Amtsblatt der Europäischen Union

L 119

Ausgabe in deutscher Sprache

Rechtsvorschriften

59. Jahrgang

4. Mai 2016

Inhalt

I *Gesetzgebungsakte*

VERORDNUNGEN

★ **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)** [1] 1

RICHTLINIEN

★ **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** 89

★ **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** 132

[1] Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

I

(Gesetzgebungsakte)

VERORDNUNGEN

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 ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(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 ([4]) 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.

([1]) ABl. C 229 vom 31.7.2012, S. 90.
([2]) ABl. C 391 vom 18.12.2012, S. 127.
([3]) Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.
([4]) 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. L 281 vom 23.11.1995, S. 31).

(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 wirtschaftliche 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 ([1]) 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 ([2]) 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

([1]) Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (C (2003) 1422) (ABl. L 124 vom 20.5.2003, S. 36).

([2]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

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 ([1]) 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 Anwendungsbereich 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 ([2]) 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.

([1]) 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, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates (siehe Seite 89 dieses Amtsblatts).

([2]) Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

(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 ([1]) 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

([1]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

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 vorhersehbar 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 ([1]) 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

([1]) Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen (ABl. L 95 vom 21.4.1993, S. 29).

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 ([1]) 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 beantragen 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.

([1]) Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz (ABl. L 354 vom 31.12.2008, S. 70).

(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 Erfüllung 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 internationalen 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 ([1]) 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

([1]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

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 Verarbeitungstätigkeiten 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 unverzüglich 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 betroffene 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 Richtlinie 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 Rechtsstreit 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 ([1]) 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

([1]) Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. L 351 vom 20.12.2012, S. 1).

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 wissenschaftlichen, 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 ([1]) lässt das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des

([1]) Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

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 Bedingungen 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 ([1]) 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 ([2]) 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

([1]) Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG Text von Bedeutung für den EWR (ABl. L 158 vom 27.5.2014, S. 1).

([2]) Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften (ABl. L 87 vom 31.3.2009, S. 164).

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 ([1]) 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 ([2]) 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 —

([1]) ABl. C 192 vom 30.6.2012, S. 7.

([2]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

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 [1];

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

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“);

[1] Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

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

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, verständlicher 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

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 wegen 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 Auftragsverarbeiter 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 geeignete 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 ([1]) 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;

([1]) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

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

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, Auftragsverarbeitern 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 Kategorien 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

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

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 [1] geregelt.

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

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.

[1] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

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

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

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

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	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

RICHTLINIEN

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Ausschusses der Regionen ([1]),

gemäß dem ordentlichen Gesetzgebungsverfahren, ([2])

in Erwägung nachstehender Gründe:

(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 Richtlinie soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen.

(3) 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 für die Ausübung von Tätigkeiten wie die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung in einem noch nie dagewesenen Umfang personenbezogene Daten verarbeitet werden können.

(4) Der freie Verkehr personenbezogener Daten zwischen den 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 innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen, sollte erleichtert und dabei gleichzeitig ein hohes Schutzniveau für personenbezogene Daten gewährleistet werden. Angesichts dieser Entwicklungen bedarf es des Aufbaus eines soliden und kohärenteren Rechtsrahmens für den Schutz personenbezogener Daten in der Union, die konsequent durchgesetzt werden.

(5) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([3]) gilt für jegliche Verarbeitung personenbezogener Daten in den Mitgliedstaaten sowohl im öffentlichen als auch im privaten Bereich. Ausgenommen ist jedoch die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.

([1]) ABl. C 391, 18.12.2012, S. 127.
([2]) Standpunkt des Europäischen Parlamentes vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlamentes vom 14. April 2016.
([3]) 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. L 281 vom 23.11.1995, S. 31).

(6) Für den Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit gilt der Rahmenbeschluss 2008/977/JI des Rates ([1]). Der Anwendungsbereich dieses Rahmenbeschlusses beschränkt sich auf die Verarbeitung personenbezogener Daten, die zwischen Mitgliedstaaten weitergegeben oder bereitgestellt werden.

(7) Für den Zweck der wirksamen justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit ist es entscheidend, ein einheitliches und hohes Schutzniveau für die personenbezogenen Daten natürlicher Personen zu gewährleisten und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten zu erleichtern. Im Hinblick darauf sollte dafür gesorgt werden, dass die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch zuständige 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, in allen Mitgliedstaaten gleichwertig geschützt werden. Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung der Rechte der betroffenen Personen und eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten, und auch gleichwertige Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten.

(8) 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 personenbezogener Daten zu erlassen.

(9) Auf dieser Grundlage sind in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]) allgemeine Bestimmungen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten in der Union niedergelegt.

(10) In der Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon annahm, erkannte die Regierungskonferenz an, dass es sich aufgrund der Besonderheiten dieser Bereiche als erforderlich erweisen könnte, auf Artikel 16 AEUV gestützte spezifische Vorschriften über den Schutz personenbezogener Daten und den freien Verkehr personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu erlassen.

(11) Daher sollte diesen Bereichen durch eine Richtlinie Rechnung getragen werden, die spezifische Vorschriften 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, enthält, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird. Diese zuständigen Behörden können nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden einschließen, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als denen dieser Richtlinie verarbeiten, gilt die Verordnung (EU) 2016/679. Daher gilt die Verordnung (EU) 2016/679 in Fällen, in denen eine Stelle oder Einrichtung personenbezogene Daten zu anderen Zwecken erhebt und diese personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der sie unterliegt, weiterverarbeitet. Zum Beispiel speichern Finanzinstitute zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten bestimmte personenbezogene Daten, die sie verarbeiten, und stellen sie nur den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem Recht der Mitgliedstaaten zur Verfügung. Eine Stelle oder Einrichtung, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter nach dieser Richtlinie geltenden Bestimmungen gebunden sein, wobei die Anwendung der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter außerhalb des Anwendungsbereichs dieser Richtlinie durchführt, unberührt bleibt.

(12) Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen

([1]) Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Ersetzung von Richtlinie 95/46/EC (Datenschutz-Grundverordnung) (Siehe Seite 1 dieses Amtsblatts).

Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist. Die Mitgliedstaaten können die zuständigen Behörden mit anderen Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, 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 Anwendungsbereich der Verordnung (EU) 2016/679 fällt, als sie in den Anwendungsbereich des Unionsrechts fällt.

(13) Eine Straftat im Sinne dieser Richtlinie sollte ein eigenständiger Begriff des Unionsrechts in der Auslegung durch den Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") sein.

(14) Da diese Richtlinie nicht für die Verarbeitung personenbezogener Daten gelten sollte, die im Rahmen einer nicht unter das Unionsrecht fallenden Tätigkeit erfolgt, sollten die nationale Sicherheit betreffende Tätigkeiten, Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind, und die Verarbeitung personenbezogener Daten, die von den Mitgliedstaaten bei Tätigkeiten vorgenommen wird, die in den Anwendungsbereich des Titels V Kapitel 2 des Vertrags über die Europäische Union (EUV) fallen, nicht als Tätigkeiten betrachtet werden, die in den Anwendungsbereich dieser Richtlinie fallen.

(15) Um zu gewährleisten, dass natürliche Personen in der Union auf der Grundlage unionsweit durchsetzbarer Rechte das gleiche Maß an Schutz genießen und Unterschiede, die den Austausch personenbezogener Daten zwischen den zuständigen Behörden behindern könnten, beseitigt werden, sollte diese Richtlinie harmonisierte Vorschriften für den Schutz und den freien Verkehr personenbezogener Daten festlegen, die 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, verarbeitet werden. Die Angleichung der Rechtsvorschriften der Mitgliedstaaten sollte nicht zu einer Lockerung des Schutzes personenbezogener Daten in diesen Ländern führen, sondern vielmehr auf ein hohes Schutzniveau in der gesamten Union abstellen. Die Mitgliedstaaten sollten nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

(16) Diese Richtlinie berührt nicht den Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten. Gemäß der Verordnung (EU) 2016/679 können personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer öffentlichen Behörde oder einer öffentlichen oder privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die öffentliche Behörde oder Einrichtung unterliegt, offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten in Einklang zu bringen.

(17) Der durch diese Richtlinie gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten.

(18) Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung, 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 der Richtlinie fallen.

(19) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [1] 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 gemäß der Verordnung (EU) 2016/679 angepasst werden.

(20) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, in den nationalen Vorschriften für Strafverfahren Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden festzulegen, insbesondere in Bezug auf personenbezogene Daten in einer gerichtlichen Entscheidung oder in Dokumenten betreffend Strafverfahren.

[1] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

(21) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. 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 technologischen 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 mehr identifiziert werden kann.

(22) 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 für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.

(23) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und 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. Angesichts der Komplexität und Sensibilität genetischer Informationen besteht ein hohes Missbrauchs- und Wiederverwendungsrisiko für unterschiedliche Zwecke durch den Verantwortlichen. Jede Diskriminierung aufgrund genetischer Merkmale sollte grundsätzlich verboten sein.

(24) 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 Vormerkung zur Erbringung und der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([1]) erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie 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.

(25) Alle Mitgliedstaaten sind Mitglied der Internationalen Kriminalpolizeilichen Organisation (Interpol). Interpol erhält, speichert und übermittelt für die Erfüllung ihres Auftrags personenbezogene Daten, um die zuständigen Behörden dabei zu unterstützen, internationale Kriminalität zu verhüten und zu bekämpfen. Daher sollte die Zusammenarbeit zwischen der Union und Interpol gestärkt werden, indem ein effizienter Austausch personenbezogener Daten gefördert und zugleich die Achtung der Grundrechte und Grundfreiheiten hinsichtlich der automatischen Verarbeitung personenbezogener Daten gewährleistet wird. Wenn personenbezogene Daten aus der Union an Interpol und die Staaten, die Mitglieder zu Interpol abgestellt haben, übermittelt werden, sollte diese Richtlinie, insbesondere die Bestimmungen über grenzüberschreitende Datenübermittlungen, zur Anwendung kommen. Diese Richtlinie sollte die spezifischen Vorschriften unberührt lassen, die im Gemeinsamen Standpunkt 2005/69/JI des Rates ([2]) und im Beschluss 2007/533/JI des Rates ([3]) festgelegt sind.

(26) Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen natürlichen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Dies steht an sich der

([1]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

([2]) Gemeinsamer Standpunkt 2005/69/JI des Rates vom 24. Januar 2005 zum Austausch bestimmter Daten mit Interpol (ABl. L 27 vom 29.1.2005, S. 61).

([3]) Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 205 vom 7.8.2007, S. 63).

Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden nicht entgegen. Diese Maßnahmen können zwecks Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, getroffen werden, sofern sie durch Rechtsvorschriften geregelt sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen natürlichen Person gebührend berücksichtigt werden. Der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben ist ein anderes Konzept als das Recht auf ein faires Verfahren im Sinne des Artikels 47 der Charta und des Artikels 6 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK). Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogene Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt deren Erhebung feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sein. Es sollte insbesondere sichergestellt werden, dass nicht übermäßige personenbezogene Daten erhoben werden und sie nicht länger aufbewahrt werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist. 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 Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Die Mitgliedstaaten sollten geeignete Garantien für den Fall festlegen, dass personenbezogene Daten für die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für längere Zeiträume gespeichert werden.

(27) Zur Verhütung, Ermittlung und Verfolgung von Straftaten müssen die zuständigen Behörden personenbezogene Daten, die im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung einer bestimmten Straftat erhoben wurden, auch in einem anderen Kontext verarbeiten können, um sich ein Bild von den kriminellen Handlungen machen und Verbindungen zwischen verschiedenen aufgedeckten Straftaten herstellen zu können.

(28) Um stets eine sichere Verarbeitung zu gewährleisten und Verarbeitungen, die gegen diese Richtlinie verstoßen, zu verhindern, sollten personenbezogene Daten so verarbeitet werden, dass ein Maß an Sicherheit und Vertraulichkeit gegeben 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, und dass die Verarbeitung den Stand der verfügbaren Technik, die Kosten für ihre Einführung im Verhältnis zu den von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden personenbezogenen Daten berücksichtigt.

(29) Personenbezogene Daten sollten für festgelegte, eindeutige und rechtmäßige Zwecke innerhalb des Anwendungsbereichs dieser Richtlinie erhoben und nicht zu Zwecken verarbeitet werden, die nicht mit den Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zu vereinbaren sind. Werden personenbezogene Daten von demselben oder einem anderen Verantwortlichen für einen anderen in den Anwendungsbereich dieser Richtlinie fallenden Zweck als den, für den sie erhoben wurden, verarbeitet, so sollte diese Verarbeitung erlaubt sein, unter der Bedingung, dass diese Verarbeitung nach den geltenden Rechtsvorschriften zulässig ist und dass sie für diesen anderen Zweck erforderlich und verhältnismäßig ist.

(30) Der Grundsatz der sachlichen Richtigkeit der Daten sollte unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung angewandt werden. Aussagen, die personenbezogene Daten enthalten, basieren gerade in Gerichtsverfahren auf der subjektiven Wahrnehmung von natürlichen Personen und sind nicht immer nachprüfbar. Infolgedessen sollte sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.

