhält, im Einklang mit den Abkommen und Vereinbarungen, die Normen zum Schutz von PNR-Daten umfassen, solche Normen anwendet und diese den in diesem Abkommen festgelegten Normen entsprechen, oder
ii) die ausländische Behörde die von ihr mit der Europäischen Union vereinbarten Normen zum Schutz von PNR-Daten anwendet.
(2) Gibt die zuständige kanadische Behörde im Einklang mit Absatz 1 PNR-Daten einer Einzelperson weiter, die Bürger eines Mitgliedstaats der Europäischen Union ist, sorgt Kanada dafür, dass die zuständige kanadische Behörde die Behörden dieses Mitgliedstaats zum frühestmöglichen Zeitpunkt von der Weitergabe in Kenntnis setzt. Kanada übermittelt die entsprechende Mitteilung im Einklang mit den Abkommen und Vereinbarungen zwischen Kanada und diesem Mitgliedstaat auf dem Gebiet der Strafverfolgung oder des Informationsaustauschs.
(3) Werden analytische Informationen übermittelt, die im Rahmen dieses Abkommens erlangte PNR-Daten enthalten, sind die in diesem Artikel festgelegten Garantien für diese Daten einzuhalten.

ARTIKEL 20

Übermittlungsverfahren

Die Parteien stellen sicher, dass die Fluggesellschaften der zuständigen kanadischen Behörde die PNR-Daten ausschließlich im ‚Push'-Verfahren und unter Beachtung folgender Verfahrensbedingungen übermitteln:
a) Übermittlung der PNR-Daten auf elektronischem Wege entsprechend den technischen Erfordernissen der zuständigen kanadischen Behörde oder im Falle technischer Störungen auf jede sonstige geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet;
b) Übermittlung der PNR-Daten unter Verwendung eines gegenseitig anerkannten Nachrichtenformats;
c) Übermittlung der PNR-Daten in sicherer Weise unter Verwendung der von der zuständigen kanadischen Behörde geforderten gemeinsamen Protokolle.

ARTIKEL 21

Häufigkeit der Datenübermittlung

(1) Kanada sorgt dafür, dass die zuständige kanadische Behörde von den Fluggesellschaften verlangt,
a) die PNR-Daten planmäßig zu übermitteln, wobei die früheste Übermittlung bis zu 72 Stunden vor dem planmäßigen Abflug erfolgen kann, und
b) die PNR-Daten je Flug höchstens fünfmal zu übermitteln.
(2) Kanada sorgt dafür, dass die zuständige kanadische Behörde den Fluggesellschaften die Übermittlungszeitpunkte mitteilt.
(3) In Fällen, in denen Hinweise darauf vorliegen, dass ein zusätzlicher Zugang zu den Daten notwendig ist, um auf eine bestimmte Gefahr im Zusammenhang mit dem Anwendungsbereich des Artikels 3 zu reagieren, kann die zuständige kanadische Behörde die PNR-Daten auch vor, zwischen oder nach den planmäßigen Übermittlungen von einer Fluggesellschaft verlangen. Kanada nutzt diesen Ermessensspielraum mit aller Umsicht und unter Wahrung der Verhältnismäßigkeit sowie unter Einsatz des Übermittlungsverfahrens gemäß Artikel 20.

DURCHFÜHRUNGS- UND SCHLUSSBESTIMMUNGEN

ARTIKEL 22

Vor Inkrafttreten dieses Abkommens erhaltene PNR-Daten

Kanada wendet dieses Abkommen auf alle PNR-Daten an, in dessen Besitz es zum Zeitpunkt des Inkrafttretens des Abkommens ist.

ARTIKEL 23

Gegenseitigkeit

(1) Falls die Europäische Union eine PNR-Daten-Verarbeitungsregelung für die Europäische Union einführt, beraten sich die Parteien darüber, ob dieses Abkommen geändert werden sollte, um die volle Gegenseitigkeit sicherzustellen.
(2) Die jeweiligen Behörden Kanadas und der Europäischen Union arbeiten zusammen, um die Kohärenz ihrer Verarbeitungsregelungen für PNR-Daten weiter auszubauen, um die Sicherheit der Bürger in Kanada, der Europäischen Union und andernorts weiter zu verbessern.

ARTIKEL 24

Nichtabweichung

Dieses Abkommen ist nicht dahin gehend auszulegen, dass von einer aufgrund einer Amtshilfevereinbarung zwischen Kanada und Mitgliedstaaten der Europäischen Union oder Drittländern bestehenden Verpflichtung zur Übermittlung oder Beantwortung von Hilfeersuchen abgewichen werden darf.

…

ARTIKEL 26

Konsultation, Überprüfung und Änderungen

…

(2) Die Parteien überprüfen gemeinsam die Durchführung des Abkommens ein Jahr nach dessen Inkrafttreten und danach in regelmäßigen Abständen sowie auf Ersuchen einer Partei und nach gemeinsamem Beschluss.

…

ARTIKEL 28
Laufzeit
(1) Vorbehaltlich des Absatzes 2 gilt dieses Abkommen für einen Zeitraum von sieben Jahren ab dem Zeitpunkt des Inkrafttretens.
(2) Am Ende jedes Siebenjahreszeitraums verlängert sich das Abkommen automatisch um weitere sieben Jahre, sofern nicht eine Partei der anderen mitteilt, dass sie dieses Abkommen nicht verlängern will. Die Partei muss dies der anderen Partei mindestens sechs Monate vor Ablauf des Siebenjahreszeitraums auf diplomatischem Wege schriftlich notifizieren.
(3) Kanada wendet das Abkommen weiterhin auf alle PNR-Daten an, die es vor Kündigung des Abkommens erhalten hat.
…
ANHANG
Elemente von Fluggastdatensätzen nach Artikel 2 Buchstabe b
1. PNR-Buchungscode (Locator Code)
2. Datum der Buchung bzw. der Ausstellung des Flugscheins
3. Datum bzw. Daten des geplanten Flugs
4. Name(n)
5. Verfügbare Vielflieger- und Bonus-Daten (Gratisflugscheine, Upgrades usw.)
6. Andere Namen im PNR-Datensatz sowie Anzahl der in dem Datensatz erfassten Reisenden
7. Sämtliche verfügbaren Kontaktangaben, einschließlich Informationen zur Identifizierung des Dateneingebers
8. Sämtliche verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)
9. Von dem jeweiligen PNR-Datensatz erfasste Reiseroute
10. Reisebüro/Sachbearbeiter
11. Code-Sharing-Informationen
12. Informationen über Buchungssplitting bzw. -teilung
13. Reisestatus des Fluggastes (einschließlich Bestätigungen und Eincheckstatus)
14. Flugscheininformationen (Ticketing Information), einschließlich Flugscheinnummer, Hinweis auf einen etwaigen einfachen Flug (One Way Ticket) und automatische Tarifanzeige (Automatic Ticket Fare Quote)
15. Sämtliche Informationen zum Gepäck
16. Sitzplatzinformationen, inklusive Sitzplatznummer
17. Allgemeine Eintragungen einschließlich OSI- (Other Supplementary Information), SSI- (Special Service Information) und SSR-Informationen (Special Service Request)
18. Etwaige für Buchungszwecke erhobene Daten zur Advance Passenger Information (API)
19. Historie aller Änderungen in Bezug auf die unter den Nummern 1 bis 18 aufgeführten PNR-Daten.“

*VI. Ausführungen des Parlaments in seinem Gutachtenantrag*

A. **Zur geeigneten Rechtsgrundlage des Beschlusses des Rates über den Abschluss des geplanten Abkommens**

31 Das Parlament trägt vor, mit dem geplanten Abkommen würden nach dessen Art. 1 zwei Ziele verfolgt: die Gewährleistung der öffentlichen Sicherheit und die Festlegung der Bedingungen, unter denen die PNR-Daten zu schützen seien. Hauptziel sei aber der Schutz personenbezogener Daten. Das Unionsrecht im Bereich des Schutzes personenbezogener Daten stehe nämlich der Übermittlung von PNR-Daten an Drittländer, die keinen angemessenen Schutz solcher Daten gewährleisteten, entgegen. Mit dem geplanten Abkommen solle somit eine Art „Angemessenheitsbeschluss“ im Sinne von Art. 25 Abs. 6 der Richtlinie 95/46 geschaffen werden, um eine Rechtsgrundlage für die rechtmäßige Übermittlung der PNR-Daten von der Union nach Kanada zu haben. Dieser Ansatz entspreche dem, der zuvor im Abkommen von 2006 und der auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 erlassenen Entscheidung 2006/253 verfolgt worden sei.

32 Art. 82 Abs. 1 Unterabs. 2 Buchst. d und Art. 87 Abs. 2 Buchst. a AEUV eigneten sich nicht als Rechtsgrundlagen für den Beschluss des Rates über den Abschluss des geplanten Abkommens. Der Beschluss sei vielmehr auf Art. 16 AEUV zu stützen, der in sämtlichen Bereichen des Unionsrechts anwendbar sei, auch in denen des Titels V des Dritten Teils des AEU-Vertrags über den Raum der Freiheit, der Sicherheit und des Rechts, was durch die Erklärung zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang der Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon angenommen habe (ABl. 2010, C 83, S. 345), bestätigt werde.

33 Dass der Hauptbestandteil des geplanten Abkommens den Schutz personenbezogener Daten betreffe, werde durch dessen Inhalt bestätigt. Die meisten Bestimmungen des Abkommens, insbesondere seine Kernbestimmungen, nämlich Art. 4 Abs. 1 und Art. 5, die die Rechtsgrundlage der rechtmäßigen Übermittlung von PNR-Daten aus der Union nach Kanada darstellten, beträfen den Schutz personenbezogener Daten. Zudem gehe es in

dem Abkommen um die Übermittlung von PNR-Daten an die kanadischen Behörden nicht durch die europäischen Behörden, sondern durch Unternehmen, und zwar die Fluggesellschaften. Es könne deshalb schwerlich angenommen werden, dass die Bestimmungen unter die polizeiliche und justizielle Zusammenarbeit im engeren Sinne fielen. Außerdem sei Art. 6 („Polizeiliche und justizielle Zusammenarbeit“) des geplanten Abkommens gegenüber dessen Art. 4 und 5 von untergeordneter Bedeutung, weil er nur bei deren Anwendung zum Zuge komme. Kanada könne die betreffenden Informationen nämlich nur übermitteln, wenn es von den Fluggesellschaften zuvor die PNR-Daten erhalten habe. Und die Fluggesellschaften dürften Kanada die PNR-Daten nur auf der Grundlage eines „Angemessenheitsbeschlusses“ übermitteln. Außerdem regele Art. 6 nicht den Austausch von Informationen zwischen den betreffenden Behörden. Er verweise lediglich auf andere internationale Übereinkünfte in diesem Bereich.

34 Sollte der Gerichtshof dennoch zu der Ansicht gelangen, dass mit dem geplanten Abkommen Ziele verfolgt würden, die untrennbar miteinander verbunden seien, könnte der Beschluss des Rates über den Abschluss des Abkommens zugleich auf Art. 16, Art. 82 Abs. 1 Unterabs. 2 Buchst. d und Art. 87 Abs. 2 Buchst. a AEUV gestützt werden. Hinsichtlich der Anwendbarkeit der Protokolle Nrn. 21 und 22 sei auf die durch das Urteil vom 27. Februar 2014, Vereinigtes Königreich/Rat (C-656/11, EU:C:2014:97, Rn. 49), begründete Rechtsprechung des Gerichtshofs hinzuweisen, nach der sich auf die Rechtmäßigkeit der Wahl der Rechtsgrundlage einer Handlung der Union nicht auswirke, welche Folge sie im Hinblick auf die Anwendung oder die fehlende Anwendung eines den Verträgen beigefügten Protokolls haben könne.

B. **Zur Vereinbarkeit des geplanten Abkommens mit den Vorschriften des AEU-Vertrags und der Charta der Grundrechte der Europäischen Union**

35 Das Parlament vertritt die Auffassung, in Anbetracht der ernsthaften Zweifel, die der EDSB insbesondere in seiner Stellungnahme vom 30. September 2013 geäußert habe, und der durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), begründeten Rechtsprechung bestehe Rechtsunsicherheit hinsichtlich der Frage, ob das geplante Abkommen mit Art. 16 AEUV sowie mit Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) vereinbar sei.

36 Die im geplanten Abkommen vorgesehene Übermittlung von PNR-Daten aus der Union nach Kanada, auf die die kanadischen Behörden dann gegebenenfalls zugreifen könnten, falle unter die Art. 7 und 8 der Charta. Aus den PNR-Daten ließen sich insgesamt sehr genaue Schlüsse auf das Privatleben der betreffenden Personen ziehen, z. B. ihr ständiger oder vorübergehender Aufenthaltsort, ihre Reisen und ihre Tätigkeiten. Mit dem Abkommen werde daher in großem Umfang und besonders schwer in die durch die Art. 7 und 8 der Charta garantierten Grundrechte eingegriffen.

37 Angesichts der Anforderungen von Art. 52 Abs. 1 und Art. 8 Abs. 2 der Charta sei zu prüfen, ob das geplante Abkommen ein „Gesetz“ im Sinne dieser Vorschriften darstelle und ob es als Rechtsgrundlage für Einschränkungen der Ausübung der durch die Art. 7 und 8 der Charta garantierten Rechte herhalten könne. Der Begriff des Gesetzes decke sich mit dem des Gesetzgebungsakts im Sinne des AEU-Vertrags. Eine internationale Übereinkunft stelle aber keinen Gesetzgebungsakt dar, so dass sich die Frage stelle, ob es nicht zweckmäßiger wäre, auf der Grundlage von Art. 16 AEUV einen internen Rechtsakt zu erlassen als gemäß Art. 218 AEUV eine internationale Übereinkunft wie das geplante Abkommen zu schließen.

38 Hinsichtlich des Grundsatzes der Verhältnismäßigkeit sei auf die durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 47 und 48), begründete Rechtsprechung des Gerichtshofs zu verweisen. Im vorliegenden Fall sei der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt. Es müsse gerichtlich streng überprüft werden, ob der Grundsatz der Verhältnismäßigkeit beachtet worden sei, u. a., weil Grundrechtseingriffe in Rede stünden.

39 Außerdem ergebe sich aus der durch das Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 1. Juli 2008, Liberty u. a./Vereinigtes Königreich (CE:ECHR:2008:0701JUD005824300, §§ 62 und 63), begründeten Rechtsprechung und der durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und die dort angeführte Rechtsprechung), begründeten Rechtsprechung des Gerichtshofs, dass das geplante Abkommen klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahmen vorsehen und Mindestanforderungen aufstellen müsse, so dass die Personen, deren personenbezogene Daten verarbeitet worden seien, über ausreichende Garantien verfügten, die einen wirksamen Schutz der Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung ermöglichten.

40 Erstens sei fraglich, ob die Schaffung eines „PNR-Systems“ im Sinne von Art. 52 Abs. 1 Satz 2 der Charta erforderlich sei. Der Rat und die Kommission hätten bislang nicht dargetan, dass der Abschluss des geplanten Abkommens tatsächlich erforderlich sei.

41 Zweitens betreffe das geplante Abkommen pauschal sämtliche Fluggäste. Diese müssten sich nicht in einer Situation befinden, die Strafverfolgungsmaßnahmen nach sich ziehen könne. Es sei auch nicht erforderlich, dass ein Zusammenhang zwischen ihren PNR-Daten und einer Gefahr für die öffentliche Sicherheit bestehe. Es gebe also überhaupt keine Grenzen. Außerdem seien die im Abkommen genannten Kriterien und Voraussetzungen unbestimmt. Mit ihnen lasse sich die Verarbeitung der PNR-Daten durch die kanadischen Behörden nicht auf das absolut Notwendige beschränken. Das Abkommen mache den Zugang zu den PNR-Daten durch die

kanadischen Behörden nicht von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Behörde abhängig, die dazu diene, den Zugang zu den Daten und ihre Verwendung auf das zu beschränken, was zur Erreichung des verfolgten Ziels absolut notwendig sei, und die auf einen begründeten Antrag an das Gericht oder die Behörde im Rahmen von Verfahren der Verhütung, Aufklärung oder Verfolgung von Straftaten hin durchgeführt werde.

42 Drittens gelte die Dauer der Speicherung von PNR-Daten, die in Art. 16 des geplanten Abkommens auf fünf Jahre festgesetzt sei, unterschiedslos für sämtliche Fluggäste. Der Rat habe die Entscheidung für eine solche Dauer der Speicherung in keiner Weise objektiv gerechtfertigt. Selbst wenn die im Abkommen von 2006 vorgesehene Dauer von dreieinhalb Jahren zulässig wäre, stelle sich die Frage, warum sie auf fünf Jahre habe angehoben werden müssen.

43 Viertens schließlich gewährleiste das geplante Abkommen nicht, dass die von den kanadischen Behörden zu treffenden Maßnahmen angemessen seien und den wesentlichen Anforderungen von Art. 8 der Charta und Art. 16 AEUV entsprächen.

*VII. Zusammenfassung der beim Gerichtshof eingereichten Stellungnahmen*

44 Die bulgarische und die estnische Regierung, Irland, die spanische und die französische Regierung, die Regierung des Vereinigten Königreichs sowie der Rat und die Kommission haben beim Gerichtshof schriftliche Stellungnahmen zum vorliegenden Gutachtenantrag eingereicht.