(31) Bei der Verarbeitung personenbezogener Daten im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geht es naturgemäß um betroffene Personen verschiedener Kategorien. Daher sollte gegebenenfalls und so weit wie möglich klar zwischen den personenbezogenen Daten der einzelnen Kategorien betroffener Personen unterschieden werden wie Verdächtige, verurteilte Straftäter, Opfer und andere Parteien, beispielsweise Zeugen, Personen, die über einschlägige Informationen verfügen, oder Personen, die mit Verdächtigen oder verurteilten Straftätern in Kontakt oder in Verbindung stehen. Dies sollte nicht der Anwendung des Rechts auf die Unschuldsvermutung, wie es in der Charta und in der EMRK gewährleistet ist, in der Auslegung durch die Rechtsprechung des Gerichtshofs bzw. des Europäischen Gerichtshofs für Menschenrechte entgegenstehen.

(32) Die zuständigen Behörden sollten dafür sorgen, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Um den Schutz natürlicher Personen, die Richtigkeit, die Vollständigkeit oder den Aktualitätsgrad sowie die Zuverlässigkeit der übermittelten oder bereitgestellten personenbezogenen Daten zu gewährleisten, sollten die zuständigen Behörden möglichst bei allen Übermittlungen personenbezogener Daten die erforderlichen Informationen beifügen.

(33) Wenn in dieser Richtlinie auf Recht der Mitgliedstaaten, eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen

Gesetzgebungsakt, wobei Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats unberührt bleiben. Recht der Mitgliedstaaten, Rechtsgrundlagen oder Gesetzgebungsmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte gefordert. Im Recht der Mitgliedstaaten, das die Verarbeitung personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie regelt, sollten zumindest die Ziele, die zu verarbeitenden personenbezogenen Daten, die Zwecke der Verarbeitung sowie Verfahren zur Wahrung von Integrität und Vertraulichkeit der personenbezogenen Daten und Verfahren für ihre Vernichtung angegeben werden, um hinreichende Garantien gegen die Gefahr des Missbrauchs und der Willkür zu bieten.

(34) Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sollte jeden mit Hilfe automatisierter Verfahren oder auf anderem Wege 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, den Abgleich oder die Verknüpfung, die Einschränkung der Verarbeitung, das Löschen oder die Vernichtung abdecken. Insbesondere sollte diese Richtlinie Anwendung finden, wenn personenbezogene Daten für die Zwecke dieser Richtlinie an einen Empfänger übermittelt werden, der nicht dieser Richtlinie unterliegt. Unter einem solchen Empfänger sollte eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle zu verstehen sein, gegenüber der personenbezogene Daten von der zuständigen Behörde rechtmäßig offengelegt werden. Wurden personenbezogene Daten ursprünglich von einer zuständigen Behörde für einen der Zwecke dieser Richtlinie erhoben, so sollte die Verordnung (EU) 2016/679 für die Verarbeitung dieser Daten für andere Zwecke als diejenigen dieser Richtlinie gelten, wenn eine solche Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist. Insbesondere sollte die Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten für Zwecke gelten, die außerhalb des Anwendungsbereichs dieser Richtlinie liegen. Für die Verarbeitung personenbezogener Daten durch einen Empfänger, der keine zuständige Behörde im Sinne dieser Richtlinie ist oder nicht als solche handelt und gegenüber dem personenbezogene Daten von einer zuständigen Behörde rechtmäßig offengelegt werden, sollte die Verordnung (EU) 2016/679 gelten. Bei der Umsetzung dieser Richtlinie sollten die Mitgliedstaaten außerdem, die Anwendung der Vorschriften der Verordnung (EU) 2016/679 — vorbehaltlich der darin genannten Bedingungen — genauer regeln können.

(35) Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde im öffentlichen Interesse auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten 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, ausführt. Diese Tätigkeiten sollten sich auf die Wahrung lebenswichtiger Interessen der betroffenen Person erstrecken. Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.

(36) Die Mitgliedstaaten sollten vorsehen, dass immer dann, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung von personenbezogenen Daten unter bestimmten Umständen besondere Bedingungen, etwa zur Verwendung von Bearbeitungscodes, gelten, die übermittelnde zuständige Behörde den Empfänger der personenbezogenen Daten auf diese Bedingungen und die Verpflichtung sie einzuhalten hinweisen sollte. Hierzu könnte beispielsweise das Verbot, personenbezogene Daten an andere weiter zu übermitteln, oder das Verbot, sie für andere Zwecke, als die Zwecke zu denen sie an den Empfänger übermittelt wurden, zu verwenden, oder das Verbot, die betroffene Person im Falle der Einschränkung des Rechts auf Unterrichtung ohne vorheriger Genehmigung der übermittelnden zuständigen Behörde zu informieren, zählen. Diese Pflichten gelten auch für Übermittlungen durch die übermittelnde zuständige Behörde an Empfänger in Drittländern oder an internationale Organisationen. Die Mitgliedstaaten sollten sicherstellen, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen nur solche Bedingungen anwendet, die auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

(37) 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 Richtlinie nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Solche personenbezogenen Daten sollten nur dann verarbeitet werden, wenn die Verarbeitung vorbehaltlich geeigneter Garantien für die durch Rechtsvorschriften festgelegten Rechte und Freiheiten der betroffenen Person erfolgt und in durch Rechtsvorschriften geregelten Fällen erlaubt ist oder anderenfalls zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist oder aber sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Zu den geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person kann beispielsweise zählen, dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird. Die Verarbeitung solcher Daten sollte ebenfalls durch Rechtsvorschriften erlaubt sein, wenn die betroffene Person der Datenverarbeitung, die besonders stark in ihre Privatsphäre eingreift, ausdrücklich zugestimmt hat. Die Einwilligung der betroffenen Person allein sollte jedoch noch keine rechtliche Grundlage für die Verarbeitung solch sensibler personenbezogener Daten durch die zuständigen Behörden liefern.

(38) Die betroffene Person sollte das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die nachteilige rechtliche Wirkung für sie entfaltet oder sie in erheblichem Maße beeinträchtigt. In jedem Fall sollte eine solche Verarbeitung mit geeigneten Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Rechts, das Eingreifen einer Person zu erwirken, insbesondere auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung. Ein Profiling, das zur Folge hat, dass natürliche Personen aufgrund von personenbezogenen Daten diskriminiert werden, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, sollte gemäß den Bestimmungen der Artikel 21 und 52 der Charta verboten werden.

(39) Damit die betroffene Person ihre Rechte wahrnehmen kann, sollten alle Informationen für sie leicht zugänglich — auch auf der Website des Verantwortlichen — und verständlich, also in klarer und einfacher Sprache abgefasst sein. Diese Informationen sollten an die Bedürfnisse von schutzbedürftigen Personen, wie etwa Kindern, angepasst werden.

(40) Es sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung ihrer Rechte aufgrund der nach dieser Richtlinie erlassenen Vorschriften erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. Der Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person unverzüglich zu beantworten, es sei denn, er wendet Einschränkungen in Bezug auf die Rechte der betroffenen Person gemäß dieser Richtlinie an. Bei offenkundig unbegründeten oder exzessiven Anträgen, zum Beispiel wenn die betroffene Person ungebührlich und wiederholt Informationen verlangt oder wenn die betroffene Person ihr Recht auf Unterrichtung missbraucht, beispielsweise indem sie in ihrem Antrag falsche oder irreführende Angaben macht, sollte der Verantwortliche, eine angemessene Gebühr erheben können oder sich weigern können, aufgrund des Antrags tätig zu werden.

(41) Fordert der Verantwortliche zusätzliche Informationen an, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, so sollten diese Informationen nur für diesen konkreten Zweck verarbeitet werden und nicht länger gespeichert werden, als es für diesen Zweck notwendig ist.

(42) Der betroffenen Person sollten zumindest folgende Informationen zur Verfügung gestellt werden: die Identität des Verantwortlichen, die Existenz des Verarbeitungsvorgangs, die Zwecke der Verarbeitung, das Beschwerderecht und das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung durch den Verantwortlichen. Dies könnte auf der Website der zuständigen Behörde erfolgen. Außerdem sollte die betroffene Person in bestimmten Fällen und zur Ermöglichung der Ausübung ihrer Rechte über die Rechtsgrundlage der Verarbeitung und die Speicherfrist informiert werden, soweit diese zusätzlichen Informationen unter Berücksichtigung der spezifischen Umstände, unter denen die Daten verarbeitet werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(43) Eine natürliche Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden 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. Jede betroffene Person sollte daher das Recht haben, zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie verarbeitet werden und wer deren Empfänger, einschließlich solcher in Drittländern, sind. Enthalten solche Mitteilungen Informationen über den Ursprung der personenbezogenen Daten, so sollten die Informationen nicht die Identität natürlicher Personen und insbesondere keine vertraulichen Quellen preisgeben. Damit diesem Recht entsprochen wird, braucht die betroffene Person lediglich im Besitz einer vollständigen Übersicht über diese Daten in verständlicher Form zu sein, d. h. in einer Form, die es ihr ermöglicht, sich dieser Daten bewusst zu werden und nachzuprüfen, ob sie richtig sind und im Einklang mit dieser Richtlinie verarbeitet werden, so dass

sie die ihr durch diese Richtlinie verliehenen Rechte ausüben kann. Eine solche Übersicht könnte in Form einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, bereitgestellt werden.

(44) Die Mitgliedstaaten sollten Gesetzgebungsmaßnahmen erlassen können, mit denen die Unterrichtung der betroffenen Person aufgeschoben, eingeschränkt oder unterlassen oder die Auskunft über ihre personenbezogenen Daten ganz oder teilweise in dem Umfang und so lange eingeschränkt wird, wie dies in einer demokratischen Gesellschaft unter gebührender Berücksichtigung der Grundrechte und der berechtigten Interessen der betroffenen natürlichen Person eine erforderliche und verhältnismäßige Maßnahme darstellt, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen. Der Verantwortliche sollte im Wege einer konkreten Einzelfallprüfung feststellen, ob das Auskunftsrecht teilweise oder vollständig eingeschränkt werden sollte.

(45) Eine Verweigerung oder Einschränkung der Auskunft sollte der betroffenen Person grundsätzlich unter Angabe der sachlichen oder rechtlichen Gründe hierfür schriftlich mitgeteilt werden.

(46) Jede Einschränkung der Rechte der betroffenen Person muss mit der Charta und mit der EMRK in der Auslegung durch die Rechtsprechung des Gerichtshofs bzw. des Europäischen Gerichtshofs für Menschenrechte vereinbar sein und insbesondere den Wesensgehalt dieser Rechte und Freiheiten achten.

(47) Eine natürliche Person sollte das Recht auf Berichtigung sie betreffender unrichtiger personenbezogener Daten, insbesondere bei Bezug auf Tatsachen, sowie das Recht auf Löschung besitzen, wenn die Datenverarbeitung gegen diese Richtlinie verstößt. Das Recht auf Berichtigung sollte allerdings beispielsweise nicht den Inhalt einer Zeugenaussage berühren. Eine natürliche Person sollte auch das Recht auf Einschränkung der Verarbeitung besitzen, wenn sie die Richtigkeit personenbezogener Daten bestreitet und deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann oder wenn die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen. Insbesondere sollte statt der Löschung personenbezogener Daten die Verarbeitung eingeschränkt werden, wenn in einem konkreten Fall berechtigter Grund zu der Annahme besteht, dass eine Löschung die berechtigten Interessen der betroffenen Person beeinträchtigen könnte. In einem solchen Fall sollten Daten mit Einschränkungsmarkierung nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand. Methoden zur Einschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte Daten, beispielsweise zu Archivierungszwecken, auf ein anderes Verarbeitungssystem übertragen oder gesperrt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden. Entsprechende Berichtigungen oder Löschungen personenbezogener Daten oder Einschränkungen der Verarbeitung sollten den Empfängern, gegenüber dem die personenbezogenen Daten offengelegt wurden, und den zuständigen Behörden, von denen die unrichtigen Daten stammen, mitgeteilt werden. Der Verantwortliche sollte auch von jeglicher Weiterverbreitung dieser Daten Abstand nehmen.

(48) Verweigert ein Verantwortlicher einer betroffenen Person ihr Recht auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung, so sollte die betroffene Person die nationale Aufsichtsbehörde ersuchen können, die Rechtmäßigkeit der Verarbeitung zu überprüfen. Die betroffene Person sollte über dieses Recht unterrichtet werden. Handelt die Aufsichtsbehörde im Namen der betroffenen Person, so sollte sie die betroffene Person zumindest darüber informieren, dass alle erforderlichen Prüfungen oder Überprüfungen durchgeführt wurden. Die Aufsichtsbehörde sollte die betroffene Person zudem über ihr Recht auf gerichtlichen Rechtsbehelf in Kenntnis setzen.

(49) Werden personenbezogene Daten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen verarbeitet, so sollten die Mitgliedstaaten vorsehen können, dass die Ausübung des Rechts auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung nach Maßgabe des einzelstaatlichen Strafverfahrensrechts erfolgt.

(50) 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 Richtlinie stehen. 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. Im Rahmen der von ihm ergriffenen Maßnahmen sollte der Verantwortliche auch spezifische Garantien für die Verarbeitung personenbezogener Daten von schutzbedürftigen natürlichen Personen, wie etwa Kindern, ausarbeiten und implementieren.

(51) Risiken für die Rechte und Freiheiten der natürlichen Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Datenverarbeitung 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 Daten, der unbefugten Umkehr 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, die Religion oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, wenn genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über die Gesundheit oder Daten über das Sexualleben und sexuelle Orientierung oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln 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 und prognostiziert werden, um ein persönliches Profil 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 Personen betrifft.

(52) Eintrittswahrscheinlichkeit und Schwere des Risikos sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen.

(53) 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 Richtlinie erfüllt werden. Die Umsetzung dieser Maßnahmen sollte nicht ausschließlich von wirtschaftlichen Erwägungen abhängig gemacht werden. Um die Einhaltung dieser Richtlinie nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun. Hat der Verantwortliche eine Datenschutz-Folgenabschätzung gemäß dieser Richtlinie vorgenommen, sollten die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt werden. Die Maßnahmen könnten u. a. aus einer möglichst frühen Pseudonymisierung bestehen. Gerade durch die Pseudonymisierung für die Zwecke dieser Richtlinie könnte der freie Verkehr personenbezogener Daten im Raum der Freiheit, der Sicherheit und des Rechts erleichtert werden.

(54) 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 gemäß dieser Richtlinie, 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.

(55) Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf der Grundlage eines Rechtsinstruments einschließlich eines Vertrags erfolgen, der den Auftragsverarbeiter an den Verantwortlichen bindet und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter nur auf Weisung des Verantwortlichen handeln sollte. Der Auftragsverarbeiter sollte den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigen.

(56) Zum Nachweis der Einhaltung dieser Richtlinie sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis aller Kategorien von Tätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage dieses Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieses Verzeichnisses kontrolliert werden können. Der Verantwortliche oder der Auftragsverarbeiter, der personenbezogene Daten in nicht automatisierten Verarbeitungssystemen verarbeitet, sollte über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Verarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.

(57) In automatisierten Verarbeitungssystemen werden zumindest über folgende Verarbeitungsvorgänge Protokolle geführt: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlungen, Kombination oder Löschung. Die Identifizierung der Person, die personenbezogene Daten abgefragt oder offengelegt hat, sollte protokolliert werden und aus dieser Identifizierung sollt sich die Begründung für die Verarbeitungsvorgänge ableiten lassen. Die Protokolle sollten ausschließlich zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Daten sowie für Strafverfahren verwendet werden. Die Eigenüberwachung umfasst auch interne Disziplinarverfahren der zuständigen Behörden.

(58) Eine Datenschutz-Folgenabschätzung, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, die geplant sind den Schutz personenbezogener Daten zu gewährleisten und die die Einhaltung der Bestimmungen dieser Richtlinie nachweisen sollen, sollte durch den Verantwortlichen durchgeführt werden, wenn die Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben. Datenschutz-Folgenabschätzungen sollten auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen abstellen, nicht jedoch auf Einzelfälle.

(59) Um einen wirksamen Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten, sollte der Verantwortliche oder der Auftragsverarbeiter in bestimmten Fällen vor der Verarbeitung die Aufsichtsbehörde konsultieren.

(60) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Richtlinie 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. Solche Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau — auch hinsichtlich der Vertraulichkeit — gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, 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. Der Verantwortliche und der Auftragsverarbeiter sollten sicherstellen, dass personenbezogene Daten nicht durch Unbefugte verarbeitet werden.

(61) 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 personenbezogenen 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.

(62) Natürliche Personen, sollten unverzüglich benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, damit sie 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. Die Benachrichtigung der betroffenen Person sollte 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 erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen des Schutzes von Daten zu treffen. In Ausnahmefällen könnte die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen natürlichen Person unterbleiben, wenn ein Aufschub oder eine Einschränkung dieser Benachrichtigung nicht ausreicht, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen.

(63) Der Verantwortliche sollte eine Person benennen, die ihn dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen, es sei denn, ein Mitgliedstaat beschließt eine Ausnahmeregelung für Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Bei dieser Person kann es sich um ein Mitglied des vorhandenen Personals des Verantwortlichen handeln, das eine besondere Schulung auf dem Gebiet der Datenschutzvorschriften und der Datenschutzpraxis erhalten hat, um einschlägiges Fachwissen in diesem Bereich zu erwerben. Der Grad des erforderlichen Fachwissens sollte sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem Verantwortlichen verarbeiteten personenbezogenen Daten richten. Die betreffende Person kann ihre Aufgabe auf Teilzeit- oder Vollzeitbasis wahrnehmen. Mehrere Verantwortliche können unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe gemeinsam einen Datenschutzbeauftragten bestellen, zum Beispiel im Falle einer gemeinsamen Nutzung von Ressourcen in zentralen Stellen. Die betreffende Person kann auch für verschiedene Positionen innerhalb der Struktur der jeweils Verantwortlichen benannt werden. Sie sollte den Verantwortlichen und die Beschäftigten, die personenbezogene Daten verarbeiten, unterstützen, indem sie diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Diese Datenschutzbeauftragten sollten ihren Auftrag und ihre Aufgaben auf unabhängige Weise gemäß dem Recht der Mitgliedstaaten wahrnehmen können.

(64) Die Mitgliedstaaten sollten dafür sorgen, dass Daten nur dann an ein Drittland oder eine internationale Organisation übermittelt werden, wenn dies für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von

Straftaten oder für die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, notwendig ist und es sich bei dem Verantwortlichen in dem Drittland oder in der internationalen Organisation um eine zuständige Behörde im Sinne dieser Richtlinie handelt. Eine Übermittlung sollte nur durch zuständige Behörden vorgenommen werden, die als Verantwortliche agieren, es sei denn, Auftragsverarbeiter werden ausdrücklich beauftragt, im Namen der Verantwortlichen Übermittlungen vorzunehmen. Derartige Übermittlungen können erfolgen, wenn die Kommission beschlossen hat, dass das betreffende Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau gewährleistet, oder wenn geeignete Garantien bestehen oder wenn Ausnahmen für bestimmte Fälle gelten. Das durch diese Richtlinie unionsweit gewährleistete Schutzniveau für natürliche Personen sollte 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 dem Drittland oder von der internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden.

(65) Werden personenbezogene Daten von einem Mitgliedstaat an Drittländer oder internationale Organisationen übermittelt, so sollte die Übermittlung grundsätzlich erst dann erfolgen, wenn der Mitgliedstaat, von dem die Daten stammen, die Übermittlung genehmigt hat. Im Interesse einer wirksamen Zusammenarbeit bei der Verhütung, Ermittlung und Aufdeckung von Straftaten ist es erforderlich, dass im Falle einer Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats, die so unvermittelt eintritt, dass es unmöglich ist, rechtzeitig eine vorherige Genehmigung einzuholen, die zuständige Behörde die maßgeblichen personenbezogenen Daten ohne vorherige Genehmigung an das betreffende Drittland oder die betreffende internationale Organisation übermitteln können sollte. Die Mitgliedstaaten sollten vorsehen, dass Drittländern oder internationalen Organisationen etwaige besondere Bedingungen für die Übermittlung mitgeteilt werden. Die Weiterübermittlung personenbezogener Daten sollte der vorherigen Genehmigung durch die zuständige Behörde bedürfen, die die ursprüngliche Übermittlung durchgeführt hat. Bei der Entscheidung über einen Antrag auf die Genehmigung einer Weiterübermittlung sollte die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, alle maßgeblichen Faktoren gebührend berücksichtigen, einschließlich der Schwere der Straftat, der spezifischen Auflagen und des Zwecks der ursprünglichen Datenübermittlung, der Art und der Bedingungen der Strafvollstreckung sowie des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden sollen. Die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, sollte die Weiterübermittlung auch an besondere Bedingungen knüpfen können. Diese besonderen Bedingungen können zum Beispiel in Bearbeitungscodes dargelegt werden.

(66) Die Kommission sollte mit Wirkung für die gesamte Union beschließen können, dass bestimmte Drittländer, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen sollten personenbezogene Daten ohne besondere Genehmigung an diese Länder übermittelt werden können, es sei denn, dass ein anderer Mitgliedstaat, von dem die Daten stammen, die Übermittlung zu genehmigen hat.

(67) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlandes oder eines Gebiets oder eines bestimmten Sektors in einem Drittland berücksichtigen, inwieweit in einem bestimmten Drittland 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, die nationale Sicherheit und öffentliche Ordnung sowie das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor in einem Drittland 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 im Wesentlichen dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen 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 behördliche und gerichtliche Rechtsbehelfe eingeräumt werden.

(68) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlandes oder der internationalen 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 Drittlandes 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 durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss (im Folgenden „Ausschuss") konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet. Die Kommission sollte ferner alle maßgeblichen Angemessenheitsbeschlüsse berücksichtigen, die sie nach Artikel 45 der Verordnung (EU) 2016/679 angenommen hat.

(69) Die Kommission sollte die Wirksamkeit von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem spezifischen Sektor in einem Drittland oder einer internationalen Organisation überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung ihrer 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.

(70) Die Kommission sollte auch feststellen können, dass ein Drittland, ein Gebiet oder ein spezifischer Sektor in einem Drittland 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 Richtlinie in Bezug auf Datenübermittlung vorbehaltlich geeigneter Garantien und Ausnahmen für bestimmte Fälle werden erfüllt. Es sollten Verfahren für 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.

(71) Datenübermittlungen, die nicht auf der Grundlage eines Angemessenheitsbeschlusses erfolgen, sollten nur dann zulässig sein, wenn in einem rechtsverbindlichen Instrument geeignete Garantien festgelegt sind, die den Schutz personenbezogener Daten gewährleisten, oder wenn der Verantwortliche alle Umstände beurteilt hat, die bei der Datenübermittlung eine Rolle spielen, und auf der Grundlage dieser Beurteilung zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen. Solche rechtsverbindlichen Instrumente könnten beispielsweise rechtsverbindliche bilaterale Abkommen sein, die von den Mitgliedstaaten geschlossen und in ihre Rechtsordnung übernommen wurden und von ihren betroffenen Personen durchgesetzt werden können und die sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe beachtet werden. Der Verantwortliche sollte Kooperationsvereinbarungen zwischen Europol oder Eurojust und Drittländern berücksichtigen können, die den Austausch personenbezogener Daten ermöglichen, wenn er alle Umstände im Zusammenhang mit der Datenübermittlung beurteilt. Der Verantwortliche sollte außerdem berücksichtigen können, dass die Übermittlung personenbezogener Daten Geheimhaltungspflichten und dem Grundsatz der Spezialität unterliegt, damit gewährleistet wird, dass die Daten nicht zu anderen Zwecken als zu den Zwecken, zu denen sie übermittelt wurden, verarbeitet werden. Darüber hinaus sollte der Verantwortliche berücksichtigen, dass die personenbezogenen Daten nicht verwendet werden, um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken. Diese Bedingungen könnten zwar als geeignete Garantien angesehen werden, die die Datenübermittlung zulassen, jedoch sollte der Verantwortliche zusätzliche Garantien verlangen können.

(72) Sind weder ein Angemessenheitsbeschluss noch geeignete Garantien vorhanden, so sollte eine Übermittlung oder eine Kategorie von Übermittlungen nur in bestimmten Fällen erfolgen können, in denen dies erforderlich ist: zur Wahrung wesentlicher Interessen der betroffenen oder einer anderen Person; zum Schutz berechtigter Interessen der betroffenen Person, wenn dies nach dem Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist; zur Abwehr einer unmittelbaren, ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes; in einem Einzelfall 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; oder in einem Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Diese Ausnahmen sollten restriktiv ausgelegt werden, häufige, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen in großem Umfang ausschließen und daher auf unbedingt notwendige Daten beschränkt sein. Derartige Übermittlungen sollten dokumentiert werden, und die entsprechende Dokumentation sollte der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden, damit diese die Rechtmäßigkeit der Übermittlung überprüfen kann.