45 Ferner hat der Gerichtshof den Mitgliedstaaten und den in Art. 196 Abs. 3 seiner Verfahrensordnung genannten Organen Fragen zur schriftlichen Beantwortung gestellt. Er hat gemäß Art. 24 Abs. 2 der Satzung des Gerichtshofs der Europäischen Union auch den EDSB aufgefordert, die Fragen zu beantworten. Dieser hat seine Stellungnahme beim Gerichtshof eingereicht.

A. **Zur Zulässigkeit des Gutachtenantrags**

46 Die französische Regierung und der Rat haben Zweifel an der Zulässigkeit der zweiten Frage des vorliegenden Gutachtenantrags. Mit dieser Frage stelle das Parlament nämlich weder die Zuständigkeit der Union für den Abschluss des geplanten Abkommens noch die Verteilung der Zuständigkeiten zwischen der Union und den Mitgliedstaaten in diesem Bereich in Frage. Außerdem hätte die Heranziehung der Art. 82 und 87 AEUV, auch wenn sie unzutreffend wäre, keinen Einfluss auf das beim Erlass des Beschlusses des Rates über den Abschluss des geplanten Abkommens einzuhaltende Verfahren, da sowohl bei der Anwendung von Art. 16 AEUV als auch bei der Anwendung der Art. 82 und 87 AEUV eine Entscheidung im ordentlichen Gesetzgebungsverfahren erforderlich wäre. In beiden Fällen wäre daher Art. 218 Abs. 6 Buchst. a Ziff. v AEUV anwendbar, so dass die Zustimmung des Parlaments erforderlich wäre.

B. **Zur geeigneten Rechtsgrundlage des Beschlusses des Rates über den Abschluss des geplanten Abkommens**

47 Die bulgarische und die estnische Regierung, Irland, die französische Regierung, die Regierung des Vereinigten Königreichs sowie der Rat und die Kommission vertreten die Auffassung, Hauptziel des geplanten Abkommens sei die Gewährleistung der öffentlichen Sicherheit, wie sich u. a. aus den Abs. 1, 2, 3 und 5 der Präambel des Abkommens und aus dessen Art. 1 und 3 ergebe. Zwar werde mit dem Abkommen auch der Schutz personenbezogener Daten bezweckt. Dieses Ziel sei gegenüber dem Hauptziel jedoch von untergeordneter Bedeutung.

48 Der Rat und die Kommission fügen hinzu, bei der Übermittlung von PNR-Daten in Drittländer müsse zwar die Charta beachtet werden. Die den Schutz dieser Daten betreffenden Bestimmungen des geplanten Abkommens stellten aber lediglich das Mittel dar, mit dem das Abkommen das Ziel der Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität verfolge. Auch wenn das Abkommen mit zahlreichen Bestimmungen die Modalitäten und Voraussetzungen der Übermittlung von PNR-Daten unter Beachtung der Grundrechte festlege und eine Art von „Angemessenheitsbeschluss“ schaffe, bleibe sein Hauptziel die Gewährleistung der öffentlichen Sicherheit. Art. 16 AEUV komme nur dann als Rechtsgrundlage für einen Rechtsakt in Betracht, wenn der Schutz personenbezogener Daten dessen Hauptziel sei. Rechtsakte zur Verwirklichung von Politiken in bestimmten Bereichen, die gewisse Verarbeitungen personenbezogener Daten erforderten, müssten hingegen auf die bereichsspezifische Rechtsgrundlage gestützt werden und sowohl mit Art. 8 der Charta als auch mit den auf der Grundlage von Art. 16 AEUV erlassenen Unionsrechtsakten im Einklang stehen.

49 Die französische Regierung macht hilfsweise geltend, es sei durchaus möglich, den Beschluss des Rates über den Abschluss des geplanten Abkommens gleichzeitig auf mehrere materielle Rechtsgrundlagen, nämlich Art. 16, Art. 82 Abs. 1 Unterabs. 2 Buchst. d und Art. 87 Abs. 2 Buchst. a AEUV, zu stützen. Alle diese Rechtsgrundlagen sähen das ordentliche Gesetzgebungsverfahren vor und seien deshalb miteinander kompatibel. Da sich Irland und das Vereinigte Königreich sowie das Königreich Dänemark nach den Protokollen Nrn. 21 und 22 nicht an der Annahme von Maßnahmen beteiligten, die zum Dritten Teil Titel V des AEU-Vertrags gehörten, könne ein Rechtsakt im Prinzip zwar nicht gleichzeitig auf unter diesen Titel und nicht unter diesen Titel fallende Vorschriften gestützt werden. Würden aber auf der Grundlage von Art. 16 AEUV Vorschriften über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten erlas-

sen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 oder 5 des AEU-Vertrags fielen, würden sich Irland und das Vereinigte Königreich sowie das Königreich Dänemark nicht an ihrer Annahme beteiligen, weil die Vorschriften sie gemäß Art. 6a des Protokolls Nr. 21 bzw. Art. 2a des Protokolls Nr. 22 nicht bänden.

50 Der Rat vertritt hingegen die Auffassung, dass eine Kombination von Art. 16 AEUV und der Art. 82 und 87 AEUV wegen der speziellen Regeln über die Abstimmungsmodalitäten des Rates, wie sie sich aus den Protokollen Nrn. 21 und 22 für die Beteiligung Irlands und des Vereinigten Königreichs bzw. des Königreichs Dänemark ergäben, rechtlich nicht zulässig sei.

C. **Zur Vereinbarkeit des geplanten Abkommens mit den Vorschriften des AEU-Vertrags und der Charta**

51 Alle Mitgliedstaaten, die beim Gerichtshof Erklärungen eingereicht haben, sowie der Rat und die Kommission sind im Kern der Auffassung, dass das geplante Abkommen mit den Vorschriften des AEU-Vertrags und der Charta vereinbar sei.

52 In Bezug auf das Vorliegen eines Eingriffs in die in den Art. 7 und 8 der Charta verankerten Grundrechte teilen die estnische und die französische Regierung die Auffassung des Parlaments, dass das geplante Abkommen einen solchen Eingriff darstelle, weil es die Union verpflichte, die Übermittlung von PNR-Daten an die zuständige kanadische Behörde nicht zu verhindern (Art. 4 Abs. 1), und die Verarbeitung der Daten durch diese Behörde vorsehe (Art. 3). Die französische Regierung vertritt jedoch die Auffassung, dass der Eingriff nicht als besonders schwer zu qualifizieren sei. Er sei weniger einschneidend als der Eingriff durch die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54), die Gegenstand der Rechtssache gewesen sei, in der das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), ergangen sei. Im Übrigen ließen sich aus PNR-Daten keine besonders genauen Schlüsse auf das Privatleben der Fluggäste ziehen.

53 Alle Mitgliedstaaten, die Erklärungen eingereicht haben, sowie der Rat und die Kommission vertreten die Auffassung, dass das geplante Abkommen eine dem Gemeinwohl dienende Zielsetzung habe, nämlich die Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität.

54 In Bezug auf die Anforderungen, die sich aus dem Grundsatz der Verhältnismäßigkeit ergeben, teilen der Rat und die Kommission die Auffassung des Parlaments. Unter Berufung auf die durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 54), begründete Rechtsprechung des Gerichtshofs und auf Art. 6 Abs. 1 Buchst. c der Richtlinie 95/46 machen sie geltend, dass das geplante Abkommen klare und präzise Regeln für die Tragweite und die Anwendung des fraglichen Eingriffs und ausreichende Garantien vorsehen müsse, die einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichten.

55 Was insbesondere die Erforderlichkeit der Übermittlung der PNR-Daten an Kanada angeht, räumt die Kommission, unterstützt durch den Rat, ein, dass es keine genauen Statistiken gebe, aus denen ersichtlich wäre, inwieweit die Daten zur Vorbeugung, Aufklärung, Untersuchung und strafrechtlichen Verfolgung von Kriminalität und Terrorismus beitrügen. Dass die Verwendung der PNR-Daten unerlässlich sei, werde aber durch Informationen aus Drittländern und Mitgliedstaaten bestätigt, die die Daten bereits zur strafrechtlichen Verfolgung heranzögen. Wie in der Begründung des Vorschlags vom 2. Februar 2011 für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM[2011] 32 endgültig) ausgeführt werde, habe die Verwendung von PNR-Daten, wie die Erfahrung bestimmter Länder zeige, insbesondere zu entscheidenden Fortschritten im Kampf gegen Drogenhandel, Menschenhandel und Terrorismus sowie zu besseren Erkenntnissen über die Zusammensetzung und Operationen von Terrornetzen und sonstigen kriminellen Netzen geführt.

56 Außerdem hätten die kanadischen Behörden Informationen vorgelegt, aus denen hervorgehe, dass die PNR-Daten entscheidend zur Identifizierung von Personen beigetragen hätten, die terroristischer oder schwerer Straftaten verdächtig gewesen seien. Von April 2014 bis März 2015 seien 28 Mio. Fluggäste aus der Union nach Kanada geflogen. Die PNR-Daten hätten in 178 Fällen die Feststellung der Identität, in 71 Fällen die Beschlagnahme von Betäubungsmitteln und in 2 Fällen die Beschlagnahme kinderpornografischen Materials ermöglicht. Aufgrund der PNR-Daten sei es ferner möglich gewesen, in 169 Fällen Ermittlungen im Zusammenhang mit terroristischen Straftaten einzuleiten oder fortzusetzen. Schließlich müsse nach der Mitteilung der Kommission vom 21. September 2010 über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer (KOM[2010] 492 endgültig, im Folgenden: Mitteilung KOM[2010] 492) die Union „nicht nur in ihrem eigenen Interesse, sondern auch im Interesse von Drittländern mit diesen gemeinsam gegen [Terrorismus und grenzübergreifende schwere Kriminalität] vorgehen“.

57 Die estnische Regierung, Irland, die spanische und die französische Regierung, die Regierung des Vereinigten Königreichs sowie der Rat und die Kommission stimmen im Wesentlichen darin überein, dass das geplante Abkommen den Anforderungen des Grundsatzes der Verhältnismäßigkeit genüge und dass sich der vorliegende Fall von dem unterscheide, um den es im Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und

C-594/12, EU:C:2014:238), gegangen sei. Der durch das geplante Abkommen vorgesehene Mechanismus komme eher systematischen Kontrollen an den Außengrenzen und Sicherheitskontrollen in Flughäfen gleich als einer Vorratsspeicherung von Daten im Sinne der Richtlinie 2006/24. Außerdem sei das geplante Abkommen in seiner Rechtsnatur und seinen Wirkungen deutlich begrenzter als die Richtlinie. Anders als die Richtlinie enthalte es strenge Regeln über die Voraussetzungen und Grenzen des Zugangs zu den Daten und deren Verwendung sowie Regeln über die Sicherheit der Daten. Und es sehe eine Überwachung der Beachtung der Regeln durch eine unabhängige Behörde, die Information der betroffenen Personen über die Übermittlung und Verarbeitung ihrer Daten, ein Recht auf Auskunft und Berichtigung sowie Verwaltungs- und gerichtliche Rechtsbehelfe vor, um die Rechte dieser Personen zu gewährleisten.

58 Zu dem Vorbringen des Parlaments, das geplante Abkommen mache die Übermittlung von PNR-Daten nicht vom Vorliegen einer Gefährdung der öffentlichen Sicherheit abhängig, machen die estnische und die französische Regierung, die Regierung des Vereinigten Königreichs sowie die Kommission im Wesentlichen geltend, mit der Verwendung solcher Daten solle die Identifizierung von Personen ermöglicht werden, von denen eine potenzielle Gefahr für die Sicherheit ausgehe und die den zuständigen Behörden bislang nicht bekannt gewesen seien. Personen, die den Behörden bereits bekannt seien, könnten auf der Grundlage zuvor zusammengetragener Informationen über die Fluggäste identifiziert werden. Wäre nur die Übermittlung von PNR-Daten über Personen, bei denen bereits mitgeteilt worden sei, dass von ihnen eine Gefahr für die Sicherheit ausgehe, zulässig, könnte das Ziel der Vorbeugung nicht erreicht werden.

59 Zu den Grenzen der Verwendung von PNR-Daten machen der Rat und die Kommission geltend, das geplante Abkommen sei nicht deshalb zu unbestimmt, weil in seinem Art. 3 Abs. 3 auf das kanadische Recht verwiesen werde. In eine internationale Übereinkunft könnten schwerlich ausschließlich unionsrechtliche Begriffe aufgenommen werden. Hintergrund von Art. 3 Abs. 5 Buchst. b des Abkommens sei die allen kanadischen Behörden durch die kanadische Verfassung auferlegte Verpflichtung, einer rechtskräftigen Gerichtsentscheidung Folge zu leisten. Außerdem setze diese Vorschrift voraus, dass der Zugang zu den PNR-Daten vom Gericht anhand der Kriterien der Erforderlichkeit und der Verhältnismäßigkeit geprüft und in seiner Entscheidung begründet worden sei. Im Übrigen hätten die kanadischen Behörden die Vorschrift seit dem Inkrafttreten der Vereinbarung von 2006 in der Praxis noch nie angewandt.

60 Zur Begrenzung der Behörden und Personen, die Zugang zu den PNR-Daten haben, vertreten der Rat und die Kommission die Auffassung, die fehlende Benennung der zuständigen kanadischen Behörde im geplanten Abkommen sei eine verfahrensrechtliche Frage, die dafür, ob das Abkommen den Grundsatz der Verhältnismäßigkeit einhalte, unerheblich sei. Jedenfalls habe Kanada der Union im Juni 2014 mitgeteilt, dass die zuständige kanadische Behörde im Sinne von Art. 2 Buchst. d des Abkommens die CBSA sei. Nach Art. 16 Abs. 2 des geplanten Abkommens habe Kanada den Datenzugriff auf eine „begrenzte Anzahl von durch Kanada eigens hierzu befugten Bediensteten“ zu beschränken. Folglich seien nur die Bediensteten der CBSA befugt, Daten zu erhalten und zu verarbeiten. Zusätzliche Garantien fänden sich in Art. 9 Abs. 2 Buchst. a und b sowie in Art. 9 Abs. 4 und 5 des Abkommens.

61 Was die Tatsache angeht, dass das geplante Abkommen den Zugang zu den PNR-Daten nicht von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Behörde abhängig macht, vertritt Irland die Auffassung, dass eine solche Kontrolle in Anbetracht der in den Art. 11 bis 14, 16, 18 und 20 des Abkommens enthaltenen Garantien nicht unerlässlich sei. Die estnische Regierung und die Regierung des Vereinigten Königreichs vertreten die Auffassung, die Kriterien der PNR-Daten, die verarbeitet werden müssten, ließen sich nicht im Voraus bestimmen, so dass nicht generell die Einholung einer vorherigen Genehmigung verlangt werden könne. Eine vorherige Genehmigung könnte daher lediglich allgemein sein und brächte keinen Mehrwert.

62 Zu der Frage der Weitergabe von PNR-Daten an andere Behörden macht die Kommission geltend, in den Art. 1, 3, 18 und 19 des geplanten Abkommens sei streng geregelt, für welche Zwecke PNR-Daten verarbeitet und unter welchen Voraussetzungen sie weitergegeben werden dürften. Jedenfalls müsse jede Weitergabe von PNR-Daten nach Art. 17 des geplanten Abkommens protokolliert und dokumentiert und nachträglich durch eine unabhängige Behörde überprüft werden.

63 Die Dauer der Speicherung von PNR-Daten geht nach Auffassung der estnischen und der französischen Regierung, Irlands und der Regierung des Vereinigten Königreichs nicht über das hinaus, was im allgemeinen Kontext des geplanten Abkommens absolut notwendig sei. Ermittlungen im Bereich des Terrorismus und der grenzübergreifenden schweren Kriminalität seien komplex und schwierig. Zwischen der Reise eines Fluggasts, der an entsprechenden Straftaten beteiligt sei, und dem Zeitpunkt, zu dem die Strafverfolgungsbehörden Zugang zu den Fluggastdaten erhalten müssten, um solche Taten aufzudecken, zu untersuchen und strafrechtlich zu verfolgen, könne eine gewisse Zeit vergehen. Das Strafverfahren könne mitunter erst mehr als fünf Jahre nach der Weitergabe der PNR-Daten abgeschlossen werden. Zu berücksichtigen seien ferner die Vorschriften von Art. 16 des geplanten Abkommens, die für die Unkenntlichmachung der PNR-Daten und die Aufhebung ihrer Unkenntlichmachung zum besseren Schutz personenbezogener Daten strenge Modalitäten vorschrieben, und die Vorschriften von Art. 8 Abs. 5 des Abkommens, die eine Sonderregelung für sensible Daten enthielten.