(73) Die zuständigen Behörden der Mitgliedstaaten wenden die geltenden bilateralen oder multilateralen internationalen Übereinkünfte, die mit Drittländern auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geschlossen wurden, für den Austausch maßgeblicher Informationen an, um ihnen zu ermöglichen, die ihnen rechtlich zugewiesenen Aufgaben wahrzunehmen. Grundsätzlich erfolgt dies über die im betreffenden Drittland für die Zwecke dieser Richtlinie zuständigen Behörden oder zumindest in Zusammenarbeit mit diesen Behörden des Drittlandes, mitunter auch dann, wenn keine bilaterale oder multilaterale internationale Übereinkunft existiert. In speziellen Einzelfällen können die regulären Verfahren, die eine Kontaktaufnahme mit dieser Behörde in dem betreffenden Drittland vorschreiben, wirkungslos oder ungeeignet sein, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden konnte oder weil diese Behörde in dem betreffenden Drittland die Rechtsstaatlichkeit oder die internationalen Menschenrechtsbestimmungen nicht achtet, so dass die zuständigen Behörden der Mitgliedstaaten beschließen

können, die personenbezogenen Daten direkt an in Drittländern niedergelassene Empfänger zu übermitteln. Dies kann der Fall sein, wenn es dringend geboten ist, personenbezogene Daten zu übermitteln, um das Leben einer Person zu schützen, die Gefahr läuft, Opfer einer Straftat zu werden, oder um die unmittelbar bevorstehende Begehung einer Straftat, einschließlich einer terroristischen Straftat, zu verhindern. Auch wenn eine solche Übermittlung zwischen zuständigen Behörden und in Drittländern niedergelassenen Empfängern nur in speziellen Einzelfällen erfolgen sollte, sollte diese Richtlinie die Voraussetzungen für die Regelung solcher Fälle vorsehen. Diese Bestimmungen sollten nicht als Ausnahmen von geltenden bilateralen oder multilateralen internationalen Übereinkünften auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit betrachtet werden. Diese Vorschriften sollten zusätzlich zu den sonstigen Vorschriften dieser Richtlinie gelten, insbesondere den Vorschriften über die Rechtmäßigkeit der Verarbeitung und Kapitel V.

(74) Wenn personenbezogene Daten in ein anderes Land übermittelt werden, kann dies dazu führen, dass natürliche Personen weniger Möglichkeiten haben, ihre Datenschutzrechte wahrzunehmen und sich gegen eine unrechtmäßige Nutzung oder Offenlegung dieser Daten 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 grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse und durch widersprüchliche Rechtsordnungen behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, um ihnen den Informationsaustausch mit Aufsichtsbehörden in anderen Ländern zu erleichtern.

(75) Die Einrichtung von Aufsichtsbehörden in den Mitgliedstaaten, die ihre Aufgaben völlig unabhängig erfüllen können, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Aufsichtsbehörden sollten die Anwendung der nach dieser Richtlinie erlassenen Vorschriften überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.

(76) Die Mitgliedstaaten können einer bereits gemäß der Verordnung (EU) 2016/679 errichteten Aufsichtsbehörde die Verantwortung für die Aufgaben übertragen, die von den nach dieser Richtlinie einzurichtenden nationalen Aufsichtsbehörden auszuführen sind.

(77) Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde einrichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht. Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über eigene, öffentliche, jährliche Haushaltspläne verfügen, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

(78) Die Aufsichtsbehörden sollten unabhängigen Kontroll- oder Überwachungsmechanismen hinsichtlich ihrer Ausgaben unterliegen, sofern diese Finanzkontrolle ihre Unabhängigkeit nicht berührt.

(79) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Recht der Mitgliedstaaten geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des betreffenden Mitgliedstaats auf Vorschlag der Regierung oder eines Regierungsmitglieds oder des Parlaments oder dessen Kammer oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder integer handeln, 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. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollte ihr Personal von der Aufsichtsbehörde selbst ausgewählt werden; dabei kann eine unabhängige, nach dem Recht des Mitgliedstaats betraute Stelle eingeschaltet werden.

(80) Obgleich diese Richtlinie auch für die Tätigkeit der nationalen Gerichte und anderer Justizbehörden gilt, sollte sich die Zuständigkeit der Aufsichtsbehörden nicht auf die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Datenverarbeitungen erstrecken, damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben gewahrt bleibt. Diese Ausnahme sollte allerdings begrenzt werden auf justizielle Tätigkeiten in Gerichtssachen und sich nicht auf andere Tätigkeiten beziehen, mit denen Richter nach dem Recht der Mitgliedstaaten betraut werden können. Die Mitgliedstaaten sollten außerdem vorsehen können, dass sich die Zuständigkeit der Aufsichtsbehörde nicht auf die Überwachung der Verarbeitung personenbezogener Daten erstreckt, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit, beispielsweise Staatsanwaltschaften, erfolgt. Die Einhaltung der Vorschriften dieser Richtlinie durch die Gerichte und andere unabhängige Justizbehörden unterliegt in jedem Fall stets der unabhängigen Überwachung gemäß Artikel 8 Absatz 3 der Charta.

(81) Jede Aufsichtsbehörde sollte sich mit Beschwerden von betroffenen Personen befassen und die Angelegenheit untersuchen oder an die zuständige Aufsichtsbehörde übermitteln. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich einer gerichtlichen Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, so sollte die betroffene Person über den Zwischenstand informiert werden.

(82) Um die wirksame, zuverlässige und einheitliche Überwachung der Einhaltung und Durchsetzung dieser Richtlinie in der gesamten Union gemäß dem AEUV in der Auslegung durch den Gerichtshof sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse, die notwendige Instrumente zur Erfüllung ihrer Aufgaben darstellen. Ihre Befugnisse dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschließlich der Ermittlung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren. Unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten sollten die Aufsichtsbehörden außerdem die Befugnis haben, Verstöße gegen diese Richtlinie den Justizbehörden zur Kenntnis zu bringen oder Gerichtsverfahren anzustrengen. 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 Richtlinie 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 die betroffene Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für sie zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Recht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Der Erlass eines rechtsverbindlichen Beschlusses sollte in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, einer gerichtlichen Überprüfung unterliegen.

(83) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und einander Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung der nach dieser Richtlinie erlassenen Vorschriften gewährleistet ist.

(84) Der Ausschuss sollte zur einheitlichen Anwendung dieser Richtlinie in der Union beitragen, einschließlich der Beratung der Kommission und der Förderung der Zusammenarbeit der Aufsichtsbehörden in der Union.

(85) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten aufgrund von nach dieser Richtlinie erlassenen Vorschriften 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 zuständige Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, so 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.

(86) Jede natürliche oder juristische Person sollte 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. Dieses Recht umfasst jedoch nicht andere — 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 Recht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit maßgeblichen Sach- und Rechtsfragen zu prüfen, einschließt.

(87) Betroffene Personen, die sich in ihren Rechten gemäß dieser Richtlinie verletzt sehen, sollten das Recht haben, Einrichtungen, die sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Schutzes

ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, zu beauftragen, in ihrem Namen eine Beschwerde bei einer Aufsichtsbehörde einzureichen und einen gerichtlichen Rechtsbehelf einzulegen. Das Recht betroffener Personen auf Vertretung sollte das Verfahrensrecht der Mitgliedstaaten unberührt lassen, nach dem eine obligatorische Vertretung betroffener Personen durch einen Rechtsanwalt im Sinne der Richtlinie 77/249/EWG des Rates ([1]) vor nationalen Gerichten erforderlich sein kann.

(88) Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die gegen nach dieser Richtlinie erlassene Vorschriften verstößt, sollten von dem Verantwortlichen oder einer anderen nach dem Recht der Mitgliedstaaten zuständigen Behörde ersetzt werden. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit und auf eine Art und Weise ausgelegt werden, die den Zielen dieser Richtlinie in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Wird auf eine Verarbeitung Bezug genommen, die unrechtmäßig ist oder nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften steht, so gilt dies auch für Verarbeitungen, die gegen gemäß dieser Richtlinie erlassene Durchführungsrechtsakte verstoßen. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.

(89) Gegen jede natürliche oder juristische — privatem oder öffentlichem Recht unterliegende — Person, die gegen diese Richtlinie verstößt, sollten Sanktionen verhängt werden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sind, und alle Maßnahmen zur Anwendung der Sanktionen treffen.

(90) Um einheitliche Bedingungen für die Anwendung dieser Richtlinie sicherzustellen, sollten der Kommission Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: die Angemessenheit des Datenschutzniveaus in einem Drittland, in einem Gebiet oder einem spezifischen Sektor in einem Drittland oder in einer internationalen Organisation, das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([2]) ausgeübt werden.

(91) Durchführungsrechtsakte über die Angemessenheit des Datenschutzniveaus in einem Drittland, in einem Gebiet oder einem spezifischen Sektor in einem Drittland oder in einer internationalen Organisation, über das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.

(92) Die Kommission sollte in hinreichend begründeten Fällen äußerster Dringlichkeit, die ein Drittland, ein Gebiet oder einen spezifischen Sektor in einem Drittland oder eine internationale Organisation betreffen, die kein angemessenes Schutzniveau mehr gewährleisten, sofort geltende Durchführungsrechtsakte erlassen.

(93) Da die Ziele dieser Richtlinie, nämlich die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten und den ungehinderten Austausch personenbezogener Daten im Verkehr zwischen den zuständigen Behörden innerhalb der Union zu gewährleisten, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(94) Besondere Bestimmungen, die in vor Erlass dieser Richtlinie im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander sowie den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen im

([1]) Richtlinie 77/249/EWG des Rates vom 22. März 1977 zur Erleichterung der tatsächlichen Ausübung des freien Dienstleistungsverkehrs der Rechtsanwälte (ABl. L 78 vom 26.3.1977, S. 17).

([2]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

Anwendungsbereich dieser Richtlinie regeln, sollten unberührt bleiben, beispielsweise die besonderen Bestimmungen betreffend den Schutz personenbezogener Daten gemäß dem Beschluss 2008/615/JI des Rates ([1]) oder Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union ([2]). Da Artikel 8 der Charta und Artikel 16 AEUV vorschreiben, dass das Grundrecht auf Schutz personenbezogener Daten in der Union einheitlich angewendet werden sollte, sollte die Kommission das Verhältnis zwischen dieser Richtlinie und den vor ihrem Erlass angenommenen Rechtsakten, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander oder den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen regeln, daraufhin prüfen, inwieweit die besonderen Bestimmungen dieser Rechtsakte an diese Richtlinie angepasst werden müssen. Die Kommission sollte gegebenenfalls Vorschläge zur Gewährleistung einheitlicher Rechtsvorschriften in Bezug auf die Verarbeitung personenbezogener Daten unterbreiten.

(95) Zur Gewährleistung eines umfassenden und einheitlichen Schutzes personenbezogener Daten in der Union sollten internationale Übereinkünfte, die von den Mitgliedstaaten vor Inkrafttreten dieser Richtlinie geschlossen wurden und die im Einklang mit dem maßgeblichen vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht stehen, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden.

(96) Die Mitgliedstaaten sollten gehalten sein, diese Richtlinie innerhalb von höchstens zwei Jahren nach ihrem Inkrafttreten umzusetzen. Verarbeitungen, die zu diesem Zeitpunkt bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Richtlinie mit ihr in Einklang gebracht werden. Stehen die Verarbeitungen jedoch im Einklang mit dem vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht, so sollten die Anforderungen der vorliegenden Richtlinie betreffend die vorherige Konsultation der Aufsichtsbehörde nicht für Verarbeitungsvorgänge gelten, die bereits vor diesem Zeitpunkt begonnen wurden, da diese Anforderungen naturgemäß vor der Verarbeitung erfüllt sein müssen. Nehmen Mitgliedstaaten die längere Umsetzungsfrist, die sieben Jahre nach dem Inkrafttreten dieser Richtlinie endet, in Anspruch, um den Protokollierungspflichten für vor dem Inkrafttreten dieser Richtlinie eingerichtete automatisierte Verarbeitungssysteme nachzukommen, so sollte der Verantwortliche oder der Auftragsverarbeiter über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Datenverarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.

(97) Diese Richtlinie lässt die Vorschriften zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie nach Maßgabe der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates ([3]) unberührt.

(98) Der Rahmenbeschluss 2008/977/JI sollte daher aufgehoben werden.

(99) Nach Artikel 6a des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Bestimmungen dieser Richtlinie 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 AEUV fallen, für das Vereinigte Königreich und Irland nicht bindend, wenn das Vereinigte Königreich und Irland nicht durch die Vorschriften gebunden sind, die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften eingehalten werden müssen.

(100) Nach den Artikeln 2 und 2a des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks ist Dänemark durch die Bestimmungen dieser Richtlinie, die sich auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten beziehen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet. Da diese Richtlinie den Schengen-Besitzstand gemäß dem Dritten Teil Titel V AEUV ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten nach Erlass dieser Richtlinie, ob es sie in nationales Recht umsetzt.

(101) Für Island und Norwegen stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([4])

([1]) Rahmenbeschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1).

([2]) Rechtsakt des Rates vom 29. Mai 2000 über die Erstellung — gemäß Artikel 34 des Vertrags über die Europäische Union — des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. C 197 vom 12.7.2000, S. 1).

([3]) Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

([4]) ABl. L 176 vom 10.7.1999, S. 36.

(102) Für die Schweiz stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([1])

(103) Für Lichtenstein stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([2])

(104) Diese Richtlinie steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta anerkannt wurden und im AEUV verankert sind, insbesondere mit dem Recht auf Achtung des Privat- und Familienlebens, dem Recht auf Schutz personenbezogener Daten sowie dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren. Die Einschränkungen dieser Rechte stehen im Einklang mit Artikel 52 Absatz 1 der Charta, da sie erforderlich sind, um den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und der Freiheiten anderer zu entsprechen.

(105) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission vom 28. September 2011 zu erläuternden Dokumenten haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen einzelstaatlicher Umsetzungsmaßnahmen erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

(106) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat seine Stellungnahme am 7. März 2012 abgegeben ([3]).