64 Der Rat und die Kommission machen geltend, die Dauer der Speicherung von PNR-Daten müsse sich gemäß Art. 6 der Richtlinie 95/46 nach ihrer Erforderlichkeit für die Realisierung der Zwecke, für die sie erhoben würden, richten. Deshalb lasse sich die Verhältnismäßigkeit einer bestimmten Speicherdauer nicht abstrakt

beurteilen. Die Parteien des geplanten Abkommens seien davon ausgegangen, dass die darin vorgesehene Speicherdauer von fünf Jahren absolut notwendig sei, um die mit ihm verfolgten Ziele zu erreichen. Bei einer Dauer von dreieinhalb Jahren, wie sie im Abkommen von 2006 vorgesehen sei, hätten die PNR-Daten nach Auffassung Kanadas nicht wirksam genutzt werden können, um Sachverhalte aufzudecken, bei denen eine erhöhte Gefahr von Terrorismus oder organisiertem Verbrechen bestehe. Die Ermittlungen brauchten Zeit. Außerdem sei in Art. 16 Abs. 3 des geplanten Abkommens eine erste Unkenntlichmachung der PNR-Daten 30 Tage nach Erhalt und eine weitere zwei Jahre nach Erhalt vorgesehen.

65 Zur Überwachung der Einhaltung der Vorschriften über den Schutz personenbezogener Daten durch eine unabhängige Stelle, wie sie von Art. 8 Abs. 3 der Charta und Art. 16 Abs. 2 AEUV gefordert wird, machen der Rat und die Kommission geltend, die fehlende Nennung der zuständigen kanadischen Behörde im geplanten Abkommen ändere nichts daran, dass die von Kanada zu treffenden Maßnahmen angemessen seien. Im Übrigen sei der Kommission mitgeteilt worden, wer die zuständigen Behörden gemäß den Art. 10 und 14 des geplanten Abkommens seien.

66 Was die Beachtung der u. a. durch das Urteil vom 9. März 2010, Kommission/Deutschland (C-518/07, EU:C:2010:125, Rn. 30), begründeten Rechtsprechung des Gerichtshofs angeht, wonach die für die Überwachung zuständige Stelle mit einer Unabhängigkeit ausgestattet sein muss, die es ihr ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen, weist die Kommission darauf hin, dass der Privacy Commissioner of Canada eine sowohl institutionell als auch funktional unabhängige Stelle sei. In den Art. 10 und 14 des geplanten Abkommens habe die Einrichtung einer „durch administrative Mittel eingerichteten Stelle“ vorgesehen werden müssen, um zu garantieren, dass sämtliche möglicherweise betroffenen Personen ihre Rechte ausüben könnten, einschließlich des Rechts auf Auskunft, denn die kanadischen Rechtsvorschriften sähen für Ausländer, die sich nicht in Kanada aufhielten, kein solches Recht vor.

*VIII. Stellungnahme des Gerichtshofs*

67 Zunächst ist darauf hinzuweisen, dass nach ständiger Rechtsprechung des Gerichtshofs Bestimmungen einer internationalen Übereinkunft, die die Union gemäß den Art. 217 und 218 AEUV geschlossen hat, ab dem Inkrafttreten der Übereinkunft Bestandteil der Unionsrechtsordnung sind (vgl. in diesem Sinne Urteile vom 30. April 1974, Haegeman, 181/73, EU:C:1974:41, Rn. 5, und vom 11. März 2015, Oberto und O’Leary, C-464/13 und C-465/13, EU:C:2015:163, Rn. 29; Gutachten 2/13 [Beitritt der Union zur EMRK] vom 18. Dezember 2014, EU:C:2014:2454, Rn. 180). Sie müssen darum mit den Verträgen und den Verfassungsgrundsätzen, die sich aus ihnen ableiten lassen, im Einklang stehen.

A. **Zur Zulässigkeit des Gutachtenantrags**

68 Nach Art. 218 Abs. 11 AEUV können ein Mitgliedstaat, das Europäische Parlament, der Rat oder die Kommission ein Gutachten des Gerichtshofs über die Vereinbarkeit einer geplanten Übereinkunft mit den Verträgen einholen.

69 Nach ständiger Rechtsprechung des Gerichtshofs dient diese Bestimmung dazu, Komplikationen zu vermeiden, die entstehen könnten, wenn die Vereinbarkeit internationaler Übereinkünfte, die die Union verpflichten, mit den Verträgen vor Gericht bestritten würde. Eine gerichtliche Entscheidung, mit der eine die Union verpflichtende internationale Übereinkunft nach ihrem Abschluss wegen ihres Inhalts oder des Verfahrens ihres Zustandekommens für mit den Verträgen unvereinbar erklärt würde, würde nämlich nicht nur unionsintern, sondern auch auf dem Gebiet der internationalen Beziehungen zu ernsten Schwierigkeiten führen und könnte für alle Beteiligten einschließlich der Drittstaaten Nachteile mit sich bringen (Gutachten 2/13 [Beitritt der Union zur EMRK] vom 18. Dezember 2014, EU:C:2014:2454, Rn. 145 und 146 sowie die dort angeführte Rechtsprechung).

70 Demnach müssen im Rahmen des Verfahrens gemäß Art. 218 Abs. 11 AEUV alle Fragen zulässig sein, die Zweifel an der materiellen oder formellen Vereinbarkeit des Abkommens mit den Verträgen hervorrufen können. Die Beurteilung der Vereinbarkeit eines Abkommens mit den Verträgen kann insoweit nicht nur von den Vorschriften über die Zuständigkeit, das Verfahren oder das institutionelle Gefüge der Union, sondern auch von den Bestimmungen des materiellen Rechts abhängen (vgl. in diesem Sinne, in Bezug auf Art. 300 Abs. 6 EG, Gutachten 1/08 [Abkommen zur Änderung der Listen spezifischer Verpflichtungen nach dem GATS] vom 30. November 2009, EU:C:2009:739, Rn. 108 und die dort angeführte Rechtsprechung). Dasselbe gilt für eine Frage nach der Vereinbarkeit einer internationalen Übereinkunft mit Art. 6 Abs. 1 Unterabs. 1 EUV und folglich mit den Garantien der Charta, die den Verträgen rechtlich gleichrangig ist.

71 Zu der Frage der geeigneten Rechtsgrundlage für den Beschluss des Rates über den Abschluss des geplanten Abkommens ist festzustellen, dass die Wahl der geeigneten Rechtsgrundlage verfassungsrechtliche Bedeutung hat, da die Union, die nur über begrenzte Ermächtigungen verfügt, die Rechtsakte, die sie erlässt, mit einer Bestimmung des AEU-Vertrags verknüpfen muss, die sie tatsächlich hierzu ermächtigt (vgl. in diesem Sinne Urteil vom 1. Oktober 2009, Kommission/Rat, C-370/07, EU:C:2009:590, Rn. 47).

72 Die Wahl einer ungeeigneten Rechtsgrundlage kann somit den Abschlussakt selbst ungültig machen – ein Mangel, unter dem dann auch die Zustimmung der Union zu ihrer Bindung an die von ihr unterzeichnete Übereinkunft leidet.

73 Das Vorbringen der französischen Regierung und des Rates, dass sich die etwaige Wahl einer ungeeigneten Rechtsgrundlage im vorliegenden Fall weder auf die Zuständigkeit der Union für den Abschluss des geplanten Abkommens noch auf die Verteilung der Zuständigkeiten zwischen der Union und den Mitgliedstaaten in diesem Bereich oder auf das anzuwendende Verfahren auswirken würde, kann nicht dazu führen, dass die zweite Frage des Gutachtenantrags für unzulässig erklärt wird.

74 Das Verfahren gemäß Art. 218 Abs. 11 AEUV dient nämlich dazu, durch die vorherige Anrufung des Gerichtshofs Komplikationen zu vermeiden, die auf Unionsebene und auf internationaler Ebene entstehen könnten, wenn ein Rechtsakt, mit dem eine internationale Übereinkunft geschlossen wird, für ungültig erklärt würde (siehe oben, Rn. 69). Deshalb ist die Anrufung des Gerichtshofs schon dann zulässig, wenn die Gefahr einer solchen Ungültigerklärung besteht. Außerdem ist die Frage, welche tatsächlichen Auswirkungen die Wahl einer oder mehrerer ungeeigneter Rechtsgrundlagen in einem konkreten Fall auf die Gültigkeit eines Rechtsakts wie des Beschlusses des Rates über den Abschluss des geplanten Abkommens hat, mit dem eine internationale Übereinkunft geschlossen wird, untrennbar mit der Prüfung der materiellen Frage verbunden, welche Rechtsgrundlage geeignet ist. Sie kann daher nicht im Rahmen der Prüfung der Zulässigkeit eines Gutachtenantrags beurteilt werden.

75 Somit ist festzustellen, dass der vorliegende Gutachtenantrag insgesamt zulässig ist.

B. **Zur geeigneten Rechtsgrundlage des Beschlusses des Rates über den Abschluss des geplanten Abkommens**

76 Nach ständiger Rechtsprechung des Gerichtshofs muss sich die Wahl der Rechtsgrundlage eines Rechtsakts der Union – einschließlich eines Rechtsakts, der im Hinblick auf den Abschluss einer internationalen Übereinkunft erlassen wird – auf objektive, gerichtlich nachprüfbare Umstände gründen, wozu das Ziel und der Inhalt des Rechtsakts gehören (Urteile vom 6. Mai 2014, Kommission/Parlament und Rat, C-43/12, EU:C:2014:298, Rn. 29, und vom 14. Juni 2016, Parlament/Rat, C-263/14, EU:C:2016:435, Rn. 43 und die dort angeführte Rechtsprechung).

77 Ergibt die Prüfung eines Unionsrechtsakts, dass er zwei Zielsetzungen hat oder aus zwei Komponenten besteht, und lässt sich eine von ihnen als die hauptsächliche oder überwiegende ausmachen, während die andere nur nebensächliche Bedeutung hat, so ist der Rechtsakt nur auf eine Rechtsgrundlage zu stützen, und zwar auf die, die die hauptsächliche oder überwiegende Zielsetzung oder Komponente erfordert. Verfolgt eine Maßnahme dagegen mehrere Zielsetzungen zugleich oder besteht sie aus mehreren Komponenten, die untrennbar miteinander verbunden sind, ohne dass die eine gegenüber der anderen nebensächlich ist, so dass verschiedene Vertragsbestimmungen anwendbar sind, ist sie ausnahmsweise auf die entsprechenden verschiedenen Rechtsgrundlagen zu stützen (Urteil vom 14. Juni 2016, Parlament/Rat, C-263/14, EU:C:2016:435, Rn. 44 und die dort angeführte Rechtsprechung).

78 Der Rückgriff auf eine doppelte Rechtsgrundlage ist jedoch ausgeschlossen, wenn sich die für die beiden Rechtsgrundlagen jeweils vorgesehenen Verfahren nicht miteinander vereinbaren lassen (Urteil vom 6. November 2008, Parlament/Rat, C-155/07, EU:C:2008:605, Rn. 37 und die dort angeführte Rechtsprechung).

79 Die geeignete Rechtsgrundlage für den Beschluss des Rates über den Abschluss des geplanten Abkommens ist im Licht dieser Erwägungen zu bestimmen.

1. *Zu Ziel und Inhalt des geplanten Abkommens*

80 Mit dem geplanten Abkommen möchten die Vertragsparteien nach Abs. 3 seiner Präambel ihre Zusammenarbeit ausbauen und weiter voranbringen. Wie es hierzu in Art. 1 („Gegenstand des Abkommens“) des Abkommens heißt, „legen die Parteien fest, unter welchen Bedingungen [PNR-Daten] zur Gewährleistung der öffentlichen Sicherheit zu übermitteln und zu verwenden [sind] und wie sie geschützt werden“.

81 Zu dem in Art. 1 des geplanten Abkommens genannten Ziel des Schutzes der öffentlichen Sicherheit heißt es in Abs. 1 seiner Präambel u. a., dass die Parteien in dem Bemühen handeln, Terrorismus und Straftaten mit terroristischem Hintergrund sowie andere grenzübergreifende schwere Kriminalität zu verhindern, zu bekämpfen, zu unterbinden und zu beseitigen. Vor diesem Hintergrund wird in den Abs. 2 und 4 der Präambel die Bedeutung der Bekämpfung von Terrorismus und Straftaten mit terroristischem Hintergrund sowie anderer grenzübergreifender schwerer Kriminalität und der Verwendung der PNR-Daten und des Austauschs von Informationen hierzu hervorgehoben. Auf der Grundlage dieser Feststellungen heißt es dann in Abs. 5 der Präambel, dass zur Gewährleistung der öffentlichen Sicherheit und zu Strafverfolgungszwecken Regeln für die Übermittlung von PNR-Daten durch die Fluggesellschaften an Kanada festgelegt werden sollten. Schließlich wird in Abs. 16 der Präambel die Bedeutung unterstrichen, die dem Austausch von PNR-Daten und einschlägigen analytischen Informationen, die solche Daten enthalten, die Kanada von den zuständigen Polizei- und Justizbehörden der Mitgliedstaaten der Union, von Europol und von Eurojust erhalten hat, als Mittel zur Stärkung der internationalen polizeilichen und justiziellen Zusammenarbeit zukommt.

82 Mit dem geplanten Abkommen wird demnach das Ziel verfolgt, die öffentliche Sicherheit zu gewährleisten, indem PNR-Daten an Kanada übermittelt und im Rahmen der Bekämpfung terroristischer Straftaten und

grenzübergreifender schwerer Kriminalität verwendet werden, auch indem sie mit den zuständigen Behörden der Mitgliedstaaten der Union sowie mit Europol und Eurojust ausgetauscht werden.

83 Zum zweiten in Art. 1 des geplanten Abkommens genannten Ziel, nämlich der Festlegung, wie die PNR-Daten geschützt werden, wird in den Abs. 2, 6 und 7 der Präambel des geplanten Abkommens hervorgehoben, dass es erforderlich ist, im Einklang mit den Verpflichtungen der Union aus Art. 6 EUV die Grundrechte zu schützen, insbesondere das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten, die durch die Art. 7 und 8 der Charta garantiert sind, und dass die Parteien durch gemeinsame Werte in Bezug auf Datenschutz und Achtung der Privatsphäre verbunden sind.

84 Ferner geht aus Art. 5 des geplanten Abkommens hervor, dass die Rechtsvorschriften, die die zuständige kanadische Behörde bei der Verarbeitung der PNR-Daten zu beachten hat, das nach dem Unionsrecht gebotene angemessene Schutzniveau im Bereich des Schutzes personenbezogener Daten aufweisen sollen. Mit dem Abkommen wird demnach auch das Ziel verfolgt, ein solches Schutzniveau der Daten zu gewährleisten.

85 In Anbetracht dieser Erwägungen werden in Art. 1 des geplanten Abkommens ausdrücklich die beiden mit ihm verfolgten Ziele genannt.

86 Zum Inhalt des geplanten Abkommens ist festzustellen, dass sein erster Teil mit der Überschrift „Allgemeine Bestimmungen“ (Art. 1 bis 6) einen Art. 5 enthält, der vorsieht, dass vorbehaltlich der Einhaltung des Abkommens davon ausgegangen wird, dass die zuständige kanadische Behörde bei der Verarbeitung und Verwendung von PNR-Daten einen angemessenen Schutz im Sinne der einschlägigen Datenschutzvorschriften der Europäischen Union gewährleistet. Ferner wird davon ausgegangen, dass alle Fluggesellschaften, die Kanada auf der Grundlage des Abkommens PNR-Daten übermitteln, die unionsrechtlichen Anforderungen bezüglich der Übermittlung dieser Daten aus der Union an Kanada erfüllen. Der erste Teil des geplanten Abkommens enthält ferner einen Art. 4, dessen Abs. 1 vorsieht, dass die Union dafür sorgt, dass die Fluggesellschaften nicht daran gehindert werden, der zuständigen kanadischen Behörde PNR-Daten zu übermitteln, wobei diese Behörde nach Art. 2 Buchst. d des Abkommens für den Erhalt und die Verarbeitung der Daten verantwortlich ist. Art. 3 des Abkommens, in dem geregelt ist, zu welchen Zwecken die Verarbeitung der PNR-Daten durch die zuständige kanadische Behörde zulässig ist, sieht in Abs. 1 vor, dass die Verarbeitung nur zum Zweck der Verhinderung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität zulässig ist, wobei in den Abs. 4 und 5 begrenzte Ausnahmen von diesem Grundsatz vorgesehen sind. Art. 6 des Abkommens sieht schließlich vor, dass PNR-Daten und sachdienliche analytische Informationen, die solche Daten enthalten, mit den zuständigen Polizei- oder Justizbehörden der Mitgliedstaaten, Europol und Eurojust im Einklang mit den Abkommen und unter Vereinbarungen auf dem Gebiet der Strafverfolgung oder des Informationsaustauschs ausgetauscht werden.

87 Der zweite Teil des geplanten Abkommens mit der Überschrift „Garantien für die Verarbeitung von PNR-Daten“ (Art. 7 bis 21) enthält die Vorschriften und Grundsätze, die die Verwendung der PNR-Daten in Kanada durch die zuständige kanadische Behörde und die Weitergabe der Daten an andere Behörden dieses Drittlands und an Behörden in anderen Drittländern regeln und begrenzen. Dabei enthält Art. 7 eine Nichtdiskriminierungsklausel und Art. 8 eine besondere Vorschrift für sensible Daten, in der u. a. die Voraussetzungen, unter denen die Verwendung solcher Daten zulässig ist, abschließend geregelt sind. Der zweite Teil des Abkommens enthält in den Art. 9 und 10 zudem Vorschriften über die Sicherheit und Integrität der PNR-Daten sowie die Beaufsichtigung der Einhaltung der Garantien des Abkommens. Die Art. 11 bis 14 des Abkommens enthalten eine Vorschrift über die Transparenz und legen die Rechte von Personen fest, deren PNR-Daten betroffen sind, etwa das Recht auf Zugang zu den Daten, das Recht auf Berichtigung oder das Recht auf einen Rechtsbehelf.