(107) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, die Bestimmungen über die Ausübung der Rechte der betroffenen Personen auf Unterrichtung, Auskunft und Berichtigung oder Löschung personenbezogener Daten und Beschränkung der Verarbeitung im Rahmen eines Strafverfahrens sowie mögliche Beschränkungen dieser Rechte in ihr einzelstaatliches Strafverfahrensrecht umzusetzen —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Richtlinie enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(2) Gemäß dieser Richtlinie haben die Mitgliedstaaten

a) die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und

b) sicherzustellen, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union — sofern er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen ist — nicht aus Gründen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verbunden sind, eingeschränkt oder verboten wird.

([1]) ABl. L 53 vom 27.2.2008, S. 52.
([2]) ABl. L 160 vom 18.6.2011, S. 21.
([3]) ABl. C 192, 30.6.2012, S. 7

(3) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken.

(2) Diese Richtlinie 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.

(3) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten

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

b) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie 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. „zuständige Behörde“

   a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

   b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

8. „Verantwortlicher“ die zuständige Behörde, 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;

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

10. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen 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 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;

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

12. „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;

13. „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;

14. „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;

15. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 eingerichtete unabhängige staatliche Stelle;

16. „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

Artikel 4

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor dass personenbezogene Daten

a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; 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,

e) 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,

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Eine Verarbeitung durch denselben oder einen anderen Verantwortlichen für einen anderen der in Artikel 1 Absatz 1 genannten Zwecke als den, für den die personenbezogenen Daten erhoben werden, ist erlaubt, sofern

a) der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und

b) die Verarbeitung für diesen anderen Zweck nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich und verhältnismäßig ist.

(3) Die Verarbeitung durch denselben oder einen anderen Verantwortlichen kann die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für die in Artikel 1 Absatz 1 genannten Zwecke umfassen, sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorhanden sind.

(4) Der Verantwortliche ist für die Einhaltung der Absätze 1, 2 und 3 verantwortlich und muss deren Einhaltung nachweisen können.

Artikel 5

Fristen für die Speicherung und Überprüfung

Die Mitgliedstaaten sehen vor, dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Durch verfahrensrechtliche Vorkehrungen ist sicherzustellen, dass diese Fristen eingehalten werden.

Artikel 6

Unterscheidung verschiedener Kategorien betroffener Personen

Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter:

a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,

b) verurteilte Straftäter,

c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen.

Artikel 7

Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der personenbezogenen Daten

(1) Die Mitgliedstaaten sehen vor, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird.

(2) Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden alle angemessenen Maßnahmen ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Zu diesem Zweck überprüft jede zuständige Behörde, soweit durchführbar, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit die erforderlichen Informationen beigefügt, die es der empfangenden zuständigen Behörde gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.

(3) Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 16 eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen.

Artikel 8

Rechtmäßigkeit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt.

(2) Im Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs dieser Richtlinie regelt, werden zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben.

Artikel 9

Besondere Verarbeitungsbedingungen

(1) Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die Verordnung (EU) 2016/679, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(2) Sind nach dem Recht der Mitgliedstaaten zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den für die in Artikel 1 Absatz 1 genannten Zwecke wahrgenommenen Aufgaben decken, gilt die Verordnung (EU) 2016/679 für die Verarbeitung zu diesen Zwecken — wozu auch im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke zählen —, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(3) Die Mitgliedstaaten sehen vor, dass immer dann, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung besondere Bedingungen gelten, die übermittelnde zuständige Behörde den Empfänger der Daten darauf hinweist, dass diese Bedingungen gelten und einzuhalten sind.

(4) Die Mitgliedstaaten sehen vor, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen keine Bedingungen nach Absatz 3 anwendet, die nicht auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

Artikel 10

Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder 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 ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

a) wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist

b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

Artikel 11

Automatisierte Entscheidungsfindung im Einzelfall

(1) Die Mitgliedstaaten sehen vor, dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung — einschließlich Profiling —, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, verboten ist, es sei denn, sie ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, erlaubt.

(2) Entscheidungen nach Absatz 1 dieses Artikels dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 10 beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10 diskriminiert werden, ist nach dem Unionsrecht verboten.

KAPITEL III

Rechte der betroffenen Person

Artikel 12

Mitteilungen und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche alle angemessenen Maßnahmen trifft, um der betroffenen Person alle Informationen gemäß Artikel 13 sowie alle Mitteilungen gemäß den Artikeln 11, 14 bis 18 und 31, die sich auf die Verarbeitung beziehen, in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Übermittlung der Informationen erfolgt in einer beliebigen geeigneten Form, wozu auch die elektronische Übermittlung zählt. Grundsätzlich übermittelt der Verantwortliche die Informationen in derselben Form, in der er den Antrag erhalten hat.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Ausübung der den betroffenen Personen gemäß den Artikeln 11 und 14 bis 18 zustehenden Rechte erleichtert.

(3) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person unverzüglich schriftlich darüber in Kenntnis setzt, wie mit ihrem Antrag verfahren wurde.

(4) Die Mitgliedstaaten sehen vor, dass die Informationen gemäß Artikel 13 und alle gemachten Mitteilungen und getroffenen Maßnahmen gemäß den Artikeln 11, 14 bis 18 und 31 unentgeltlich zur Verfügung gestellt werden. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

a) eine angemessene Gebühr verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) er kann sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(5) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 14 oder 16 stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Artikel 13

Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der betroffenen Person zumindest die folgenden Informationen zur Verfügung stellt:

a) den Namen und die Kontaktdaten des Verantwortlichen,

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden,

d) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,

e) das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) Zusätzlich zu den in Absatz 1 genannten Informationen sehen die Mitgliedstaaten durch Rechtsvorschriften vor, dass der Verantwortliche der betroffenen Person in besonderen Fällen die folgenden zusätzlichen Informationen erteilt, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:

a) die Rechtsgrundlage der Verarbeitung,

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

c) gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,

d) erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

(3) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, nach denen die Unterrichtung der betroffenen Person gemäß Absatz 2 soweit und so lange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) zum Schutz der öffentlichen Sicherheit,

d) zum Schutz der nationalen Sicherheit,

e) zum Schutz der Rechte und Freiheiten anderer.

(4) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen zur Festlegung der Verarbeitungskategorien erlassen, für die einer der Buchstaben des Absatz 3 vollständig oder teilweise zur Anwendung kommt.

Artikel 14

Auskunftsrecht der betroffenen Person

Vorbehaltlich des Artikels 15 sehen die Mitgliedstaaten vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über personenbezogene Daten und zu folgenden Informationen zu erhalten:

a) die Zwecke der Verarbeitung und deren Rechtsgrundlage,

b) die Kategorien personenbezogener Daten, die verarbeitet werden,

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, 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 personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen,

f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,

g) Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.

Artikel 15

Einschränkung des Auskunftsrechts

(1) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, die zu nachstehenden Zwecken das Recht der betroffenen Person auf Auskunft teilweise oder vollständig einschränken, soweit und so lange wie diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

(2) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen zur Festlegung der Verarbeitungskategorien erlassen, für die Absatz 1 Buchstaben a bis e vollständig oder teilweise zur Anwendung kommen.

(3) Für die in den Absätzen 1 und 2 genannten Fälle sehen die Mitgliedstaaten vor, dass der Verantwortliche die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür unterrichtet. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in Absatz 1 genannten Zwecke zuwiderliefe. Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die sachlichen oder rechtlichen Gründe für die Entscheidung dokumentiert. Diese Angaben sind der Aufsichtsbehörde zur Verfügung zu stellen.

Artikel 16

Recht auf Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung

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

(2) Die Mitgliedstaaten verlangen vom Verantwortlichen, personenbezogene Daten unverzüglich zu löschen, und sehen vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten unverzüglich zu verlangen, wenn die Verarbeitung gegen die nach den Artikeln 4, 8 und 10 erlassenen Vorschriften verstößt oder wenn die personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, der der Verantwortliche unterliegt.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

a) die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder

b) die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen.

Unterliegt die Verarbeitung einer Beschränkung gemäß Unterabsatz 1 Buchstabe a, unterrichtet der Verantwortliche die betroffene Person, bevor er die Beschränkung aufhebt.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung und über die Gründe für die Verweigerung unterrichtet. Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, die zu nachstehenden Zwecken die Pflicht, diese Informationen zur Verfügung zu stellen, teilweise oder vollständig einschränken, soweit diese Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlungen oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen Daten stammen, mitteilt.

(6) Die Mitgliedstaaten sehen vor, dass in Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1, 2 und 3 der Verantwortliche die Empfänger in Kenntnis setzt und dass die Empfänger die ihrer Verantwortung unterliegenden personenbezogenen Daten berichtigen, löschen oder deren Verarbeitung einschränken.

Artikel 17

Ausübung von Rechten durch die betroffene Person und Prüfung durch die Aufsichtsbehörde

(1) In den in Artikel 13 Absatz 3, Artikel 15 Absatz 3 und Artikel 16 Absatz 4 genannten Fällen erlassen die Mitgliedstaaten Maßnahmen, in denen vorgesehen ist, dass die Rechte der betroffenen Person auch über die zuständige Aufsichtsbehörde ausgeübt werden können.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, ihr Recht auf Befassung der Aufsichtsbehörde gemäß Absatz 1 auszuüben.

(3) Wird das in Absatz 1 genannte Recht ausgeübt, unterrichtet die Aufsichtsbehörde die betroffene Person zumindest darüber, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Aufsichtsbehörde erfolgt sind. Die Aufsichtsbehörde hat zudem die betroffene Person über ihr Recht auf einen gerichtlichen Rechtsbehelf zu unterrichten.

Artikel 18

Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren

Die Mitgliedstaaten können vorsehen, dass die Ausübung der Rechte nach den Artikeln 13, 14 und16 im Einklang mit dem Recht der Mitgliedstaaten erfolgt, wenn es um personenbezogene Daten in einer gerichtlichen Entscheidung oder einem Dokument oder einer Verfahrensakte geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden.

KAPITEL IV

Verantwortlicher und Auftragsverarbeiter

Abschnitt 1

Allgemeine Pflichten

Artikel 19

Pflichten des Verantwortlichen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche 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 umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie 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.

Artikel 20

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche 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 sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, 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.

Artikel 21

Gemeinsam Verantwortliche

(1) Die Mitgliedstaaten sehen vor, dass in dem Fall, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sie gemeinsam Verantwortliche sind. Sie legen in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben gemäß dieser Richtlinie fest insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß Artikel 13 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch das Unionsrecht oder das Recht der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung wird eine Anlaufstelle für die betroffenen Personen angegeben. Die Mitgliedstaaten können angeben, welcher der gemeinsam Verantwortlichen als zentrale Anlaufstelle für die betroffenen Personen handeln kann, wenn es um die Ausübung ihrer Rechte geht.

(2) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 können die Mitgliedstaaten vorsehen, dass die betroffene Person ihre Rechte im Rahmen der nach dieser Richtlinie erlassenen Vorschriften bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.

Artikel 22

Auftragsverarbeiter

(1) Die Mitgliedstaaten sehen vor, dass in dem Fall, dass eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, dieser nur mit Auftragsverarbeitern arbeitet, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Richtlinie erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Die Mitgliedstaaten sehen vor, dass der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt. Im Fall einer allgemeinen schriftlichen Genehmigung unterrichtet der Auftragsverarbeiter den Verantwortlichen 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 Mitgliedstaaten sehen vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und der den 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 festlegt. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) nur auf Weisung des Verantwortlichen handelt,

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

c) den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,

d) alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen — nach Wahl des Verantwortlichen — zurückgibt bzw. löscht und bestehende Kopien vernichtet, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

e) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt,

f) die in den Absätzen 2 und 3 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält.

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

(5) Ein Auftragsverarbeiter, der unter Verstoß gegen diese Richtlinie die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 23

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Die Mitgliedstaaten sehen vor, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, 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 24

Verzeichnis von Verarbeitungstätigkeiten

(1) Die Mitgliedstaaten sehen vor, dass jeder Verantwortliche ein Verzeichnis aller Kategorien von Tätigkeiten der Verarbeitung, die seiner Zuständigkeit unterliegen, führt. Dieses Verzeichnis enthält alle der folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen, gegebenenfalls des gemeinsam mit ihm Verantwortlichen und eines etwaigen Datenschutzbeauftragten,

b) die Zwecke der Verarbeitung,

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

d) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

e) gegebenenfalls die Verwendung von Profiling,

f) gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation,

g) Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind,

h) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten,

i) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 29 Absatz 1.

(2) Die Mitgliedstaaten sehen vor, dass jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führt, die Folgendes enthält:

a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie 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, wenn vom Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation,

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 29 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Der Verantwortliche und der Auftragsverarbeiter stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Artikel 25

Protokollierung

(1) Die Mitgliedstaaten sehen vor, dass in automatisierten Verarbeitungssystemen zumindest die folgenden Verarbeitungsvorgänge protokolliert werden: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.

(2) Die Protokolle werden ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet.