88 Der zweite Teil des geplanten Abkommens enthält außerdem einen Art. 15, wonach Kanada Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten treffen darf, und einen Art. 16, in dem u. a. die Dauer der Speicherung von PNR-Daten, ihre Unkenntlichmachung und die Aufhebung der Unkenntlichmachung geregelt sind. Ferner sind in den Art. 18 und 19 die Weitergabe der PNR-Daten durch die zuständige kanadische Behörde und in den Art. 20 und 21 das Verfahren und die Häufigkeit der Übermittlung von PNR-Daten geregelt.

89 Aus den verschiedenen Feststellungen zum Inhalt des geplanten Abkommens geht somit hervor, dass sein Gegenstand insbesondere die Schaffung eines Systems ist, das aus einer Gesamtheit von Regeln zum Schutz personenbezogener Daten besteht. Zu dessen Einhaltung bei der Verarbeitung der PNR-Daten hat sich Kanada verpflichtet, wie Abs. 15 der Präambel des Abkommens zu entnehmen ist.

90 Nach seinen Zielen und seinem Inhalt hat das geplante Abkommen demnach zwei Komponenten. Die eine betrifft die Erforderlichkeit der Gewährleistung der öffentlichen Sicherheit, die andere den Schutz personenbezogener Daten.

91 Zu der Frage, welche dieser beiden Komponenten überwiegt, ist festzustellen, dass die Übermittlung von PNR-Daten durch die Fluggesellschaften an Kanada und die Verwendung dieser Daten durch die zuständige kanadische Behörde als solche zwar nur durch das Ziel gerechtfertigt werden können, die öffentliche Sicherheit in diesem Drittland und in der Union zu gewährleisten.

92 Inhaltlich besteht das geplante Abkommen aber zu einem großen Teil aus detaillierten Regeln, mit denen gewährleistet wird, dass die Bedingungen, unter denen die Übermittlung von PNR-Daten an Kanada für die

Verwendung zu Zwecken des Schutzes der öffentlichen Sicherheit erfolgt, mit dem Schutz personenbezogener Daten im Einklang stehen.

93 Die Übermittlung personenbezogener Daten wie der PNR-Daten aus der Union in ein Drittland ist nämlich nur zulässig, wenn es dort Regeln gibt, die ein Schutzniveau der Grundfreiheiten und Grundrechte gewährleisten, das dem in der Union garantierten der Sache nach gleichwertig ist (vgl. in diesem Sinne Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 68 und 74).

94 Die beiden Komponenten des geplanten Abkommens sind also untrennbar miteinander verbunden, so dass beide als wesentlich anzusehen sind.

2. *Zur geeigneten Rechtsgrundlage nach dem AEU-Vertrag*

95 In Anbetracht der vorstehenden Erwägungen ist der Beschluss über den Abschluss des geplanten Abkommens als Erstes unmittelbar dem mit Art. 16 Abs. 2 AEUV verfolgten Ziel zuzuordnen.

96 Unbeschadet des Art. 39 EUV stellt diese Vorschrift nämlich eine geeignete Rechtsgrundlage dar, wenn der Schutz personenbezogener Daten eines der wesentlichen Ziele oder Komponenten der vom Unionsgesetzgeber erlassenen Regeln ist. Das gilt auch für Regeln im Rahmen des Erlasses von Maßnahmen, die unter die Bestimmungen des AEU-Vertrags über die justizielle Zusammenarbeit in Strafsachen und die polizeiliche Zusammenarbeit fallen, wie Art. 6a des Protokolls Nr. 21 und Art. 2a des Protokolls Nr. 22 sowie die in Rn. 32 angeführte Erklärung bestätigen.

97 Der Beschluss des Rates über den Abschluss des geplanten Abkommens ist mithin auf Art. 16 AEUV zu stützen.

98 Als Zweites ist der Beschluss auch auf Art. 87 Abs. 2 Buchst. a AEUV zu stützen. Diese Vorschrift sieht nämlich vor, dass das Europäische Parlament und der Rat für die Zwecke von Art. 87 Abs. 1 AEUV – wonach die Union „eine polizeiliche Zusammenarbeit zwischen allen zuständigen Behörden der Mitgliedstaaten [entwickelt]“ – Maßnahmen erlassen können, die das „Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen“ betreffen.

99 Unter den Begriff der sachdienlichen Informationen im Sinne von Art. 87 Abs. 2 Buchst. a AEUV können in den Bereichen der Verhütung oder Aufdeckung von Straftaten sowie entsprechender Ermittlungen personenbezogene Daten fallen, unter die Begriffe „Verarbeiten“ und „Austauschen“ solcher Daten sowohl ihre Weitergabe an die Behörden der zuständigen Mitgliedstaaten als auch die Verwendung der Daten durch diese Behörden. Maßnahmen, die die Übermittlung personenbezogener Daten an die zuständigen Behörden in den Bereichen der Verhütung oder Aufdeckung von Straftaten sowie entsprechender Ermittlungen und die Verarbeitung der Daten durch diese Behörden betreffen, gehören mithin zur polizeilichen Zusammenarbeit im Sinne von Art. 87 Abs. 2 Buchst. a AEUV und können auf diese Vorschrift gestützt werden.

100 Im vorliegenden Fall werden durch das geplante Abkommen u. a. die Übermittlung der PNR-Daten an die zuständige kanadische Behörde und die Verwendung der Daten durch diese Behörde geregelt. Nach Art. 2 Buchst. d des geplanten Abkommens in Verbindung mit dessen Art. 3 Abs. 1 ist diese Behörde für die Verarbeitung der PNR-Daten zum Zweck der Verhinderung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität zuständig. Art. 6 des Abkommens sieht zudem vor, dass Kanada sachdienliche analytische Informationen, die PNR-Daten enthalten, zum frühestmöglichen Zeitpunkt mit Europol und Eurojust sowie mit den Polizei- oder Justizbehörden eines Mitgliedstaats austauscht und in konkreten Fällen auf Ersuchen dieser Behörden PNR-Daten oder analytische Informationen, die PNR-Daten enthalten, austauscht, um eine terroristische Straftat oder grenzübergreifende schwere Kriminalität in der Union zu verhindern, aufzudecken, zu untersuchen oder strafrechtlich zu verfolgen. Wie der Generalanwalt in den Nrn. 105 und 106 seiner Schlussanträge ausgeführt hat, ist Gegenstand des geplanten Abkommens demnach das Verarbeiten und Austauschen sachdienlicher Informationen im Sinne von Art. 87 Abs. 2 Buchst. a AEUV, so dass es auch dem Zweck von Art. 87 Abs. 1 AEUV zuzuordnen ist (siehe insbesondere oben, Rn. 80).

101 Der Umstand, dass die PNR-Daten ursprünglich von Fluggesellschaften für gewerbliche Zwecke erhoben wurden und nicht durch eine zuständige Behörde zur Verhütung oder Aufdeckung von Straftaten sowie zu entsprechenden Ermittlungen, steht daher, anders als das Parlament geltend macht, der Heranziehung von Art. 87 Abs. 2 Buchst. a AEUV als geeignete Rechtsgrundlage für den Beschluss des Rates über den Abschluss des geplanten Abkommens nicht entgegen.

102 Hingegen kann der Beschluss nicht auf Art. 82 Abs. 1 Unterabs. 2 Buchst. d AEUV gestützt werden, wonach das Parlament und der Rat Maßnahmen erlassen dürfen, um „die Zusammenarbeit zwischen den Justizbehörden oder entsprechenden Behörden der Mitgliedstaaten im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen zu erleichtern“.

103 Wie der Generalanwalt in Nr. 108 seiner Schlussanträge ausgeführt hat, dient nämlich keine Bestimmung des geplanten Abkommens dazu, eine solche Zusammenarbeit zu erleichtern. Außerdem stellt die zuständige kanadische Behörde weder eine Justizbehörde noch eine entsprechende Behörde dar.

104 Somit ist in Anbetracht der in Rn. 77 angeführten Rechtsprechung festzustellen, dass der Beschluss des Rates über den Abschluss des geplanten Abkommens sowohl auf Art. 16 Abs. 2 als auch auf Art. 87 Abs. 2 Buchst. a AEUV gestützt werden müsste, sofern eine solche Kombination von Rechtsgrundlagen nicht nach der in Rn. 78 angeführten Rechtsprechung ausgeschlossen ist.

3. *Zur Vereinbarkeit der Verfahren gemäß Art. 16 Abs. 2 und Art. 87 Abs. 2 Buchst. a AEUV*

105 Zunächst ist darauf hinzuweisen, dass im Rahmen des Verfahrens zum Abschluss einer internationalen Übereinkunft nach Art. 218 AEUV die materiellen Rechtsgrundlagen des Beschlusses über den Abschluss der Übereinkunft die Art des Verfahrens bestimmen, das nach Art. 218 Abs. 6 AEUV Anwendung findet (Urteil vom 24. Juni 2014, Parlament/Rat, C-658/11, EU:C:2014:2025, Rn. 58).
106 Die beiden hier einschlägigen materiellen Rechtsgrundlagen, Art. 16 Abs. 2 und Art. 87 Abs. 2 Buchst. a AEUV, sehen das ordentliche Gesetzgebungsverfahren vor, das die Abstimmung mit qualifizierter Mehrheit im Rat und die volle Beteiligung des Parlaments am Verfahren verlangt. Der gemeinsame Rückgriff auf beide Vorschriften führt also grundsätzlich nicht zu verschiedenen Rechtsetzungsverfahren.
107 Der Rat macht jedoch im Wesentlichen geltend, wegen der in den Protokollen Nrn. 21 und 22 enthaltenen Vorschriften unterschieden sich die Regeln über die Abstimmung im Rat, je nachdem, ob der Beschluss über den Abschluss einer internationalen Übereinkunft auf Art. 16 Abs. 2 oder auf Art. 87 Abs. 2 Buchst. a AEUV gestützt werde.
108 Insoweit hat der Gerichtshof zwar bereits entschieden, dass die Protokolle Nrn. 21 und 22 keine wie auch immer gearteten Auswirkungen auf die Frage der geeigneten Rechtsgrundlage für den Erlass des betreffenden Beschlusses haben können (vgl. in diesem Sinne Urteil vom 22. Oktober 2013, Kommission/Rat, C-137/12, EU:C:2013:675, Rn. 73).
109 Da ein Unterschied bei den Regeln über die Abstimmung im Rat aber zur Unvereinbarkeit der fraglichen Rechtsgrundlagen führen kann (vgl. in diesem Sinne Urteile vom 10. Januar 2006, Kommission/Parlament und Rat, C-178/03, EU:C:2006:4, Rn. 58, und vom 19. Juli 2012, Parlament/Rat, C-130/10, EU:C:2012:472, Rn. 47 und 48), ist zu prüfen, welche Auswirkungen die genannten Protokolle auf die Abstimmungsregeln im Rat haben, wenn der Beschluss des Rates über den Abschluss des geplanten Abkommens auf Art. 16 Abs. 2 gemeinsam mit Art. 87 Abs. 2 Buchst. a AEUV gestützt wird.
110 Zum Protokoll Nr. 21 geht aus dem fünften Erwägungsgrund des Vorschlags für einen Beschluss des Rates über den Abschluss des geplanten Abkommens hervor, dass Irland und das Vereinigte Königreich mitgeteilt haben, dass sie sich an dem Beschluss beteiligen wollen. Wie der Generalanwalt in Nr. 128 seiner Schlussanträge ausgeführt hat, haben die Vorschriften des Protokolls Nr. 21 daher keine Auswirkungen auf die Abstimmungsregeln im Rat, wenn der Beschluss auf Art. 16 Abs. 2 gemeinsam mit Art. 87 Abs. 2 Buchst. a AEUV gestützt wird.
111 Mit dem Protokoll Nr. 22 soll, wie sich aus den Abs. 3 bis 5 seiner Präambel ergibt und wie der Generalanwalt in Nr. 132 seiner Schlussanträge ausgeführt hat, ein Rechtsrahmen festgelegt werden, der es den Mitgliedstaaten ermöglicht, ihre Zusammenarbeit im Bereich des Raums der Freiheit, der Sicherheit und des Rechts durch den Erlass von Maßnahmen ohne Beteiligung des Königreichs Dänemark, die für diesen Mitgliedstaat nicht bindend sind, weiter auszubauen, und dem Königreich Dänemark gleichzeitig die Option bietet, sich am Erlass von Maßnahmen in diesem Bereich zu beteiligen und an sie unter den Bedingungen von Art. 8 des Protokolls gebunden zu sein.
112 Hierzu heißt es in Art. 1 Abs. 1 des Protokolls Nr. 22, dass sich das Königreich Dänemark nicht an der Annahme von Maßnahmen durch den Rat beteiligt, die nach dem Dritten Teil Titel V des AEU-Vertrags vorgeschlagen werden. Außerdem sieht Art. 2 des Protokolls vor, dass solche Maßnahmen für das Königreich Dänemark nicht bindend sind. Nach Art. 2a des Protokolls gilt dessen Art. 2 „auch für die auf der Grundlage des Artikels 16 [AEUV] festgelegten Vorschriften über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 des genannten Vertrags fallen“, also zur polizeilichen Zusammenarbeit und justiziellen Zusammenarbeit in Strafsachen gehören.
113 Im vorliegenden Fall ist der Beschluss über den Abschluss des geplanten Abkommens sowohl auf Art. 16 als auch auf Art. 87 AEUV zu stützen. Soweit er auf Art. 87 AEUV zu stützen ist, fällt er also unter den Dritten Teil Titel V Kapitel 5 des AEU-Vertrags. Nach den Art. 2 und 2a des Protokolls Nr. 22 sind für das Königreich Dänemark deshalb weder die Bestimmungen des Beschlusses noch das geplante Abkommen bindend. Außerdem wird sich das Königreich Dänemark nach Art. 1 des Protokolls Nr. 22 nicht am Erlass des Beschlusses beteiligen.
114 Anders als der Rat offenbar meint, wird diese Feststellung nicht dadurch entkräftet, dass in Art. 2a des Protokolls Nr. 22 lediglich auf dessen Art. 2 verwiesen wird, ohne dass ausdrücklich ausgeschlossen wird, dass sich das Königreich Dänemark am Erlass der dort genannten, auf Art. 16 AEUV gestützten Vorschriften beteiligt.
115 Nach der Systematik des Protokolls Nr. 22 kann dessen Art. 2 nämlich nicht unabhängig von Art. 1 verstanden und angewandt werden. Die in Art. 2 enthaltene Regel, dass die dort genannten Maßnahmen, Vorschriften und Entscheidungen für das Königreich Dänemark nicht bindend sind, ist ihrem Wesen nach verbunden mit der in Art. 1 enthaltenen Regel, dass sich das Königreich Dänemark nicht an der Annahme von Maßnahmen nach dem Dritten Teil Titel V des AEU-Vertrags beteiligt. Die beiden Regeln können also nicht unabhängig voneinander verstanden werden. Der Verweis in Art. 2a des Protokolls Nr. 22 auf dessen Art. 2 ist deshalb zwingend dahin auszulegen, dass er auch Art. 1 des Protokolls umfasst.
116 Würde dem Königreich Dänemark gestattet, sich am Erlass eines Unionsrechtsakts zu beteiligen, dessen Rechtsgrundlage sowohl Art. 16 AEUV als auch eine der Bestimmungen des AEU-Vertrags über die polizeiliche

Zusammenarbeit und die justizielle Zusammenarbeit in Strafsachen ist, ohne dass der Rechtsakt für das Königreich Dänemark bindend wäre, liefe dies im Übrigen dem Ziel des Protokolls Nr. 22 (siehe oben, Rn. 111) zuwider, wie der Generalanwalt in Nr. 132 seiner Schlussanträge ausgeführt hat.

117 Das Protokoll Nr. 22 kann somit im vorliegenden Fall bei gemeinsamem Rückgriff auf Art. 16 Abs. 2 und Art. 87 Abs. 2 Buchst. a AEUV nicht zu unterschiedlichen Abstimmungsregeln im Rat führen.

118 Daher ist auf die zweite Frage des vorliegenden Gutachtenantrags zu antworten, dass der Beschluss des Rates über den Abschluss des geplanten Abkommens auf Art. 16 Abs. 2 gemeinsam mit Art. 87 Abs. 2 Buchst. a AEUV zu stützen ist.

## C. **Zur Vereinbarkeit des geplanten Abkommens mit den Vorschriften des AEU-Vertrags und der Charta**

119 Da bei der Frage nach der Vereinbarkeit des geplanten Abkommens mit den Vorschriften des AEU-Vertrags und der Charta auf Art. 16 AEUV und auf die Art. 7 und 8 der Charta Bezug genommen wird, ist im Licht der Ausführungen des Parlaments im Gutachtenantrag davon auszugehen, dass es ein Gutachten des Gerichtshofs über die Vereinbarkeit des geplanten Abkommens insbesondere mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten begehrt.

120 Soweit sich die folgenden Ausführungen auf die Vereinbarkeit des geplanten Abkommens mit dem Recht auf Schutz personenbezogener Daten beziehen, das sowohl in Art. 16 Abs. 1 AEUV als auch in Art. 8 der Charta niedergelegt ist, wird lediglich auf Art. 8 der Charta Bezug genommen. Zwar heißt es in beiden Bestimmungen, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Die Voraussetzungen, unter denen solche Daten verarbeitet werden dürfen, sind aber allein in Art. 8 der Charta, und zwar in dessen Abs. 2, näher geregelt.

### 1. *Zu den betroffenen Grundrechten und den Eingriffen in sie*

121 Nach der Aufzählung im Anhang des geplanten Abkommens gehören zu den PNR-Daten, auf die sich das Abkommen bezieht, außer dem Namen des Fluggasts bzw. der Fluggäste u. a. Informationen, die für die Reservierung erforderlich sind, wie die Daten des geplanten Flugs und die Reiseroute, Flugscheininformationen, Gruppen von Personen, die unter derselben Reservierungsnummer registriert sind, die Kontaktangaben des Fluggasts bzw. der Fluggäste, Zahlungs- oder Abrechnungsinformationen, Informationen zum Gepäck und allgemeine Eintragungen über die Fluggäste.

122 Die PNR-Daten enthalten also Informationen über bestimmte natürliche Personen, und zwar die Fluggäste, die aus der Union nach Kanada reisen. Die verschiedenen Verarbeitungen, die mit den PNR-Daten nach dem geplanten Abkommen vorgenommen werden können, nämlich ihre Übermittlung von der Union an Kanada, der Zugang zu den Daten zu ihrer Verwendung oder ihre Speicherung, berühren das Grundrecht auf Achtung des Privatlebens, das in Art. 7 der Charta garantiert ist. Denn dieses Recht erstreckt sich auf jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft (vgl. in diesem Sinne Urteile vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 52, vom 24. November 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 und C-469/10, EU:C:2011:777, Rn. 42, und vom 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 26).

123 Die im geplanten Abkommen vorgesehenen Verarbeitungen der PNR-Daten fallen zudem unter Art. 8 der Charta, weil sie Verarbeitungen personenbezogener Daten im Sinne dieses Artikels darstellen und deshalb zwangsläufig die dort vorgesehenen Erfordernisse des Datenschutzes erfüllen müssen (vgl. in diesem Sinne Urteile vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 49, vom 5. Mai 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, Rn. 52, und vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 29).

124 Wie der Gerichtshof bereits entschieden hat, stellt die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht dar. Dasselbe gilt für die Speicherung personenbezogener Daten und den Zugang zu den Daten zu ihrer Verwendung durch die Behörden. Für die Feststellung eines solchen Eingriffs kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben (vgl. in diesem Sinne Urteile vom 20. Mai 2003, Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 74 und 75, vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 33 bis 35, und vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 87).

125 Somit stellen sowohl die Übermittlung der PNR-Daten von der Union an die zuständige kanadische Behörde als auch die von der Union mit Kanada ausgehandelte Regelung der Bedingungen, unter denen die Daten gespeichert, verwendet und eventuell an andere kanadische Behörden, Europol, Eurojust, gerichtliche oder Polizeibehörden der Mitgliedstaaten oder Behörden weiterer Drittländer weitergegeben werden können, wie es u. a. die Art. 3, 4, 6, 8, 12, 15, 16, 18 und 19 des geplanten Abkommens gestatten, Eingriffe in das durch Art. 7 der Charta garantierte Grundrecht dar.

126 Diese Vorgänge stellen, weil es sich bei ihnen um Verarbeitungen personenbezogener Daten handelt, auch einen Eingriff in das durch Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar (vgl. in diesem Sinne Urteile vom 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 25, und vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 36).

127 Insoweit ist zum einen festzustellen, dass das geplante Abkommen die systematische und kontinuierliche Übermittlung der PNR-Daten sämtlicher Fluggäste ermöglicht, die aus der Union nach Kanada reisen.
128 Zum anderen können die PNR-Daten, auch wenn einige von ihnen für sich genommen nicht geeignet sein dürften, bedeutsame Informationen über das Privatleben der betreffenden Personen zu liefern, zusammen betrachtet u. a. einen gesamten Reiseverlauf, Reisegewohnheiten, Beziehungen zwischen zwei oder mehreren Personen sowie Informationen über die finanzielle Situation der Fluggäste, ihre Ernährungsgewohnheiten oder ihren Gesundheitszustand offenbaren und sogar sensible Daten über die Fluggäste im Sinne von Art. 2 Buchst. e des geplanten Abkommens liefern.
129 Die Merkmale, die der im geplanten Abkommen vorgesehenen Regelung der Übermittlung und Verarbeitung von PNR-Daten inhärent sind, bestätigen, dass das Abkommen Eingriffe von realer Bedeutung zulässt.
130 Nach Art. 21 Abs. 1 des geplanten Abkommens sind die Daten nämlich vor dem planmäßigen Abflug des betreffenden Fluggasts zu übermitteln. Wie sich insbesondere aus den Stellungnahmen des Rates, der Kommission und des EDSB sowie aus Abschnitt 2.1 der Mitteilung KOM(2010) 492 ergibt, werden sie vor allem zur „Erkenntnisgewinnung“ verwendet.
131 Wie aus Abschnitt 2.2 dieser Mitteilung hervorgeht und wie insbesondere das Parlament, der Rat, die Kommission und der EDSB in ihren Antworten auf Fragen des Gerichtshofs bestätigt haben, sind die übermittelten PNR-Daten nach dem geplanten Abkommen dazu bestimmt, vor der Ankunft des Flugzeugs in Kanada durch automatisierte Verfahren systematisch analysiert zu werden, die auf im Voraus festgelegten Modellen und Kriterien beruhen. Die Daten können auch automatisiert überprüft werden, indem sie mit anderen Datenbanken abgeglichen werden. Durch solche Verarbeitungen können weitere Informationen über das Privatleben der Fluggäste erlangt werden.
132 Diese Analysen können zudem bei Fluggästen, bei denen davon ausgegangen wird, dass von ihnen eine Gefahr für die öffentliche Sicherheit ausgehen könnte, Anlass zu weiteren Überprüfungen an der Grenze geben sowie auf deren Grundlage gegebenenfalls zu individuellen Entscheidungen mit Zwangswirkung führen. Die Analysen werden zudem durchgeführt, ohne dass konkrete Anhaltspunkte dafür vorliegen, dass von den betreffenden Personen eine Gefahr für die öffentliche Sicherheit ausgehen könnte. Schließlich ermöglicht es die Dauer der Speicherung der PNR-Daten, die nach Art. 16 Abs. 1 des geplanten Abkommens bis zu fünf Jahre betragen kann, während eines besonders langen Zeitraums über Informationen über das Privatleben der Fluggäste zu verfügen.
2. *Zur Rechtfertigung der mit dem geplanten Abkommen verbundenen Eingriffe*
133 Nach Art. 7 der Charta hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Darüber hinaus gewährt Art. 8 Abs. 1 der Charta jeder Person ausdrücklich das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
134 Das Recht auf Schutz personenbezogener Daten verlangt u. a., dass im Fall der Übermittlung personenbezogener Daten aus der Union in ein Drittland der Fortbestand des durch das Unionsrecht gewährten hohen Niveaus des Schutzes der Grundfreiheiten und Grundrechte gewährleistet wird. Auch wenn sich die Mittel zur Gewährleistung eines solchen Schutzniveaus von denen unterscheiden können, die in der Union herangezogen werden, um die Wahrung der Anforderungen, die sich aus dem Unionsrecht ergeben, zu gewährleisten, müssen sie sich gleichwohl in der Praxis als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten der Sache nach gleichwertig ist (vgl. entsprechend Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 72 bis 74).
135 In diesem Kontext ist ferner festzustellen, dass es nach Abs. 4 der Präambel der Charta „angesichts der Weiterentwicklung der Gesellschaft, des sozialen Fortschritts und der wissenschaftlichen und technologischen Entwicklungen“ notwendig ist, „den Schutz der Grundrechte zu stärken“.
136 Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (vgl. in diesem Sinne Urteile vom 12. Juni 2003, Schmidberger, C-112/00, EU:C:2003:333, Rn. 80, vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 48, und vom 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 33).
137 Insoweit ist auch darauf hinzuweisen, dass nach Art. 8 Abs. 2 der Charta personenbezogene Daten nur „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ verarbeitet werden dürfen.
138 Überdies muss nach Art. 52 Abs. 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten (Satz 1); unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Satz 2).
139 Hinzuzufügen ist, dass das Erfordernis, dass jede Einschränkung der Ausübung der Grundrechte gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss (vgl. in diesem Sinne Urteil vom 17. Dezember 2015, WebMindLicenses, C-419/14, EU:C:2015:832, Rn. 81).

140 Zum Grundsatz der Verhältnismäßigkeit ist festzustellen, dass der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken (Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56, vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 51 und 52, vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92, und vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 96 und 103).

141 Um diesem Erfordernis zu genügen, muss die betreffende Regelung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden. Dies gilt insbesondere, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55, sowie vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 109 und 117; vgl. in diesem Sinne EGMR, 4. Dezember 2008, S. und Marper/Vereinigtes Königreich, CE:ECHR:2008:1204JUD003056204, § 103).

a) *Zur Grundlage der im geplanten Abkommen vorgesehenen Verarbeitungen von PNR-Daten*

142 Zu der Frage, ob die Übermittlung der PNR-Daten an Kanada und ihre spätere Verarbeitung mit „Einwilligung“ der Fluggäste erfolgen oder auf „einer sonstigen gesetzlich geregelten legitimen Grundlage“ im Sinne von Art. 8 Abs. 2 der Charta beruhen, ist festzustellen, dass mit solchen Verarbeitungen der PNR-Daten ein anderer Zweck verfolgt wird als der, für den die Daten von den Fluggesellschaften erhoben wurden.

143 Deshalb kann nicht davon ausgegangen werden, dass sich die Einwilligung der Fluggäste zur Erhebung der PNR-Daten durch die Fluggesellschaften zum Zweck der Reservierung auf solche Verarbeitungen erstreckt. Die Verarbeitungen erfordern daher als solche eine spezielle Einwilligung der Fluggäste oder eine sonstige gesetzlich geregelte legitime Grundlage.

144 Da keine Bestimmung des geplanten Abkommens die Übermittlung der PNR-Daten an Kanada und ihre anschließende Verarbeitung von der Einwilligung der betroffenen Fluggäste abhängig macht, ist zu prüfen, ob das Abkommen eine sonstige gesetzlich geregelte legitime Grundlage im Sinne von Art. 8 Abs. 2 der Charta darstellt.

145 Insoweit kann das Argument des Parlaments, das geplante Abkommen falle, da es keinen „Gesetzgebungsakt“ darstelle, nicht unter den Begriff des Gesetzes im Sinne von Art. 8 Abs. 2 der Charta und somit von Art. 52 Abs. 1 der Charta, jedenfalls keinen Erfolg haben.

146 Art. 218 Abs. 6 AEUV spiegelt nämlich auf internationaler Ebene die Verteilung der Befugnisse der Organe bei interner Rechtsetzung wider und stellt eine Symmetrie zwischen dem internen Rechtsetzungsverfahren bei Unionsmaßnahmen und dem Verfahren zum Erlass internationaler Übereinkünfte her, um zu gewährleisten, dass das Parlament und der Rat im Zusammenhang mit einem bestimmten Bereich unter Wahrung des durch die Verträge vorgesehenen institutionellen Gleichgewichts die gleichen Befugnisse haben (Urteil vom 24. Juni 2014, Parlament/Rat, C-658/11, EU:C:2014:2025, Rn. 56). Deshalb ist für den Abschluss von internationalen Übereinkünften, die Bereiche betreffen, in denen im internen Rechtsetzungsverfahren das in Art. 294 AEUV vorgesehene ordentliche Gesetzgebungsverfahren Anwendung findet, nach Art. 218 Abs. 6 Buchst. a Ziff. v AEUV die Zustimmung des Parlaments erforderlich. Wie der Generalanwalt in Nr. 192 seiner Schlussanträge ausgeführt hat, kann eine solche Übereinkunft daher als das Äquivalent auf internationaler Ebene eines Gesetzgebungsakts im internen Rechtsetzungsverfahren angesehen werden. Im Übrigen ist im vorliegenden Verfahren von keiner Seite behauptet worden, dass das geplante Abkommen die Voraussetzungen der Zugänglichkeit und der Vorhersehbarkeit, die vorliegen müssen, damit die Eingriffe, die mit ihm verbunden sind, als im Sinne von Art. 8 Abs. 2 und Art. 52 Abs. 1 der Charta gesetzlich vorgesehen eingestuft werden können, nicht erfüllen könnte.

147 Somit ist festzustellen, dass die Übermittlung der PNR-Daten an Kanada auf einer „sonstigen gesetzlich geregelten … Grundlage“ im Sinne von Art. 8 Abs. 2 der Charta beruht. Die Frage, ob diese Grundlage legitim im Sinne dieser Bestimmung ist, überschneidet sich im vorliegenden Fall mit der in den Rn. 148 ff. des vorliegenden Gutachtens untersuchten Frage, ob das mit dem geplanten Abkommen verfolgte Ziel dem Gemeinwohl dient.

b) *Zur dem Gemeinwohl dienenden Zielsetzung und zur Achtung des Wesensgehalts der betreffenden Grundrechte*

148 Mit dem geplanten Abkommen wird u. a. das Ziel verfolgt, die öffentliche Sicherheit zu gewährleisten, indem PNR-Daten an Kanada übermittelt und im Rahmen der Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität verwendet werden (siehe oben, Rn. 82).

149 Nach der Rechtsprechung des Gerichtshofs stellt dieses Ziel eine dem Gemeinwohl dienende Zielsetzung der Union dar, die auch schwere Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte

rechtfertigen kann. Darüber hinaus trägt der Schutz der öffentlichen Sicherheit auch zum Schutz der Rechte und Freiheiten anderer bei. Insoweit ist festzustellen, dass nach Art. 6 der Charta jeder Mensch das Recht nicht nur auf Freiheit, sondern auch auf Sicherheit hat (vgl. in diesem Sinne Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 42 und 44, sowie vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 53).

150 Zum Wesensgehalt des in Art. 7 der Charta niedergelegten Grundrechts auf Achtung des Privatlebens ist festzustellen, dass die PNR-Daten zwar unter Umständen sehr genaue Informationen über das Privatleben einer Person liefern können, doch ist die Art dieser Informationen auf bestimmte Aspekte dieses Privatlebens beschränkt, die insbesondere Flugreisen zwischen Kanada und der Union betreffen. Zum Wesensgehalt des in Art. 8 der Charta niedergelegten Rechts auf Schutz personenbezogener Daten ist festzustellen, dass die Zwecke der Verarbeitung der PNR-Daten in Art. 3 des geplanten Abkommens begrenzt werden und dass sein Art. 9 Regeln enthält, mit denen u. a. die Sicherheit, die Vertraulichkeit und die Integrität dieser Daten gewährleistet und die Daten vor unbefugten Zugriffen und unrechtmäßiger Verarbeitung geschützt werden sollen.

151 Unter diesen Umständen haben die Eingriffe, die mit dem geplanten Abkommen verbunden sind, eine dem Gemeinwohl dienende Zielsetzung der Union und sind nicht geeignet, den Wesensgehalt der in den Art. 7 und 8 der Charta niedergelegten Grundrechte zu beeinträchtigen.

c) *Zur Eignung der im geplanten Abkommen vorgesehenen Verarbeitungen von PNR-Daten für die Verwirklichung des Ziels der Gewährleistung der öffentlichen Sicherheit*

152 Zu der Frage, ob die Übermittlung der PNR-Daten an Kanada und ihre anschließende Verarbeitung in diesem Drittstaat geeignet sind, die öffentliche Sicherheit zu gewährleisten, ergibt sich aus Abschnitt 2.2 der Mitteilung KOM(2010) 492, dass aufgrund der Bewertung der von den Fluggästen ausgehenden Risiken durch die Analyse dieser Daten vor Ankunft der Fluggäste „die Sicherheits- und Grenzkontrollen … wesentlich erleichtert und beschleunigt [werden]“. Außerdem hat die Kommission in ihren schriftlichen Erklärungen darauf hingewiesen, dass die Verarbeitung der PNR-Daten nach den Angaben der CBSA u. a. dazu geführt habe, dass von den 28 Mio. Fluggästen, die von April 2014 bis März 2015 aus der Union nach Kanada gereist seien, 178 Personen hätten festgenommen werden können.

153 Unter diesen Umständen kann davon ausgegangen werden, dass die Übermittlung der PNR-Daten an Kanada und ihre anschließende Verarbeitung geeignet sind, die Verwirklichung des mit dem geplanten Abkommen verfolgten Ziels des Schutzes der öffentlichen Sicherheit zu gewährleisten.

d) *Zur Erforderlichkeit der mit dem geplanten Abkommen verbundenen Eingriffe*

154 Hinsichtlich der Erforderlichkeit der mit dem geplanten Abkommen verbundenen Eingriffe ist nach der in den Rn. 140 und 141 angeführten Rechtsprechung zu prüfen, ob sich die Eingriffe auf das absolut Notwendige beschränken und, in diesem Rahmen, ob das Abkommen klare und präzise Regeln für die Tragweite und die Anwendung der darin vorgesehenen Maßnahmen enthält.