(3) Der Verantwortliche sowie der Auftragsverarbeiter stellen die Protokolle der Aufsichtsbehörde auf Anforderung zur Verfügung.

Artikel 26

Zusammenarbeit mit der Aufsichtsbehörde

Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.

Artikel 27

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 sehen die Mitgliedstaaten vor, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.

(2) Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird.

Artikel 28

Vorherige Konsultation der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Aufsichtsbehörde konsultiert, wenn

a) aus einer Datenschutz-Folgenabschätzung gemäß Artikel 27 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder

b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

(2) Die Mitgliedstaaten sehen vor, dass bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen, die Aufsichtsbehörde konsultiert wird.

(3) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellen kann, die der Pflicht zur vorherigen Konsultation nach Absatz 1 unterliegen.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der Aufsichtsbehörde die Datenschutz-Folgenabschätzung gemäß Artikel 27 vorlegt und ihr auf Anfrage alle sonstigen Informationen übermittelt, die sie benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(5) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, wenn sie der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 dieses Artikels gegen die nach dieser Richtlinie erlassenen Vorschriften verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen unterbreitet und ihre in Artikel 47 genannten Befugnisse ausüben kann. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um einen weiteren Monat verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortliche oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung.

Abschnitt 2

Sicherheit personenbezogener Daten

Artikel 29

Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter 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 geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 10.

(2) Die Mitgliedstaaten sehen im Hinblick auf die automatisierte Verarbeitung vor, dass der Verantwortliche oder der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen ergreift, die Folgendes bezwecken:

a) Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

b) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle),

c) Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

d) Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

e) Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugangskontrolle),

f) 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),

g) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

h) Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

i) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),

j) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Artikel 30

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche diese unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde meldet, 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 personenbezogener Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,

b) Name und 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 Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der 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) Die Mitgliedstaaten sehen vor, dass der Verantwortliche Verletzungen des Schutzes personenbezogener Daten nach Absatz 1 einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentiert. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

(6) Die Mitgliedstaaten sehen vor, dass, soweit von der Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaats übermittelt wurden, die in Absatz 3 genannten Informationen dem Verantwortlichen jenes Mitgliedstaats unverzüglich übermittelt werden.

Artikel 31

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Die Mitgliedstaaten sehen vor, dass, wenn die Verletzung des Schutzes personenbezogener voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, der Verantwortliche die betroffene Person unverzüglich von der Verletzung benachrichtigt.

(2) Die in Absatz 1 dieses Artikels 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 30 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.

(5) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 dieses Artikels kann unter zu den in Artikel 13 Absatz 3 genannten Voraussetzungen und aus den dort genannten Gründen aufgeschoben, eingeschränkt oder unterlassen werden.

Abschnitt 3

Datenschutzbeauftragter

Artikel 32

Benennung eines Datenschutzbeauftragten

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche einen Datenschutzbeauftragten benennt. Mitgliedstaaten können Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von dieser Pflicht befreien.

(2) 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 34 genannten Aufgaben.

(3) Ein Datenschutzbeauftragter kann für mehrere zuständige Behörden gemeinsam ernannt werden, wobei deren Organisationsstruktur und Größe Rechnung getragen wird.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitteilt.

Artikel 33

Stellung des Datenschutzbeauftragten

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche sicherstellt, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 34, indem er die hierfür erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

Artikel 34

Aufgaben des Datenschutzbeauftragten

Die Mitgliedstaaten sehen vor, dass der Verantwortliche den Datenschutzbeauftragten mit zumindest folgenden Aufgaben betraut:

a) Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Richtlinie sowie anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten,

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

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 27,

d) Zusammenarbeit mit der Aufsichtsbehörde,

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 28, und gegebenenfalls Beratung zu allen sonstigen Fragen.

KAPITEL V

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Artikel 35

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor, dass jedwede von einer zuständigen Behörde vorgenommene Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, einschließlich der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation, nur unter Einhaltung der nach Maßgabe anderer Bestimmungen dieser Richtlinie erlassenen nationalen Bestimmungen, zulässig ist, wenn die in diesem Kapitel festgelegten Bedingungen eingehalten werden, nämlich

a) die Übermittlung für die in Artikel 1 Absatz 1 genannten Zwecke erforderlich ist;

b) die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde ist, übermittelt werden;

c) in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor in Einklang mit seinem nationalen Recht genehmigt hat;

d) die Kommission gemäß Artikel 36 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des Artikels 37 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß Artikel 36 vorliegt und keine geeigneten Garantien im Sinne des Artikels 37 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß Artikel 38 anwendbar sind und

e) im Fall der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, oder eine andere zuständige Behörde des gleichen Mitgliedstaats die Weiterübermittlung genehmigt nach gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden.

(2) Die Mitgliedstaaten sehen vor, dass Übermittlungen ohne vorherige Genehmigung durch einen anderen Mitgliedstaat gemäß Absatz 1 Buchstabe c nur dann zulässig sind, wenn die Übermittlung der personenbezogenen Daten erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die Behörde, die für die Erteilung der vorherigen Genehmigung zuständig ist, wird unverzüglich unterrichtet.

(3) Sämtliche Bestimmungen dieses Kapitels werden angewendet, um sicherzustellen, dass das durch diese Richtlinie gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 36

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, 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 Datenübermittlungen bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigt die Kommission insbesondere

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und der Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, 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 Rechtsinstrumenten sowie aus der Teilnahme des Drittlandes 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 beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 dieses Artikels bietet. In dem Durchführungsrechtsakt wird ein Mechanismus für die regelmäßige Überprüfung vorgesehen, die mindestens alle vier Jahre erfolgt und bei der allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b dieses Artikels genannte Aufsichtsbehörde oder die dort genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 erlassenen Beschlüsse 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 spezifische Sektoren 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 in Artikel 58 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen gemäß dem in Artikel 58 Absatz 3 genannten Verfahren erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 58 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 Beschluss nach Absatz 5 geführt hat.

(7) Die Mitgliedstaaten sehen vor, dass Übermittlungen personenbezogener Daten an das betreffende Drittland, an das Gebiet oder einen oder mehrere spezifischen Sektoren in einem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 37 und 38 durch einen Beschluss nach Absatz 5 nicht berührt werden.

(8) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* und auf ihrer Website eine Liste aller Drittländern beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese ein beziehungsweise kein angemessenes Schutzniveau für personenbezogene Daten bieten.

Artikel 37

Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Liegt kein Beschluss nach Artikel 36 Absatz 3 vor, so sehen die Mitgliedstaaten vor, dass eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen darf, wenn

a) in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

b) der Verantwortliche alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche unterrichtet die Aufsichtsbehörde über Kategorien von Übermittlungen gemäß Absatz 1 Buchstabe b.

(3) Übermittlungen gemäß Absatz 1 Buchstabe b werden dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt.

Artikel 38

Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 36 vorliegt noch geeignete Garantien nach Artikel 37 bestehen, sehen die Mitgliedstaaten vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig ist, wenn die Übermittlung aus einem der folgenden Gründe erforderlich ist

a) zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person,

b) zur Wahrung berechtigter Interessen der betroffenen Person, wenn dies im Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist,

c) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes,

d) im Einzelfall für die in Artikel 1 Absatz 1 genannten Zwecke, oder

e) im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Artikel 1 Absatz 1 genannten Zwecken.

(2) Personenbezogene Daten dürfen nicht übermittelt werden, wenn die übermittelnde zuständige Behörde feststellt, dass Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung im Sinne des Absatzes 1 Buchstaben d und e überwiegen.

(3) Übermittlungen gemäß Absatz 1 werden dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogene Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt.

Artikel 39

Übermittlung personenbezogener Daten an in Drittländern niedergelassene Empfänger

(1) Abweichend von Artikel 35 Absatz 1 Buchstabe b und unbeschadet der in Absatz 2 dieses Artikels genannten internationalen Übereinkünfte kann das Unionsrecht oder das Recht der Mitgliedstaaten vorsehen, dass die in Artikel 3 Nummer 7 Buchstabe a genannten zuständigen Behörden im speziellen Einzelfall nur dann personenbezogene Daten direkt an in Drittländern niedergelassene Empfänger übermitteln dürfen, wenn die übrigen Bestimmungen dieser Richtlinie eingehalten werden und alle der folgende Voraussetzungen gegeben sind:

a) Die Übermittlung ist für die Ausübung einer Aufgabe der übermittelnden zuständigen Behörde gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten für die in Artikel 1 Absatz 1 genannten Zwecke unbedingt erforderlich,

b) die übermittelnde zuständige Behörde stellt fest, dass im konkreten Fall keine Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,

c) die übermittelnde zuständige Behörde hält die Übermittlung an eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland für wirkungslos oder ungeeignet, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden kann,

d) die für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland wird unverzüglich unterrichtet, es sei denn, dies ist wirkungslos oder ungeeignet, und

e) die übermittelnde zuständige Behörde teilt dem Empfänger den festgelegten Zweck oder die festgelegten Zwecke mit, für die die personenbezogenen Daten nur dann durch diesen verarbeitet werden dürfen, wenn eine derartige Verarbeitung erforderlich ist.

(2) Eine internationale Übereinkunft im Sinne des Absatzes 1 ist jede in Kraft befindliche bilaterale oder multilaterale internationale Übereinkunft zwischen Mitgliedstaaten und Drittländern im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.

(3) Die übermittelnde zuständige Behörde unterrichtet die Aufsichtsbehörde über die Übermittlungen gemäß diesem Artikel.

(4) Übermittlungen gemäß Absatz 1 werden dokumentiert.

Artikel 40

Internationale Zusammenarbeit zum Schutz personenbezogener Daten

In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Mitgliedstaaten 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 Austausches und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten einschließlich Zuständigkeitskonflikten mit Drittländern.

KAPITEL VI

Unabhänge Aufsichtsbehörden

Abschnitt 1

Unabhängigkeit

Artikel 41

Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Richtlinie 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 Richtlinie in der gesamten Union. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII.

(3) Die Mitgliedstaaten können vorsehen, dass die gemäß der Verordnung (EU) 2016/679 in den Mitgliedstaaten errichtete Aufsichtsbehörde die in dieser Richtlinie genannte Aufsichtsbehörde ist und die Verantwortung für die Aufgaben der nach Absatz 1 zu errichtenden Aufsichtsbehörde übernimmt.

(4) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im in Artikel 51 genannten Ausschuss zu vertreten hat.

Artikel 42

Unabhängigkeit

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Richtlinie völlig unabhängig handelt.

(2) Die Mitgliedstaaten sehen vor, dass das Mitglied oder die Mitglieder ihrer Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Richtlinie weder direkter noch indirekter Beeinflussung von außen unterliegen und dass sie weder um Weisung ersuchen noch Weisungen entgegennehmen.

(3) Die Mitglieder der Aufsichtsbehörden der Mitgliedstaaten sehen von allen mit den Aufgaben ihres Amts 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 ihre eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaaten 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 43

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 Erfüllung seiner Aufgaben nicht mehr erfüllt.

Artikel 44

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, außer für die erste Amtszeit nach dem 6. 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 ihrer Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstöße gegen diese Richtlinie.

Abschnitt 2

Zuständigkeit, Aufgaben und Befugnisse

Artikel 45

Zuständigkeit

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde dafür zuständig ist, im Hoheitsgebiet ihres eigenen Mitgliedstaats die ihr gemäß dieser Richtlinie zugewiesenen Aufgaben und übertragenen Befugnisse zu erfüllen bzw. auszuüben.

(2) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. Die Mitgliedstaaten können vorsehen, dass ihre Aufsichtsbehörde nicht für die Überwachung der von anderen unabhängigen Justizbehörden im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist.

Artikel 46

Aufgaben

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde in seinem Hoheitsgebiet

a) die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisiert und sie darüber aufklärt;

c) im Einklang mit dem Recht der Mitgliedstaaten 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 berät;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Richtlinie entstehenden Pflichten sensibilisiert;

e) auf Antrag jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Richtlinie zur Verfügung stellt und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeitet;

f) sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 55 befasst, den Gegenstand der Beschwerde in angemessenem Umfang untersucht und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichtet, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) die Rechtmäßigkeit der Verarbeitung gemäß Artikel 17 überprüft und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß Absatz 3 des genannten Artikels unterrichtet oder ihr die Gründe mitteilt, aus denen die Überprüfung nicht vorgenommen wurde;

h) mit anderen Aufsichtsbehörden zusammenarbeitet, auch durch Informationsaustausch, und ihnen Amtshilfe leistet, um die einheitliche Anwendung und Durchsetzung dieser Richtlinie zu gewährleisten;

i) Untersuchungen über die Anwendung dieser Richtlinie durchführt, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

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

k) Beratung in Bezug auf die in Artikel 28 genannten Verarbeitungsvorgänge leistet; und

l) Beiträge zur Tätigkeit des Ausschusses leistet.

(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 für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — besonders wegen häufiger Wiederholung — exzessiven Anträgen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage ihrer Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast dafür, dass der Antrag offensichtlich unbegründet oder exzessiv ist.

Artikel 47

Befugnisse

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt. Diese Befugnisse umfassen zumindest die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten.

(2) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten folgenden verfügt, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die nach dieser Richtlinie erlassenen Vorschriften verstoßen;

b) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß Artikel 16;

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

(3) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Beratungsbefugnisse verfügt, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach Artikel 28 den Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an ihr nationales Parlament, ihre Regierung oder im Einklang mit seinem nationalen Recht an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

(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 jede Aufsichtsbehörde befugt ist, Verstöße gegen nach dieser Richtlinie erlassene Vorschriften den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die nach dieser Richtlinie erlassenen Vorschriften durchzusetzen.

Artikel 48

Meldung von Verstößen

Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden wirksame Vorkehrungen treffen, um vertrauliche Meldungen über Verstöße gegen diese Richtlinie zu fördern.

Artikel 49

Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der verhängten Sanktionen enthalten kann. Die 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

Artikel 50

Gegenseitige Amtshilfe

(1) Jeder Mitgliedstaat sieht vor, dass seine Aufsichtsbehörden einander maßgebliche Informationen übermitteln und Amtshilfe gewähren, um diese Richtlinie einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Jeder Mitgliedstaaten sieht vor, dass jede Aufsichtsbehörde alle geeigneten Maßnahmen ergreift, um dem 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 Richtlinie oder gegen das Unionsrecht verstoßen würde oder gegen das Recht des Mitgliedstaats, 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) 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 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 51

Aufgaben des Ausschusses

(1) Der mit der Verordnung (EU) 2016/679 eingesetzte Europäische Ausschuss nimmt in Bezug auf Verarbeitungsvorgänge im Anwendungsbereich dieser Richtlinie folgende Aufgaben wahr:

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

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

c) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 47 Absätze 1 und 3;

d) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b dieses Unterabsatzes für die Feststellung von Verletzungen des Schutzes personenbezogener Daten und die Festlegung der Unverzüglichkeit im Sinne des Artikels 30 Absätze 1 und 2 und für die konkreten Umstände, unter denen der Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben;

e) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b dieses Absatzes in Bezug auf die Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen im Sinne des Artikels 31 Absatz 1 zur Folge hat;

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

g) Abgabe einer Stellungnahme gegenüber der Kommission zur Beurteilung der Angemessenheit des in einem Drittland, einem Gebiet oder einem oder mehrere spezifischen Sektoren in einem Drittland oder einer internationalen Organisation gebotenen Schutzniveaus sowie zur Beurteilung der Frage, ob ein solches Drittland, das Gebiet, der spezifische Sektor oder die internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet.

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

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

j) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzrecht und -praxis mit Datenschutzaufsichtsbehörden in aller Welt.

In Bezug auf Unterabsatz 1 Buchstabe g stellt die Kommission dem Ausschuss alle erforderlichen Unterlagen zur Verfügung, darunter den Schriftwechsel mit der Regierung des Drittlandes, mit dem Gebiet oder spezifischen Sektor in diesem Drittland oder mit der internationalen Organisation.

(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 58 Absatz 1 genannten Ausschuss weiter und veröffentlicht sie.

(4) Die Kommission setzt den Ausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die von ihm herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren ergriffen hat.

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Artikel 52

Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde hat, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die nach dieser Richtlinie erlassenen Vorschriften verstößt.

(2) Die Mitgliedstaaten sehen vor, dass eine Beschwerde, die nicht bei der gemäß Artikel 45 Absatz 1 zuständigen Aufsichtsbehörde eingereicht wird, von der Aufsichtsbehörde, bei der die Beschwerde eingelegt wird, ohne unverzüglich an die zuständige Aufsichtsbehörde übermittelt wird. Die betroffene Person wird über die Übermittlung unterrichtet.

(3) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, auf Ersuchen der betroffenen Person weitere Unterstützung leistet.

(4) Die betroffene Person wird von der zuständigen Aufsichtsbehörde über den Stand und das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 53 unterrichtet.

Artikel 53

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jede natürliche oder juristische Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde hat.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die gemäß Artikel 45 Absatz 1 zuständige Aufsichtsbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 52 erhobenen Beschwerde in Kenntnis gesetzt hat.

(3) Die Mitgliedstaaten sehen vor, dass für Verfahren gegen eine Aufsichtsbehörde die Gerichte des Mitgliedstaats zuständig sind, in dem die Aufsichtsbehörde ihren Sitz hat.

Artikel 54

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 52 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn sie der Ansicht ist, dass die Rechte, die ihr aufgrund von nach dieser Richtlinie erlassenen Vorschriften zustehen, infolge einer nicht mit diesen Vorschriften im Einklang stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Artikel 55

Vertretung von betroffenen Personen

Die Mitgliedstaaten sehen im Einklang mit dem Verfahrensrecht der Mitgliedstaaten vor, dass die betroffene Person das Recht hat, nach dem Recht eines Mitgliedstaats ordnungsgemäß gegründete Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und in ihrem Namen die in den Artikeln 52, 53 und 54 genannten Rechte wahrzunehmen.

Artikel 56

Recht auf Schadenersatz

Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen Handlung, die gegen nach Maßgabe dieser Richtlinie erlassenen nationalen Vorschriften verstößt, ein materieller oder immaterieller Schaden entstanden ist, Recht auf Schadenersatz seitens des Verantwortlichen oder jeder sonst nach dem Recht der Mitgliedstaaten zuständigen Stelle hat.

Artikel 57

Sanktionen

Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen die nach dieser Richtlinie erlassenen Vorschriften zu verhängen sind, und treffen die zu deren Anwendung erforderlichen Maßnahmen. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

KAPITEL IX

Durchführungsrechtsakte

Artikel 58

Ausschussverfahren

(1) Die Kommission wird von dem mit Artikel 93 der Verordnung (EU) 2016/679 eingesetzten 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 X

Schlussbestimmungen

Artikel 59

Aufhebung des Rahmenbeschlusses 2008/977/JI

(1) Der Rahmenbeschluss 2008/977/JI wird mit Wirkung vom 6. Mai 2018 aufgehoben.

(2) Verweise auf den in Absatz 1 genannten aufgehobenen Beschluss gelten als Verweise auf diese Richtlinie.

Artikel 60

Bestehende Unionsrechtsakte

Die besonderen Bestimmungen zum Schutz personenbezogener Daten in Unionsrechtsakten, die am oder vor dem 6. Mai 2016 im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, die die Verarbeitung im Verkehr der Mitgliedstaaten untereinander sowie den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen im Anwendungsbereich dieser Richtlinie regeln, bleiben unberührt.

Artikel 61

Verhältnis zu bereits geschlossenen internationalen Übereinkünften im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 6. Mai 2016 geschlossen wurden und die mit dem vor dem genannten Datum geltenden Unionsrecht vereinbar sind, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

Artikel 62

Berichte der Kommission

(1) Bis zum 6. Mai 2022 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Richtlinie vor. Die Berichte werden öffentlich gemacht.

(2) Im Rahmen der Bewertungen und Überprüfungen gemäß Absatz 1prüft die Kommission insbesondere die Anwendung und Wirkungsweise des Kapitels V über die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen und vor allem die Beschlüsse nach Artikel 36 Absatz 3 und Artikel 39.

(3) Für die in den Absätzen 1 und 2 genannten Zwecke 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 sowie der anderen einschlägigen Stellen und Quellen.

(5) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Richtlinie vor und berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

(6) Bis zum 6. Mai 2019 überprüft die Kommission andere Rechtsakte der Union über die Verarbeitung durch die zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke, einschließlich der auf der Grundlage von Artikel 60 erlassenen Rechtsakte, um festzustellen, inwieweit eine Anpassung an diese Richtlinie notwendig ist, und um gegebenenfalls die erforderlichen Vorschläge zur Änderung dieser Rechtsakte zu unterbreiten, damit ein einheitliches Vorgehen beim Schutz personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie gewährleistet ist.

Artikel 63

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit. Sie wenden diese Vorschriften ab dem 6. Mai 2018 an.

Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Abweichend von Absatz 1 können die Mitgliedstaaten vorsehen, dass in Ausnahmefällen, in denen dies für die vor dem 6. Mai 2016 eingerichteten automatisierten Verarbeitungssysteme mit einem unverhältnismäßigen Aufwand verbunden ist, diese bis zum 6. Mai 2023 mit Artikel 25 Absatz 1 in Einklang gebracht werden müssen.

(3) Abweichend von Absätzen 1 und 2 dieses Artikels kann ein Mitgliedstaat in außergewöhnlichen Umständen ein automatisiertes Verarbeitungssystem im Sinne des Absatzes 2 dieses Artikels innerhalb einer bestimmten Frist nach Ablauf der in Absatz 2 dieses Artikels genannten Frist mit Artikel 25 Absatz 1 in Einklang bringen, wenn hierdurch sonst schwerwiegende Schwierigkeiten für den Betrieb dieses automatisierten Verarbeitungssystems entstehen würden. Der betreffende Mitgliedstaat begründet gegenüber der Kommission, weshalb diese schwerwiegenden Schwierigkeiten entstehen würden und die Gründe für die bestimmte Frist, innerhalb derer er das automatisierte Verarbeitungssystem mit Artikel 25 Absatz 1 in Einklang bringen wird. Diese Frist muss vor dem 6. Mai 2026 enden.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 64

Inkrafttreten

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 65

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 27. April 2016.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1 Buchstabe d und Artikel 87 Absatz 2 Buchstabe a,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Kommission hat am 6. November 2007 einen Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (im Folgenden „PNR-Daten“) zu Zwecken der Verhütung, Aufdeckung und Ermittlung angenommen. Mit dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 wurde der Kommissionsvorschlag, dessen Annahme durch den Rat zu diesem Zeitpunkt noch ausstand, jedoch hinfällig.

(2) Im „Stockholmer Programm — Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger“ ([3]) wird die Kommission aufgefordert, einen Vorschlag über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität vorzulegen.

(3) Die Kommission hat in ihrer Mitteilung vom 21. September 2010 über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer eine Anzahl an Kernelementen erläutert, die eine Politik der Union in diesem Bereich beinhalten muss.

(4) Die Richtlinie 2004/82/EG des Rates ([4]), regelt die Vorabübermittlung von Angaben über die beförderten Personen (im Folgenden „API-Daten“) durch die Fluggesellschaften an die zuständigen nationalen Behörden als Mittel zur Verbesserung der Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung.

(5) Die Ziele dieser Richtlinie bestehen unter anderem darin, für Sicherheit zu sorgen, das Leben und die Sicherheit von Personen zu schützen und einen Rechtsrahmen für den Schutz von PNR-Daten in Bezug auf deren Verarbeitung durch die zuständigen Behörden zu schaffen.

(6) Die effektive Verwendung von PNR-Daten, indem z. B. PNR-Daten mit verschiedenen Datenbanken betreffend Personen und Gegenstände abgeglichen werden, ist notwendig, um terroristische Straftaten und schwere Kriminalität zu verhüten, aufzudecken, zu ermitteln und zu verfolgen und damit einen Beitrag zur inneren Sicherheit zu leisten, um Beweismaterial zusammenzutragen und gegebenenfalls Komplizen von Straftätern aufzuspüren und kriminelle Netze auszuheben.

(7) Anhand einer Überprüfung von PNR-Daten können Personen ermittelt werden, die vor einer solchen Überprüfung nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollten. Durch die Verwendung von PNR-Daten ist es möglich, die Bedrohung durch terroristische Straftaten und schwere Kriminalität anders anzugehen, als dies durch Verarbeitung anderer Kategorien personenbezogener Daten möglich wäre. Damit die Verarbeitung von PNR-Daten jedoch auf das Erforderliche beschränkt bleibt, sollten die Aufstellung und Anwendung von

([1]) ABl. C 218 vom 23.7.2011, S. 107.
([2]) Standpunkt des Europäischen Parlaments vom 14. April 2016 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 21. April 2016.
([3]) ABl. C 115 vom 4.5.2010, S. 1.
([4]) Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (ABl. L 261 vom 6.8.2004, S. 24).

Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, beschränkt werden. Darüber hinaus sollten die Prüfkriterien so festgelegt werden, dass die Zahl unschuldiger Personen, die fälschlicherweise vom System identifiziert werden, auf ein Minimum beschränkt wird.

(8) Die Fluggesellschaften erheben und verarbeiten bereits PNR-Daten ihrer Fluggäste für ihre eigenen geschäftlichen Zwecke. Durch diese Richtlinie sollten weder Fluggesellschaften dazu verpflichtet werden, weitere Fluggastdaten zu erheben oder vorzuhalten, noch sollte von den Fluggästen verlangt werden, dass sie neben den Daten, die die Fluggesellschaften bereits von ihnen erhalten, noch zusätzliche Daten bereitstellen.

(9) Einige Fluggesellschaften halten API-Daten, die sie erheben, als Teil der PNR-Daten vor, während andere dies nicht tun. Die Verwendung von PNR-Daten zusammen mit API-Daten bietet einen Mehrwert, indem sie den Mitgliedstaaten die Feststellung der Identität einer Person erleichtert, mithin den Nutzen dieses Ergebnisses für die Verhütung, Aufdeckung und Ermittlung von Straftaten erhöht und die Gefahr minimiert, dass Überprüfungen und Ermittlungen zu unschuldigen Personen durchgeführt werden. Es muss daher sichergestellt werden, dass Fluggesellschaften, die API-Daten erheben, diese übermitteln, unabhängig davon, ob sie API-Daten auf andere technische Weise als PNR-Daten vorhalten.