1) *Zu den PNR-Daten, auf die sich das geplante Abkommen bezieht*

i) *Zur hinreichenden Bestimmtheit des geplanten Abkommens hinsichtlich der zu übermittelnden PNR-Daten*

155 Das geplante Abkommen müsste hinsichtlich der Daten, auf die es sich bezieht, klar und präzise definieren, welche PNR-Daten die Fluggesellschaften in Anwendung des Abkommens an Kanada übermitteln müssen.

156 Die 19 Rubriken von PNR-Daten im Anhang des geplanten Abkommens entsprechen zwar nach der Stellungnahme der Kommission dem Anhang I der Leitlinien der International Civil Aviation Organization (ICAO) über PNR-Daten. Wie der Generalanwalt in Nr. 217 seiner Schlussanträge ausgeführt hat, werden die zu übermittelnden PNR-Daten in den Rubriken 5 („Verfügbare Vielflieger- und Bonus-Daten [Gratisflugscheine, Upgrades usw.]“) und 7 („Sämtliche verfügbaren Kontaktangaben, einschließlich Informationen zur Identifizierung des Dateneingebers“) aber nicht hinreichend klar und präzise definiert.

157 Bei Rubrik 5 ist der Umfang der zu übermittelnden Daten wegen der Verwendung des Ausdrucks „usw.“ nicht hinreichend bestimmt. Außerdem ist aus dem Wortlaut dieser Rubrik nicht ersichtlich, ob mit ihr Informationen allein über die Teilnahme der Fluggäste an Bonusprogrammen gemeint sind oder sämtliche Informationen über die Flüge und Buchungen, die im Rahmen solcher Programme durchgeführt werden.

158 Der Umfang der zu übermittelnden Daten ist auch in Rubrik 7 nicht hinreichend bestimmt, in der der Ausdruck „[s]ämtliche verfügbaren Kontaktangaben“ verwendet wird. Insbesondere wird nicht präzisiert, welche Art von Kontaktangaben gemeint sind und ob diese auch, wie sich aus der schriftlichen Antwort der Kommission auf die Fragen des Gerichtshofs ableiten lässt, Informationen über Dritte umfassen, die die Buchung des Fluges für den Fluggast vorgenommen haben, über die ein Fluggast erreicht werden kann oder die im Notfall zu verständigen sind.

159 Rubrik 8 betrifft „[s]ämtliche verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)“. Sie könnte zwar wegen der Verwendung des Ausdrucks „[s]ämtliche verfügbaren … [I]nformationen“ besonders weit erscheinen. Wie sich aus der Antwort der Kommission auf die Fragen des Gerichtshofs ergibt, ist aber davon auszugehen, dass sie lediglich Informationen über die Modalitäten der Zahlung und die Abrechnung des Flugtickets betrifft, nicht aber andere Informationen, die keinen direkten Bezug zum Flug aufweisen. Bei dieser Auslegung genügt die Rubrik den Anforderungen an Klarheit und Präzision.

160 Rubrik 17 betrifft „[a]llgemeine Eintragungen einschließlich OSI- (Other Supplementary Information), SSI- (Special Service Information) und SSR-Informationen (Special Service Request)“. Nach den Erläuterungen, die insbesondere die Kommission gegeben hat, handelt es sich bei dieser Rubrik um eine sogenannte „free text“-Rubrik, mit der über die im Anhang des geplanten Abkommens angeführten Informationen hinaus „weitere Informationen“ einbezogen werden sollen. Eine solche Rubrik enthält keine Angaben über Art und Umfang der zu übermittelnden Informationen und könnte selbst Informationen umfassen, die keinerlei Bezug zum Zweck der Übermittlung der PNR-Daten haben. Da die in dieser Rubrik genannten Informationen lediglich beispielhaft genannt werden, wie aus der Verwendung des Wortes „einschließlich“ hervorgeht, begrenzt sie Art und Umfang der Informationen, die von ihr erfasst werden können, nicht. Rubrik 17 ist mithin nicht hinreichend klar und präzise abgegrenzt.

161 Schließlich betrifft Rubrik 18 „[e]twaige für Buchungszwecke erhobene Daten zur Advance Passenger Information (API)“. Nach den Erläuterungen, die der Rat und die Kommission gegeben haben, entsprechen diese Informationen den Angaben gemäß Art. 3 Abs. 2 der Richtlinie 2004/82, d. h. Nummer und Art des mitgeführten Reisedokuments, Staatsangehörigkeit, vollständiger Name, Geburtsdatum, Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten, Beförderungs-Codenummer, Abreise- und Ankunftszeit, Gesamtzahl der beförderten Personen und ursprünglicher Abreiseort. Soweit die Rubrik dahin ausgelegt wird, dass sie sich lediglich auf die ausdrücklich in Art. 3 Abs. 2 der Richtlinie 2004/82 genannten Angaben erstreckt, kann davon ausgegangen werden, dass sie die Anforderungen an Klarheit und Präzision erfüllt.

162 Die Vorschriften von Art. 4 Abs. 3 des geplanten Abkommens, die die Verpflichtung Kanadas vorsehen, alle von den Fluggesellschaften übermittelten PNR-Daten, die nicht in der Liste im Anhang des Abkommens aufgeführt sind, zu löschen, kann die mangelnde Bestimmtheit der Rubriken 5, 7 und 17 des Anhangs nicht ausgleichen. Da die Liste als solche die zu übermittelnden PNR-Daten nicht hinreichend klar und präzise bestimmt, sind diese Bestimmungen nämlich nicht geeignet, die Unsicherheiten hinsichtlich der zu übermittelnden PNR-Daten zu beseitigen.

163 Somit ist hinsichtlich der an Kanada zu übermittelnden PNR-Daten festzustellen, dass die Rubriken 5, 7 und 17 des Anhangs des geplanten Abkommens den Umfang des Eingriffs in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte nicht hinreichend klar und präzise regeln.

ii) *Zu den sensiblen Daten*

164 Zur Übermittlung sensibler Daten im Sinne von Art. 2 Buchst. e des geplanten Abkommens ist festzustellen, dass sensible Daten dort definiert werden als Informationen, aus denen „die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit“ hervorgehen, sowie Informationen über „Gesundheit oder Sexualleben einer Person“. Ausdrücklich werden solche Daten in keiner der 19 Rubriken im Anhang des Abkommens erwähnt. Wie insbesondere die Kommission in ihrer Antwort auf die Fragen des Gerichtshofs bestätigt hat, könnten sie aber unter Rubrik 17 fallen. Der Umstand, dass die Art. 8 und 16 des geplanten Abkommens spezielle Regeln für die Verwendung und Speicherung sensibler Daten vorsehen, bedeutet zudem zwangsläufig, dass die Parteien des Abkommens die Möglichkeit der Übermittlung solcher Daten an Kanada zugelassen haben.

165 Insoweit ist festzustellen, dass jede Maßnahme, die auf dem Postulat beruht, dass eines oder mehrere der in Art. 2 Buchst. e des geplanten Abkommens genannten Merkmale als solche, unabhängig vom konkreten Verhalten des betreffenden Fluggasts, für das in der Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität bestehende Ziel der Verarbeitung von PNR-Daten erheblich sein könnte, gegen die in den Art. 7 und 8 der Charta in Verbindung mit deren Art. 21 niedergelegten Rechte verstößt. In Anbetracht des Risikos einer gegen Art. 21 der Charta verstoßenden Verarbeitung von Daten bedürfte die Übermittlung sensibler Daten an Kanada einer präzisen und besonders fundierten, auf andere Gründe als den Schutz der öffentlichen Sicherheit vor Terrorismus und grenzübergreifender schwerer Kriminalität gestützten Rechtfertigung. Im vorliegenden Fall fehlt es aber an einer solchen Rechtfertigung.

166 Überdies hat der Unionsgesetzgeber die Verarbeitung sensibler Daten in Art. 6 Abs. 4, Art. 7 Abs. 6 und Art. 13 Abs. 4 der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. 2016, L 119, S. 132) ausgeschlossen.

167 In Anbetracht der Ausführungen in den beiden vorstehenden Randnummern ist festzustellen, dass Art. 7, Art. 8, Art. 21 und Art. 52 Abs. 1 der Charta sowohl der Übermittlung sensibler Daten an Kanada als auch der von der Union mit diesem Drittstaat ausgehandelten Regelung der Bedingungen für die Verwendung und Speicherung solcher Daten durch die Behörden dieses Drittstaats entgegenstehen.

2) *Zur automatisierten Verarbeitung von PNR-Daten*

168 Wie der Generalanwalt in Nr. 252 seiner Schlussanträge ausgeführt hat, sollen die an Kanada übermittelten PNR-Daten hauptsächlich automatisierten Analysen unterzogen werden, die auf im Voraus festgelegten Modellen und Kriterien und dem Abgleich mit verschiedenen Datenbanken beruhen (siehe oben, Rn. 130 bis 132).

169 Die Bewertung der Gefahren, die von den Fluggästen für die öffentliche Sicherheit ausgehen, erfolgt mittels automatisierter Analysen der PNR-Daten vor der Ankunft der Fluggäste in Kanada (siehe oben, Rn. 130 und 131). Da diese Analysen anhand von nicht überprüften personenbezogenen Daten durchgeführt werden und auf

im Voraus festgelegten Modellen und Kriterien beruhen, sind sie zwangsläufig mit einer gewissen Fehlerquote behaftet, wie insbesondere die französische Regierung und die Kommission in der mündlichen Verhandlung eingeräumt haben.

170 Nach den Angaben in Rn. 30 der Stellungnahme des EDSB zum Entwurf eines Vorschlags für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken (ABl. 2008, C 110, S. 1), auf die der EDSB in seiner Antwort auf die Fragen des Gerichtshofs Bezug genommen hat, ist diese Fehlerquote offenbar erheblich.

171 Zwar sieht Art. 15 des geplanten Abkommens hinsichtlich der Folgen einer automatisierten Verarbeitung von PNR-Daten vor, dass Kanada „Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten" trifft. Außerdem gelten für eine derartige Verarbeitung Art. 3 des Abkommens, der die Zwecke jeglicher Datenverarbeitung durch die zuständige kanadische Behörde begrenzt, und Art. 7 des Abkommens, der eine Nichtdiskriminierungsklausel enthält.

172 Der Umfang des Eingriffs der automatisierten Analysen der PNR-Daten in die in den Art. 7 und 8 der Charta niedergelegten Rechte hängt aber im Wesentlichen von den im Voraus festgelegten Modellen und Kriterien sowie den Datenbanken ab, auf denen die automatisierte Verarbeitung der Daten beruht. In Anbetracht der Erwägungen in den Rn. 169 und 170 müssten die im Voraus festgelegten Modelle und Kriterien deshalb spezifisch und zuverlässig sein, so dass sie, wie der Generalanwalt in Nr. 256 seiner Schlussanträge ausgeführt hat, die Identifizierung von Personen ermöglichen, gegen die ein begründeter Verdacht der Beteiligung an terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität bestehen könnte, und dürften nicht diskriminierend sein. Ferner müssten die Datenbanken, mit denen die PNR-Daten abgeglichen werden, zuverlässig und aktuell sein und von Kanada in Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden.

173 Da die automatisierten Analysen der PNR-Daten zwangsläufig eine gewisse Fehlerquote aufweisen (siehe oben, Rn. 169), muss jedes positive Ergebnis, das durch eine automatisierte Verarbeitung von PNR-Daten erlangt wurde, nach Art. 15 des geplanten Abkommens individuell mit nicht automatisierten Mitteln überprüft werden, bevor eine individuelle Maßnahme mit nachteiligen Auswirkungen auf die betreffenden Fluggäste getroffen wird. Eine solche Maßnahme darf nach Art. 15 nämlich nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten getroffen werden.

174 Um in der Praxis zu gewährleisten, dass die im Voraus festgelegten Modelle und Kriterien, deren Anwendung und die verwendeten Datenbanken nicht diskriminierend sind und sich auf das absolut Notwendige beschränken, muss die Zuverlässigkeit und Aktualität dieser Modelle und Kriterien sowie der verwendeten Datenbanken, unter Berücksichtigung statistischer Daten und der Ergebnisse der internationalen Forschung, Gegenstand der in Art. 26 Abs. 2 des geplanten Abkommens vorgesehenen gemeinsamen Überprüfung seiner Durchführung sein.

3) *Zu den Zwecken der Verarbeitung von PNR-Daten*

i) *Vorbeugung, Aufdeckung und strafrechtliche Verfolgung von terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität*

175 Nach Art. 3 Abs. 1 des geplanten Abkommens dürfen PNR-Daten von der zuständigen kanadischen Behörde nur zum Zweck der Verhinderung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität verarbeitet werden.

176 Was den Begriff „terroristische Straftat" angeht, definiert Art. 3 Abs. 2 des geplanten Abkommens klar und präzise sowohl die Handlungen, die unter diesen Begriff fallen, als auch die Personen, Gruppen und Organisationen, die als „terroristische Einheit" einzustufen sind.

177 Desgleichen ist zum Begriff „grenzübergreifende schwere Kriminalität" festzustellen, dass Art. 3 Abs. 3 Unterabs. 1 des geplanten Abkommens, indem er verlangt, dass diese mit einer Freiheitsstrafe im Höchstmaß von mindestens vier Jahren oder mit einer schwereren Strafe geahndet wird, klar und präzise den Schweregrad der betreffenden Straftaten definiert. Auch was die Art dieser Straftaten angeht, ist die Vorschrift durch die Bezugnahme auf die Straftaten nach kanadischem Recht hinreichend präzise. Schließlich sind in Art. 3 Abs. 3 Unterabs. 2 des Abkommens klar und präzise die verschiedenen Fälle aufgeführt, in denen eine Straftat als grenzübergreifend gilt.

178 Somit ist festzustellen, dass Art. 3 Abs. 1 bis 3 des geplanten Abkommens klare und präzise Regeln enthält, die sich auf das absolut Notwendige beschränken.

ii) *Weitere Zwecke*

179 Nach Art. 3 Abs. 4 des geplanten Abkommens kann die zuständige kanadische Behörde in Ausnahmefällen PNR-Daten zum Schutz lebenswichtiger Interessen von Einzelpersonen verarbeiten, z. B. wenn Gefahr für Leib und Leben besteht oder die Gesundheit der Allgemeinheit erheblich gefährdet ist, vor allem im Sinne international anerkannter Normen. Nach Art. 3 Abs. 5 Buchst. a und b des Abkommens kann Kanada außerdem „im Einzelfall" PNR-Daten verarbeiten, damit „die Aufsicht oder Rechenschaftspflicht der öffentlichen Verwaltung gewährleistet ist" oder „einer Vorladung, einem erlassenen Haftbefehl oder einer gerichtlichen Verfügung Folge geleistet werden kann".

180 Da Art. 3 Abs. 4 des geplanten Abkommens die Fälle, in denen die zuständige kanadische Behörde die gemäß dem Abkommen erhobenen PNR-Daten zu anderen Zwecken verwenden darf als zu der mit ihm ange-

strebten Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität, auf den Schutz der lebenswichtigen Interessen von Personen beschränkt, definiert er klar und präzise die Fälle, in denen eine solche Verwendung zulässig ist. Im Übrigen sieht die Vorschrift vor, dass die zuständige kanadische Behörde hierzu nur in Ausnahmefällen ermächtigt ist. Ihre Regeln beschränken sich mithin auf das absolut Notwendige.

181 Hingegen ist der Wortlaut der Fälle, in denen Kanada PNR-Daten nach Art. 3 Abs. 5 Buchst. a und b des geplanten Abkommens verarbeiten darf, zu unbestimmt und zu allgemein, um den Anforderungen an Klarheit und Präzision zu genügen. Die in dieser Vorschrift enthaltenen Regeln beschränken sich daher nicht auf das zur Erreichung des mit dem Abkommen verfolgten Ziels absolut Notwendige.

4) *Zu den kanadischen Behörden, auf die sich das geplante Abkommen bezieht*

182 Nach Art. 2 Buchst. d des geplanten Abkommens ist die zuständige kanadische Behörde für den Erhalt und die Verarbeitung von PNR-Daten im Rahmen des Abkommens verantwortlich. Nach dessen Art. 5 wird davon ausgegangen, dass diese Behörde bei der Verarbeitung und Verwendung von PNR-Daten einen angemessenen Schutz im Sinne des Unionsrechts gewährleistet. Wie sich aus Abs. 15 der Präambel des Abkommens ergibt, verpflichtet sich Kanada ferner, sicherzustellen, dass diese Behörde die im Abkommen enthaltenen Garantien für den Schutz der Privatsphäre und den Schutz personenbezogener Daten einhält.

183 Die zuständige kanadische Behörde wird im geplanten Abkommen zwar nicht bezeichnet. Nach Art. 30 Abs. 2 Buchst. a des Abkommens ist Kanada aber verpflichtet, sie der Kommission vor Inkrafttreten des Abkommens mitzuteilen. Das Abkommen ist somit hinsichtlich der Identität der zuständigen kanadischen Behörde hinreichend klar und präzise.

184 In Art. 18 Abs. 1 des geplanten Abkommens ist zwar nicht bestimmt, an welche „anderen [Behörden] in Kanada“ die zuständige kanadische Behörde die PNR-Daten unter den dort genannten Voraussetzungen weitergeben darf. Aus Art. 18 Abs. 1 Buchst. a, c und e des geplanten Abkommens geht aber eindeutig hervor, dass die PNR-Daten nur an Behörden weitergegeben werden dürfen, „deren Aufgaben einen direkten Bezug zum Anwendungsbereich des Artikels 3 aufweisen“, sofern die Weitergabe „zu den in Artikel 3 genannten Zwecken notwendig [ist]“ und die Behörde „einen den in diesem Abkommen beschriebenen Garantien entsprechenden Schutz [gewährleistet]“.

185 Soweit in mehreren Bestimmungen des geplanten Abkommens (Art. 3 Abs. 5, Art. 6 Abs. 1 und 2, Art. 8 Abs. 3 bis 5, Art. 12 Abs. 3, Art. 16 und Art. 17) als für die Verarbeitung der in den betreffenden Bestimmungen genannten PNR-Daten zuständige Stelle „Kanada“ genannt ist, ist das Abkommen dahin auszulegen, dass entweder die zuständige kanadische Behörde oder die in Art. 18 genannten Behörden gemeint sind. Bei dieser Auslegung entsprechen Art. 3 Abs. 5, Art. 6 Abs. 1 und 2, Art. 8 Abs. 3 bis 5, Art. 12 Abs. 3, Art. 16 und Art. 17 des geplanten Abkommens den Anforderungen an Klarheit und Präzision.

5) *Zu den betroffenen Fluggästen*

186 Das geplante Abkommen gilt für die PNR-Daten sämtlicher Fluggäste, die aus der Union nach Kanada reisen. Die Daten werden an Kanada unabhängig davon übermittelt, ob objektive Anhaltspunkte dafür vorliegen, dass von den Fluggästen eine Gefahr für die öffentliche Sicherheit in Kanada ausgeht.

187 Die PNR-Daten sind vor allem dazu bestimmt, automatisiert verarbeitet zu werden (siehe oben, Rn. 152 und 169). Wie mehrere Beteiligte geltend gemacht haben, soll mit der automatisierten Verarbeitung ermittelt werden, ob möglicherweise eine Gefahr für die öffentliche Sicherheit von Personen ausgeht, die den zuständigen Stellen zu diesem Zeitpunkt nicht bekannt sind und die wegen dieser Gefahr einer eingehenden Überprüfung unterzogen werden könnten. Die automatisierte Verarbeitung der PNR-Daten vor der Ankunft der Fluggäste in Kanada erleichtert und beschleunigt dabei die Sicherheitskontrollen, insbesondere an den Grenzen. Der Ausschluss bestimmter Kategorien von Personen oder bestimmter Herkunftsländer könnte dem Ziel der automatisierten Verarbeitung der PNR-Daten zuwiderlaufen, das darin besteht, unter sämtlichen Fluggästen mittels einer Überprüfung dieser Daten die Personen zu ermitteln, von denen eine Gefahr für die öffentliche Sicherheit ausgehen kann. Außerdem könnte diese Überprüfung umgangen werden.

188 Im Übrigen haben alle Fluggäste nach Art. 13 des Abkommens von Chicago, auf den insbesondere der Rat und die Kommission in ihren Antworten auf die Fragen des Gerichtshofs Bezug genommen haben, beim Ein- und Ausflug sowie während des Aufenthalts im Hoheitsgebiet eines Vertragsstaats die Gesetze und Vorschriften dieses Staates über den Ein- und Ausflug von Fluggästen zu befolgen. Sämtliche Fluggäste, die nach Kanada einreisen oder aus Kanada ausreisen möchten, unterliegen nach diesem Artikel daher den Grenzkontrollen und sind verpflichtet, die Voraussetzungen des geltenden kanadischen Rechts für die Ein- oder Ausreise zu erfüllen. Zudem gehört die Identifizierung von Fluggästen, von denen ein Risiko für die öffentliche Sicherheit ausgehen kann, anhand der PNR-Daten zur Grenzkontrolle (siehe oben, Rn. 152 und 187). Sofern Fluggäste, die nach Kanada einreisen und sich dort aufhalten möchten, Gegenstand dieser Kontrollen sind, unterliegen sie deshalb schon wegen der Art dieser Maßnahme der Überprüfung ihrer PNR-Daten.

189 Unter diesen Umständen geht das geplante Abkommen dadurch, dass es die Übermittlung der PNR-Daten sämtlicher Fluggäste an Kanada ermöglicht, nicht über das hinaus, was absolut notwendig ist.

6) *Zur Speicherung und Verwendung der PNR-Daten*

190 Um zu gewährleisten, dass die Speicherung der übermittelten PNR-Daten, der Zugang zu ihnen durch die im geplanten Abkommen vorgesehenen kanadischen Behörden und die Verwendung der Daten durch diese Behörden auf das absolut Notwendige beschränkt wird, müsste das geplante Abkommen nach der in Rn. 141 ange-

führten ständigen Rechtsprechung des Gerichtshofs klare und präzise Regeln vorsehen, aus denen hervorgeht, unter welchen Umständen und unter welchen Voraussetzungen diese Behörden die Daten speichern, Zugang zu ihnen haben und sie verwenden dürfen.

191 In Bezug auf die Speicherung personenbezogener Daten ist festzustellen, dass die fragliche Regelung u. a. stets objektiven Kriterien genügen muss, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen (vgl. in diesem Sinne Urteile vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93, und vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 110).

192 Zur Verwendung rechtmäßig gespeicherter personenbezogener Daten durch eine Behörde hat der Gerichtshof entschieden, dass sich eine Unionsregelung nicht darauf beschränken darf, dass der Zugang zu solchen Daten einem der in der Regelung genannten Zwecke zu entsprechen hat, sondern auch die materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung der Daten festlegen muss (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 117 und 118 sowie die dort angeführte Rechtsprechung).

193 Im vorliegenden Fall begrenzt das geplante Abkommen in Art. 3 die Zwecke der Verwendung der PNR-Daten durch die zuständige kanadische Behörde, sieht in Art. 7 eine Nichtdiskriminierungsklausel vor und enthält in Art. 15 eine Vorschrift über Entscheidungen Kanadas auf der Grundlage einer automatisierten Verarbeitung der PNR-Daten (siehe oben, Rn. 171).

194 Außerdem sieht Art. 16 des geplanten Abkommens vor, dass die PNR-Daten von Kanada fünf Jahre nach Erhalt gespeichert werden dürfen (Abs. 1) und teilweise 30 Tage bzw. zwei Jahre nach Erhalt unkenntlich zu machen sind (Abs. 3). Da diese Vorschriften nicht anhand der betroffenen Fluggäste differenzieren, ermöglichen sie die Speicherung der PNR-Daten sämtlicher Fluggäste.

195 Schließlich darf nach Art. 16 Abs. 4 des geplanten Abkommens die Unkenntlichmachung aufgehoben werden, wenn Untersuchungen nach Maßgabe von Art. 3 des Abkommens durchgeführt werden müssen, wobei die Aufhebung der Unkenntlichmachung durch eine begrenzte Zahl eigens hierzu befugter Bediensteter oder mit vorheriger Genehmigung des Leiters der zuständigen kanadischen Behörde oder eines vom Leiter eigens hiermit beauftragten hohen Beamten erfolgt.

i) *Zur Speicherung und Verwendung der PNR-Daten vor der Ankunft der Fluggäste, während ihres Aufenthalts in Kanada und bei ihrer Ausreise*

196 Nach dem geplanten Abkommen ist es somit zulässig, die PNR-Daten sämtlicher Fluggäste während der gesamten Dauer ihrer Speicherung zu den in Art. 3 des Abkommens genannten Zwecken zu verwenden.

197 In Bezug auf die Speicherung der PNR-Daten und ihre Verwendung bis zur Ausreise der Fluggäste aus Kanada ist festzustellen, dass die PNR-Daten vor allem die Sicherheits- und Grenzkontrollen erleichtern. Ihre Speicherung und ihre Verwendung zu diesem Zweck können schon aufgrund ihrer Art nicht auf einen bestimmten Kreis von Fluggästen begrenzt werden oder Gegenstand einer vorherigen Genehmigung eines Gerichts oder einer unabhängigen Verwaltungsstelle sein. Somit ist im Einklang mit den in den Rn. 186 bis 188 angestellten Erwägungen festzustellen, dass, solange sich die Fluggäste in Kanada befinden oder im Begriff sind, aus diesem Drittland auszureisen, der erforderliche Zusammenhang zwischen den Daten und dem mit dem Abkommen verfolgten Ziel besteht, so dass das Abkommen nicht über das hinausgeht, was absolut notwendig ist, nur weil es die systematische Speicherung und Verwendung der PNR-Daten sämtlicher Fluggäste ermöglicht.

198 Desgleichen hängt die systematische Verwendung der PNR-Daten zu dem Zweck, die Zuverlässigkeit und Aktualität der im Voraus festgelegten Modelle und Kriterien, auf denen die automatisierten Verarbeitungen der Daten beruhen (siehe oben, Rn. 174), zu überprüfen oder neue Modelle und Kriterien für diese Verarbeitungen festzulegen, unmittelbar mit der Durchführung der Sicherheits- und Grenzkontrollen zusammen, so dass davon auszugehen ist, dass auch sie nicht über das hinausgeht, was absolut notwendig ist.

199 Außerdem können sich während des Aufenthalts der Fluggäste in Kanada unabhängig vom Ergebnis der vor ihrer Ankunft durchgeführten automatisierten Analyse der PNR-Daten Situationen ergeben, in denen die zuständige kanadische Behörde über während des Aufenthalts zusammengetragene Hinweise darauf verfügt, dass sich die Verwendung der Daten als erforderlich erweisen könnte, um Terrorismus und grenzübergreifende schwere Kriminalität zu bekämpfen.

200 Zur Verwendung der PNR-Daten in den in der vorstehenden Randnummer genannten Fällen ist jedoch festzustellen, dass den Fluggästen nach der Überprüfung ihrer PNR-Daten die Einreise in das Hoheitsgebiet dieses Drittstaats gestattet wurde, so dass eine Verwendung der Daten während ihres Aufenthalts in Kanada auf neue Umstände gestützt werden muss, die eine solche Verwendung rechtfertigen. Nach der in den Rn. 141 und 192 angeführten Rechtsprechung erfordert eine solche Verwendung deshalb Regeln, aus denen hervorgeht, unter welchen materiell- und verfahrensrechtlichen Voraussetzungen die Verwendung der Daten erfolgen darf, um diese insbesondere vor Missbrauchsrisiken zu schützen. Solche Regeln müssen sich auf objektive Kriterien stützen, die definieren, unter welchen Umständen und unter welchen Voraussetzungen die im geplanten Abkommen genannten kanadischen Behörden die Daten verwenden dürfen.

201 Gibt es objektive Anhaltspunkte dafür, dass die PNR-Daten eines oder mehrerer Fluggäste einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten oder grenzübergreifender schwerer Kriminalität leisten könnten, scheint die Verwendung der Daten nicht über das hinauszugehen, was absolut notwendig ist (vgl. ent-

sprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 119 und die dort angeführte Rechtsprechung).

202 Damit in der Praxis die vollständige Einhaltung der in den beiden vorstehenden Randnummern genannten Voraussetzungen gewährleistet ist, ist es unabdingbar, dass die Verwendung der gespeicherten PNR-Daten während des Aufenthalts der Fluggäste in Kanada grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass deren Entscheidung im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 120 und die dort angeführte Rechtsprechung).

203 Da das geplante Abkommen die in den beiden vorstehenden Randnummern genannten Anforderungen nicht erfüllt, gewährleistet es nicht, dass sich die Verwendung der PNR-Daten der Fluggäste während ihres Aufenthalts in Kanada durch die im Abkommen genannten kanadischen Behörden auf das absolut Notwendige beschränkt.

ii) *Zur Speicherung und Verwendung der PNR-Daten nach der Ausreise der Fluggäste aus Kanada*

204 Fluggäste, die aus Kanada ausgereist sind, sind in der Regel bei ihrer Ein- und Ausreise kontrolliert worden. Ebenso sind ihre PNR-Daten vor ihrer Ankunft in Kanada und gegebenenfalls während ihres Aufenthalts und bei ihrer Ausreise aus diesem Drittland überprüft worden. Daher ist davon auszugehen, dass von ihnen grundsätzlich keine Gefahr im Bereich des Terrorismus oder grenzübergreifender schwerer Kriminalität ausgeht, wenn weder diese Kontrollen und Überprüfungen noch irgendein anderer Umstand objektive Anhaltspunkte hierfür geliefert haben. Jedenfalls ist nicht ersichtlich, dass von sämtlichen Fluggästen, die nach Kanada gereist sind, nach ihrer Ausreise aus diesem Land eine höhere Gefahr ausginge als von anderen Personen, die während der letzten fünf Jahre nicht in dieses Land gereist sind und in Bezug auf die Kanada deshalb über keine PNR-Daten verfügt.

205 Daher dürfte bei Fluggästen, bei denen eine solche Gefahr weder bei ihrer Ankunft in Kanada noch bis zu ihrer Ausreise aus diesem Drittland festgestellt wurde, nach ihrer Ausreise kein Zusammenhang, sei er auch mittelbarer Art, zwischen ihren PNR-Daten und dem mit dem geplanten Abkommen verfolgten Ziel bestehen, der die Speicherung der Daten rechtfertigen würde. Die Argumente, die insbesondere der Rat und die Kommission vor dem Gerichtshof zur durchschnittlichen Bestandsdauer internationaler Netze schwerer Kriminalität sowie zu Dauer und Schwierigkeit der solche Netze betreffenden Ermittlungen vorgebracht haben, sind nicht geeignet, eine dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste nach ihrer Ausreise aus Kanada zum Zweck eines eventuellen Zugangs zu diesen Daten unabhängig von jedem Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität zu rechtfertigen (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 119).

206 Die dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste nach ihrer Ausreise aus Kanada beschränkt sich somit nicht auf das absolut Notwendige.

207 Gibt es in konkreten Fällen allerdings objektive Anhaltspunkte dafür, dass von bestimmten Fluggästen auch nach ihrer Ausreise aus Kanada eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte, erscheint eine Speicherung ihrer PNR-Daten über ihren Aufenthalt in Kanada hinaus zulässig (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 108).

208 Die Verwendung der auf diese Weise gespeicherten PNR-Daten müsste sich nach der in den Rn. 201 und 202 angeführten Rechtsprechung auf objektive Kriterien stützen, die definieren, unter welchen Umständen und unter welchen Voraussetzungen die im geplanten Abkommen genannten kanadischen Behörden Zugang zu diesen Daten haben und sie verwenden dürfen. Ferner müsste eine solche Verwendung – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werden, wobei die Entscheidung, mit der die Verwendung genehmigt wird, im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird.

209 Zur Dauer der Speicherung von PNR-Daten der in Rn. 207 beschriebenen Fluggäste ist festzustellen, dass die in Art. 16 Abs. 1 des geplanten Abkommens vorgesehene allgemeine Dauer gegenüber der im Abkommen von 2006 enthaltenen Dauer um anderthalb Jahre verlängert wurde. Insoweit ist aber in Anbetracht der Ausführungen insbesondere des Rates und der Kommission (siehe oben, Rn. 205) festzustellen, dass die in Art. 16 Abs. 1 des Abkommens vorgesehene Dauer von fünf Jahren nicht über das hinausgeht, was zur Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität absolut notwendig ist.

210 Sofern zum einen Art. 9 Abs. 2 des geplanten Abkommens, der vorsieht, dass Kanada die PNR-Daten „in einer gesicherten physischen Umgebung auf[bewahrt], die durch Zugangskontrollen geschützt ist“, bedeutet, dass die Daten im kanadischen Hoheitsgebiet aufzubewahren sind, und zum anderen Art. 16 Abs. 6 des Abkommens, wonach Kanada die PNR-Daten nach Ablauf der Speicherfrist vernichtet, so zu verstehen ist, dass er eine unwiderrufliche Vernichtung der Daten vorschreibt, genügen diese Bestimmungen den Anforderungen an Klarheit und Präzision (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 122 und die dort angeführte Rechtsprechung).

211 In Anbetracht der in den Rn. 204 bis 206 und 208 angestellten Erwägungen wird durch das geplante Abkommen nicht gewährleistet, dass sich die Speicherung und die Verwendung der PNR-Daten durch die kanadischen Behörden nach der Ausreise der Fluggäste aus Kanada auf das absolut Notwendige beschränken.

7) *Zur Weitergabe der PNR-Daten*

i) *Weitergabe der PNR-Daten an Behörden*

212 Die Art. 18 und 19 des geplanten Abkommens ermöglichen die Weitergabe von PNR-Daten durch die zuständige kanadische Behörde an andere kanadische Behörden und an Behörden in anderen Drittländern. Da diese Behörden durch eine solche Weitergabe faktisch Zugang zu den Daten erhalten und sie verwenden können, muss die Weitergabe die in den Rn. 200 bis 202 und 208 genannten Voraussetzungen für die Verwendung von PNR-Daten erfüllen.

213 Was insbesondere die Weitergabe von PNR-Daten an Behörden anderer Drittländer angeht, ist zu ergänzen, dass Art. 19 Abs. 1 Buchst. e des geplanten Abkommens der zuständigen kanadischen Behörde hinsichtlich der Beurteilung des in diesen Ländern garantierten Schutzniveaus einen Ermessensspielraum einräumt.

214 Insoweit ist darauf hinzuweisen, dass eine Weitergabe personenbezogener Daten aus der Union in ein Drittland nur zulässig ist, wenn das Drittland ein Schutzniveau der Grundfreiheiten und Grundrechte gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist. Dieses Erfordernis gilt auch im Fall der in Art. 19 des geplanten Abkommens vorgesehenen Weitergabe von PNR-Daten durch Kanada an Drittländer. Damit soll verhindert werden, dass das im Abkommen vorgesehene Schutzniveau durch die Weitergabe personenbezogener Daten an Drittländer umgangen werden könnte, und gewährleistet werden, dass das vom Unionsrecht gewährte Schutzniveau fortbesteht (vgl. entsprechend Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 72 und 73). Die Weitergabe personenbezogener Daten an ein Drittland erfordert daher ein Abkommen zwischen der Union und dem betreffenden Drittland, das dem geplanten Abkommen äquivalent ist, oder einen Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46, mit dem festgestellt wird, dass das Drittland ein angemessenes Schutzniveau im Sinne des Unionsrechts gewährleistet, und der sich auf die Behörden erstreckt, an die PNR-Daten weitergegeben werden sollen.

215 Da die Art. 18 und 19 des geplanten Abkommens den in den vorstehenden Rn. 212 bis 214 dargelegten Anforderungen nicht entsprechen, wird mit ihm nicht gewährleistet, dass sich die Weitergabe von PNR-Daten durch die zuständige kanadische Behörde an andere kanadische Behörden oder an Behörden anderer Drittländer auf das absolut Notwendige beschränkt.

ii) *Weitergabe der PNR-Daten an Einzelpersonen*

216 Nach Art. 12 Abs. 3 des geplanten Abkommens kann Kanada „jede Offenlegung von Informationen angemessenen rechtlichen Anforderungen und Beschränkungen unterwerfen, … unter gebührender Beachtung des berechtigten Interesses der betroffenen Person“. Im Abkommen ist aber weder geregelt, welche Informationen weitergegeben werden dürfen, noch, an wen sie weitergegeben oder wie sie verwendet werden dürfen.

217 Außerdem werden im geplanten Abkommen die „angemessenen rechtlichen Anforderungen und Beschränkungen“ und das „berechtigte Interesse der betroffenen Person“ nicht definiert, und es wird auch nicht verlangt, dass die Weitergabe von PNR-Daten an eine Einzelperson mit der Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität im Zusammenhang steht und von der Genehmigung eines Gerichts oder einer unabhängigen Verwaltungsstelle abhängig gemacht wird. Die Vorschrift geht daher über das absolut Notwendige hinaus.

3. *Zu den individuellen Rechten der Fluggäste*

218 Nach Art. 8 Abs. 2 Satz 2 der Charta hat jede Person, deren personenbezogene Daten erhoben wurden, das Recht, Auskunft über diese Daten zu erhalten und die Berichtigung der Daten zu erwirken.

219 Zu Art. 7 der Charta hat der Gerichtshof zudem bereits entschieden, dass das darin niedergelegte Grundrecht auf Achtung des Privatlebens voraussetzt, dass sich die betroffene Person vergewissern kann, dass ihre personenbezogenen Daten fehlerfrei verarbeitet werden und die Verarbeitung zulässig ist. Sie muss, um die nötigen Nachprüfungen durchführen zu können, ein Auskunftsrecht hinsichtlich der sie betreffenden Daten haben, die Gegenstand einer Verarbeitung sind (vgl. in diesem Sinne Urteil vom 7. Mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, Rn. 49).

220 Um zu gewährleisten, dass diese Rechte beachtet werden, muss den Fluggästen die Weitergabe ihrer PNR-Daten an Kanada und die Verwendung dieser Daten mitgeteilt werden, sobald dies die Ermittlungen der im geplanten Abkommen genannten Behörden nicht mehr beeinträchtigen kann. Diese Mitteilung ist nämlich der Sache nach erforderlich, damit die Fluggäste ihr Recht auf Auskunft über die sie betreffenden PNR-Daten und gegebenenfalls auf Berichtigung der Daten sowie ihr Recht, gemäß Art. 47 Abs. 1 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 121 und die dort angeführte Rechtsprechung).

a) *Zum Recht auf Information, Auskunft und Berichtigung*

221 Die Art. 12 und 13 des geplanten Abkommens gewähren den Fluggästen zwar ein Recht auf Zugang zu ihren PNR-Daten und ein Recht auf Berichtigung dieser Daten. Sie verlangen aber nicht, dass den Fluggästen die Weitergabe ihrer PNR-Daten an Kanada und deren Verwendung mitgeteilt wird.

222 Das geplante Abkommen enthält insoweit in Art. 11 lediglich eine Transparenzregel, die die zuständige kanadische Behörde verpflichtet, auf ihrer Website bestimmte Informationen allgemeiner Art über die Weitergabe der PNR-Daten und ihre Verwendung bereitzustellen. Es enthält keine Verpflichtung zur individuellen Information der Fluggäste.

223 Diese Transparenzregel ermöglicht es zwar in hinreichender Weise, die Fluggäste sowohl über die Weitergabe ihrer PNR-Daten an Kanada als auch über deren systematische Verwendung für Sicherheits- und Grenzkontrollen (siehe oben, Rn. 197 und 198) zu informieren. Die Fluggäste können durch die in Art. 11 des geplanten Abkommens vorgesehene allgemeine Information jedoch nicht erfahren, ob ihre Daten über diese Kontrollen hinaus von der zuständigen kanadischen Behörde verwendet wurden. In Fällen wie den in den Rn. 199 und 207 beschriebenen, in denen objektive Anhaltspunkte vorliegen, die eine solche Verwendung rechtfertigen und eine vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle erforderlich machen, ist daher eine individuelle Information der Fluggäste erforderlich. Dasselbe gilt für Fälle, in denen die PNR-Daten an andere Behörden oder an Einzelpersonen weitergegeben werden.

224 Nach der in Rn. 220 angeführten Rechtsprechung darf eine solche Mitteilung aber erst erfolgen, wenn sie die Ermittlungen der im geplanten Abkommen genannten Behörden nicht mehr beeinträchtigen kann.

225 Das geplante Abkommen müsste daher präzisieren, dass Fluggäste, deren PNR-Daten von der zuständigen kanadischen Behörde in den Fällen, die in den Rn. 199 und 207 genannt sind, verwendet und gespeichert wurden, und Fluggäste, deren Daten an andere Behörden oder an Einzelpersonen weitergegeben wurden, von dieser Behörde unter den in der vorstehenden Randnummer genannten Bedingungen über die Verwendung oder die Weitergabe informiert werden.

b) *Zum Recht auf einen Rechtsbehelf*

226 In Bezug auf das Recht der Fluggäste auf einen Rechtsbehelf sieht Art. 14 Abs. 2 des geplanten Abkommens vor, dass Kanada dafür sorgt, dass jede Person, die der Auffassung ist, dass ihre Rechte durch eine Entscheidung oder Maßnahme in Bezug auf ihre PNR-Daten verletzt wurden, Anspruch auf einen wirksamen gerichtlichen Rechtsbehelf nach kanadischem Recht im Hinblick auf eine gerichtliche Überprüfung oder auf eine andere Wiedergutmachung hat, wozu auch Schadensersatzzahlungen gehören können.

227 Da diese Vorschrift für „jede Person, die der Auffassung ist, dass ihre Rechte … verletzt wurden“, gilt, erfasst sie sämtliche Fluggäste, unabhängig von ihrer Staatsangehörigkeit, ihrem Aufenthaltsort, ihrem Wohnort oder ihrem Aufenthalt in Kanada. Außerdem ist sie, wie der Rat geltend gemacht hat, in dem Sinne zu verstehen, dass die Fluggäste über einen Rechtsbehelf vor einem Gericht, wie ihn Art. 47 Abs. 1 der Charta verlangt, verfügen. Dass Art. 14 Abs. 2 des geplanten Abkommens vorsieht, dass der „wirksame gerichtliche Rechtsbehelf“ durch eine Schadensersatzklage ergänzt werden kann, führt entgegen dem Vorbringen des Parlaments nicht dazu, dass den Fluggästen ein solcher wirksamer Rechtsbehelf genommen wird, sondern ist eher geeignet, den gerichtlichen Schutz der betreffenden Personen zu verstärken, wie der Generalanwalt in Nr. 324 seiner Schlussanträge ausgeführt hat.

4. *Zur Überwachung der Garantien im Bereich des Schutzes der PNR-Daten*

228 Nach Art. 8 Abs. 3 der Charta wird die Einhaltung der Anforderungen seiner Abs. 1 und 2 von einer unabhängigen Stelle überwacht.

229 Nach ständiger Rechtsprechung des Gerichtshofs soll die Gewährleistung der Unabhängigkeit einer solchen Kontrollstelle, deren Errichtung auch in Art. 16 Abs. 2 AEUV vorgesehen ist, die wirksame und zuverlässige Kontrolle der Einhaltung der Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen und ist im Licht dieses Zwecks auszulegen. Die Errichtung einer unabhängigen Kontrollstelle stellt daher ein wesentliches Element zur Wahrung des Schutzes der Personen bei der Verarbeitung personenbezogener Daten dar (Urteile vom 9. März 2010, Kommission/Deutschland, C-518/07, EU:C:2010:125, Rn. 25, vom 8. April 2014, Kommission/Ungarn, C-288/12, EU:C:2014:237, Rn. 48, und vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 41).

230 Im vorliegenden Fall bestimmt Art. 10 Abs. 1 Satz 1 des geplanten Abkommens, dass die Einhaltung der Datenschutzgarantien bei der Verarbeitung von PNR-Daten von einer „unabhängigen Behörde“ oder einer „durch administrative Mittel eingerichteten Stelle, die ihre Aufgaben unparteiisch wahrnimmt und nachweislich unabhängig Entscheidungen trifft“, beaufsichtigt wird. Soweit diese Vorschrift vorsieht, dass die Beaufsichtigung durch eine unabhängige Behörde erfolgt, entspricht sie den Anforderungen von Art. 8 Abs. 3 der Charta. Hingegen scheint die Alternative zu ermöglichen, dass die Überwachung ganz oder teilweise von einer Behörde vorgenommen werden kann, die ihre Aufgabe nicht in völliger Unabhängigkeit wahrnimmt, sondern einer Aufsichtsbehörde untergeordnet ist, von der sie Weisungen erhalten kann, so dass sie nicht vor jeder äußeren Einflussnahme auf ihre Entscheidungen geschützt ist.

231 Wie der Generalanwalt in Nr. 316 seiner Schlussanträge ausgeführt hat, wird durch Art. 10 des geplanten Abkommens somit nicht in hinreichend klarer und präziser Weise gewährleistet, dass die Überwachung der Einhaltung der im Abkommen vorgesehenen Regeln für den Schutz natürlicher Personen bei der Verarbeitung von PNR-Daten durch eine unabhängige Stelle im Sinne von Art. 8 Abs. 3 der Charta erfolgt.

*IX. Antwort auf den Gutachtenantrag*

232 Nach alledem ist festzustellen, dass

1. der Beschluss des Rates über den Abschluss des geplanten Abkommens auf Art. 16 Abs. 2 gemeinsam mit Art. 87 Abs. 2 Buchst. a AEUV zu stützen ist;

2. das geplante Abkommen nicht mit Art. 7, Art. 8, Art. 21 und Art. 52 Abs. 1 der Charta vereinbar ist, soweit es die Übermittlung sensibler Daten aus der Union nach Kanada und die Verwendung und Speicherung solcher Daten nicht ausschließt;

3. das geplante Abkommen, um mit Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta vereinbar zu sein,

a) die aus der Union nach Kanada zu übermittelnden PNR-Daten klar und präzise definieren muss,

b) vorsehen muss, dass die im Rahmen der automatisierten Verarbeitung von PNR-Daten verwendeten Modelle und Kriterien spezifisch und zuverlässig sowie nicht diskriminierend sind und dass nur Datenbanken verwendet werden, die von Kanada im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden,

c) außer im Rahmen der Überprüfungen der im Voraus festgelegten Modelle und Kriterien, auf denen die automatisierte Verarbeitung der PNR-Daten beruht, die Verwendung von PNR-Daten durch die zuständige kanadische Behörde während des Aufenthalts der Fluggäste in Kanada und nach ihrer Ausreise aus diesem Land sowie jede Weitergabe der Daten an andere Behörden materiell- und verfahrensrechtlichen Voraussetzungen unterwerfen muss, die sich auf objektive Kriterien stützen, sowie diese Verwendung und Weitergabe – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterwerfen muss, wobei die Entscheidung, mit der die Verwendung genehmigt wird, im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird,

d) die Speicherung von PNR-Daten nach der Ausreise der Fluggäste auf die Daten von Fluggästen beschränken muss, für die objektive Anhaltspunkte dafür vorliegen, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte,

e) die Weitergabe von PNR-Daten durch die zuständige kanadische Behörde an Behörden eines Drittlands davon abhängig machen muss, dass es ein Abkommen zwischen der Union und dem betreffenden Drittland, das dem geplanten Abkommen äquivalent ist, oder einen Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 gibt, der sich auf die Behörden erstreckt, an die PNR-Daten weitergegeben werden sollen,

f) ein Recht auf individuelle Information der Fluggäste im Fall der Verwendung der sie betreffenden PNR-Daten während ihres Aufenthalts in Kanada und nach ihrer Ausreise aus diesem Land und im Fall der Weitergabe dieser Daten durch die zuständige kanadische Behörde an andere Behörden oder Einzelpersonen vorsehen muss und

g) gewährleisten muss, dass die Kontrolle der Einhaltung der Regeln des geplanten Abkommens für den Schutz der Fluggäste bei der Verarbeitung der sie betreffenden PNR-Daten durch eine unabhängige Kontrollstelle sichergestellt wird.

Folglich äußert sich der Gerichtshof (Große Kammer) gutachtlich wie folgt:

1. **Der Beschluss des Rates über den Abschluss des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen im Namen der Union ist auf Art. 16 Abs. 2** gemeinsam mit **Art. 87 Abs. 2 Buchst. a AEUV zu stützen.**

2. **Das Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen ist nicht mit Art. 7, Art. 8, Art. 21 und Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union vereinbar, soweit es die Übermittlung sensibler Daten aus der Europäischen Union nach Kanada und die Verwendung und Speicherung solcher Daten nicht ausschließt.**

3. **Das Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen muss, um mit Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta der Grundrechte vereinbar zu sein,**

**a) die aus der Europäischen Union nach Kanada zu übermittelnden Fluggastdatensätze klar und präzise definieren,**

**b) vorsehen, dass die im Rahmen der automatisierten Verarbeitung von Fluggastdatensätzen verwendeten Modelle und Kriterien spezifisch und zuverlässig sowie nicht diskriminierend sind und dass nur Datenbanken verwendet werden, die von Kanada im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden,**

**c) außer im Rahmen der Überprüfungen der im Voraus festgelegten Modelle und Kriterien, auf denen die automatisierte Verarbeitung der Fluggastdatensätze beruht, die Verwendung von Fluggastdatensätzen durch die zuständige kanadische Behörde während des Aufenthalts der Fluggäste in Kanada und nach ihrer Ausreise aus diesem Land sowie jede Weitergabe der Daten an andere Behörden materiell- und verfahrensrechtlichen Voraussetzungen unterwerfen, die sich auf objektive Kriterien stützen, sowie diese Verwendung und Weitergabe – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterwerfen, wobei die Entscheidung, mit der die Verwendung genehmigt wird, im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von**

**den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird,**

**d) die Speicherung von Fluggastdatensätzen nach der Ausreise der Fluggäste auf die Daten von Fluggästen beschränken, für die objektive Anhaltspunkte dafür vorliegen, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte,**

**e) die Weitergabe von Fluggastdatensätzen durch die zuständige kanadische Behörde an Behörden eines Drittlands davon abhängig machen, dass es ein Abkommen zwischen der Europäischen Union und dem betreffenden Drittland, das dem Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen äquivalent ist, oder einen Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gibt, der sich auf die Behörden erstreckt, an die Fluggastdatensätze weitergegeben werden sollen,**

**f) ein Recht auf individuelle Information der Fluggäste im Fall der Verwendung der sie betreffenden Fluggastdatensätze während ihres Aufenthalts in Kanada und nach ihrer Ausreise aus diesem Land und im Fall der Weitergabe dieser Daten durch die zuständige kanadische Behörde an eine andere Behörde oder an Einzelpersonen vorsehen und**

**g) gewährleisten, dass die Kontrolle der Einhaltung der Regeln des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen für den Schutz der Fluggäste bei der Verarbeitung der sie betreffenden Fluggastdatensätze durch eine unabhängige Kontrollstelle sichergestellt wird.**

von Danwitz Da Cruz Vilaça Berger
Prechal Vilaras Rosas
Levits Šváby
A. Calot Escobar