(10) Für die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Terrorismus und schwerer Kriminalität ist es außerordentlich wichtig, dass alle Mitgliedstaaten Vorschriften erlassen, mit denen Fluggesellschaften, die Drittstaatsflüge durchführen, dazu verpflichtet werden, von ihnen erhobene PNR-Daten, einschließlich API-Daten, zu übermitteln. Die Mitgliedstaaten sollten auch die Möglichkeit haben, diese Verpflichtung auf Fluggesellschaften auszudehnen, die EU-Flüge durchführen. Diese Bestimmungen sollten die Richtlinie 2004/82/EG des Rates unberührt lassen.

(11) Die Verarbeitung von personenbezogenen Daten sollte in einem angemessenen Verhältnis zu den mit dieser Richtlinie verfolgten bestimmten Sicherheitsinteressen stehen.

(12) Die in dieser Richtlinie zugrunde gelegte Definition für „terroristische Straftaten" sollte mit der Definition im Rahmenbeschluss 2002/475/JI des Rates ([1]) identisch sein. Die Definition der schweren Kriminalität sollte die in Anhang II dieser Richtlinie genannten Kategorien von Straftaten umfassen.

(13) Um Klarheit zu gewährleisten und die Kosten für die Fluggesellschaften gering zu halten, sollten die PNR-Daten an eine einzige, genau bezeichnete Stelle (im Folgenden „PNR-Zentralstelle") des jeweiligen Mitgliedstaats übermittelt werden. Die PNR-Zentralstelle kann über verschiedene Zweigstellen in einem Mitgliedstaat verfügen, und Mitgliedstaaten können auch eine PNR-Zentralstelle gemeinsam einrichten. Die Mitgliedstaaten sollten die Informationen untereinander über maßgebliche Informationsaustauschnetze austauschen, um die Informationsweitergabe zu erleichtern und Interoperabilität zu gewährleisten.

(14) Die Kosten für die Nutzung, die Speicherung und den Austausch der PNR-Daten sollten von den Mitgliedstaaten getragen werden.

(15) Eine Liste mit den PNR-Daten, die für eine PNR-Zentralstelle bestimmt sind, sollte erstellt und inhaltlich so zusammengesetzt sein, dass sie sowohl den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gerecht werden und damit einen Beitrag zur inneren Sicherheit in der Union leisten als auch dem Grundrechtsschutz und insbesondere dem Schutz der Privatsphäre des Einzelnen und seiner personenbezogenen Daten Genüge tun. Zu diesem Zweck sollten hohe Standards zur Anwendung kommen, die mit der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta"), dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) im Einklang stehen. Eine solche Liste sollte nicht auf der Rasse oder ethnischen Herkunft, der Religion oder der Weltanschauung, der politischen oder sonstigen Meinungen, der Mitgliedschaft in einer Gewerkschaft, dem Gesundheitszustand, dem Sexualleben oder der sexuellen Orientierung einer Person beruhen. Die PNR-Daten sollten nur jene Details über den Buchungsvorgang und die Reiseroute von Fluggästen beinhalten, mit deren Hilfe die zuständigen Stellen diejenigen Fluggäste ermitteln können, die eine Bedrohung für die innere Sicherheit darstellen.

(16) Es gibt es zwei Methoden der Datenübermittlung: die „Pull-Methode", bei der die zuständigen Behörden des Mitgliedstaats, der die PNR-Daten benötigt, direkt auf das Buchungssystem der Fluggesellschaft zugreifen und eine Kopie der verlangten PNR-Daten extrahieren können, und die „Push-Methode", bei der die Fluggesellschaften die verlangten PNR-Daten an die anfragende Behörde übermitteln und somit die Kontrolle über die Art der übermittelten Daten behalten. Die „Push-Methode" gilt als die Methode, die ein höheres Datenschutzniveau bietet, und sollte daher für alle Fluggesellschaften verbindlich sein.

([1]) Rahmenbeschluss des Rates 2002/475/JI vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164 vom 22.6.2002, S. 3).

(17) Die Kommission unterstützt die Richtlinien der Internationalen Zivilluftfahrt-Organisation (ICAO) für die Übermittlung von PNR-Daten. Diese Richtlinien sollten daher die Grundlage für die Annahme der unterstützten Datenformate für die Übermittlung von PNR-Daten durch die Fluggesellschaften an die Mitgliedstaaten sein. Zur Gewährleistung einheitlicher Bedingungen für die Anwendung der unterstützten Datenformate und die für die Datenübermittlung durch die Fluggesellschaften zu verwendenden maßgeblichen Protokolle sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([1]) ausgeübt werden.

(18) Die Mitgliedstaaten sollten die nötigen Vorkehrungen treffen, damit die Fluggesellschaften ihren Verpflichtungen gemäß dieser Richtlinie nachkommen können. Für den Fall, dass Fluggesellschaften ihren Verpflichtungen im Zusammenhang mit der Übermittlung von PNR-Daten nicht nachkommen, sollten die Mitgliedstaaten wirksame, verhältnismäßige und abschreckende Sanktionen einschließlich Geldbußen vorsehen.

(19) Jeder Mitgliedstaat sollte eine Einschätzung der potenziellen Bedrohung durch terroristische Straftaten und schwere Kriminalität vornehmen.

(20) Um das Recht auf Schutz der personenbezogenen Daten und auf Nichtdiskriminierung umfassend zu wahren, sollten Entscheidungen, aus denen sich für die betreffende Person eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil ergeben könnten, nicht allein aufgrund der automatisierten Verarbeitung von PNR-Daten getroffen werden dürfen. Ebenso wenig sollten solche Entscheidungen — in Anbetracht der Artikel 8 und 21 der Charta — eine Diskriminierung aus Gründen wie dem Geschlecht, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, den genetischen Merkmalen, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, dem Vermögen, der Geburt, einer Behinderung, dem Alter oder der sexuellen Orientierung einer Person darstellen. Wenn die Kommission die Anwendung dieser Richtlinie überprüft, sollte sie auch diese Grundsätze berücksichtigen.

(21) Das Ergebnis der Verarbeitung von PNR-Daten sollte unter keinen Umständen von den Mitgliedstaaten als Mittel zur Umgehung ihrer internationalen Verpflichtungen aus dem Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge in der Fassung des Protokolls vom 31. Januar 1967 benutzt werden, noch sollte es zur Verweigerung sicherer und effektiver rechtmäßiger Wege in das Gebiet der Union gegenüber Asylsuchenden benutzt werden, damit diese dort von ihrem Recht auf internationalen Schutz Gebrauch machen können.

(22) Unter uneingeschränkter Berücksichtigung der in der jüngeren maßgeblichen Rechtsprechung des Gerichtshofs der Europäischen Union dargelegten Grundsätze sollte bei der Anwendung dieser Richtlinie sichergestellt werden, dass die Grundrechte, das Recht auf Privatsphäre und der Grundsatz der Verhältnismäßigkeit in vollem Umfang geachtet werden. Sie sollte auch wirklich den Zielen dessen, was erforderlich und verhältnismäßig ist, um die von der Union anerkannten allgemeinen Interessen zu wahren, und der Notwendigkeit entsprechen, die Rechte und Freiheiten anderer bei der Bekämpfung von terroristischen Straftaten und schwerer Kriminalität zu schützen. Die Anwendung dieser Richtlinie sollte ordnungsgemäß gerechtfertigt und die notwendigen Sicherheitsvorkehrungen getroffen werden, um die Rechtmäßigkeit einer etwaigen Speicherung, Auswertung, Übermittlung oder Verwendung von PNR-Daten sicherzustellen.

(23) Die Mitgliedstaaten sollten die erhaltenen PNR-Daten untereinander und mit Europol austauschen, wenn dies zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität für erforderlich erachtet wird. Die PNR-Zentralstellen sollten gegebenenfalls das Ergebnis der Verarbeitung der PNR-Daten umgehend an die PNR-Zentralstellen anderer Mitgliedstaaten zur weiteren Untersuchung übermitteln. Die Bestimmungen dieser Richtlinie sollten andere Rechtsakte der Union über den Austausch von Informationen zwischen Polizei und anderen Strafverfolgungsbehörden und Justizbehörden, einschließlich des Beschlusses 2009/371/JI des Rates ([2]) und des Rahmenbeschlusses 2006/960/JI des Rates ([3]), unberührt lassen. Der Austausch von PNR-Daten sollte nach den Vorschriften über die polizeiliche und justizielle Zusammenarbeit erfolgen und das von der Charta, dem Übereinkommen Nr. 108 und der EMRK geforderte hohe Niveau beim Schutz der Privatsphäre und personenbezogener Daten nicht beeinträchtigen.

(24) Ein sicherer Informationsaustausch hinsichtlich PNR-Daten zwischen den Mitgliedstaaten sollte über die bestehenden Kanäle für die Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten sowie insbesondere mit Europol durch Europols Netzanwendung für sicheren Datenaustausch (SIENA) sichergestellt werden.

([1]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

([2]) Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (ABl. L 121 vom 15.5.2009, S. 37).

([3]) Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89).

(25) Der Zeitraum, für den die PNR-Daten vorgehalten werden sollen, sollte so lang sein, wie dies für den mit ihnen verfolgten Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten sowie schwerer Kriminalität erforderlich ist und in einem angemessenen Verhältnis dazu stehen. Das Wesen der PNR-Daten und ihr Verwendungszweck bringen es mit sich, dass diese so lange gespeichert werden müssen wie nötig, um sie auswerten und für Ermittlungen nutzen zu können. Um einen unverhältnismäßigen Rückgriff auf die Daten auszuschließen, sollten die PNR-Daten nach der anfänglichen Speicherfrist durch Unkenntlichmachung von Datenelementen depersonalisiert werden. Um das höchste Datenschutzniveau zu gewährleisten, sollte Zugriff auf die vollständigen PNR-Daten, die die unmittelbare Identifizierung der betroffenen Person ermöglichen, nach dieser anfänglichen Frist nur unter eingeschränkten, sehr strengen Bedingungen gewährt werden.

(26) Wurden bestimmte PNR-Daten zur Verwendung für konkrete Ermittlungs- und Strafverfolgungszwecke an eine zuständige Behörde übermittelt, so sollte sich die Frist für die Speicherung der Daten durch diese Behörde ungeachtet der in dieser Richtlinie genannten Speicherfristen für Daten nach nationalem Recht richten.

(27) Für die Verarbeitung der PNR-Daten durch die PNR-Zentralstelle und die zuständigen Behörden der einzelnen Mitgliedstaaten sollte nationales Recht ein Datenschutzniveau im Einklang mit dem Rahmenbeschluss 2008/977/JI des Rates [1] und den in dieser Richtlinie festgelegten bestimmten Anforderungen an den Datenschutz vorsehen. Bezugnahmen auf den Rahmenbeschluss 2008/977/JI sollten als Bezugnahmen auf derzeit geltende Rechtsvorschriften sowie auf Rechtsvorschriften, die an ihre Stelle treten werden, verstanden werden.

(28) Unter Berücksichtigung des Anspruchs auf Schutz der personenbezogenen Daten müssen die Rechte der betroffenen Personen in Bezug auf die Verarbeitung ihrer PNR-Daten, insbesondere das Recht auf Zugang, Berichtigung, Löschung oder Einschränkung der Verarbeitung und das Recht auf Schadenersatz und Rechtsbehelfe, mit dem Rahmenbeschluss 2008/977/JI und mit dem hohen Schutzniveau, das durch die Charta und die EMRK vorgesehen ist, im Einklang stehen.

(29) Soweit es um das Recht von Fluggästen auf Information über die Verarbeitung ihrer personenbezogenen Daten geht, sollten die Mitgliedstaaten sicherstellen, dass Fluggäste über die Erhebung der PNR-Daten, deren Übermittlung an die PNR-Zentralstelle und über ihre Rechte als betroffene Personen korrekt und auf leicht zugängliche und verständliche Weise informiert werden.

(30) Diese Richtlinie berührt nicht das Unions- und nationale Recht zum Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten.

(31) Die Übermittlung von PNR-Daten durch die Mitgliedstaaten an Drittstaaten sollte nur im Einzelfall und unter voller Einhaltung der von den Mitgliedstaaten in Anwendung des Rahmenbeschlusses 2008/977/JI festgelegten Bestimmungen gestattet sein. Im Interesse des Datenschutzes sollten bei solchen Übermittlungen an Drittstaaten weitere Anforderungen an den Zweck der Übermittlung gestellt werden. Für diese Übermittlungen sollten auch die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit sowie das hohe Schutzniveau, das durch die Charta und die EMRK vorgesehen sind, gelten.

(32) Die im Zuge der Umsetzung des Rahmenbeschlusses 2008/977/JI eingerichtete nationale Kontrollstelle sollte auch in Bezug auf die Anwendung der von den Mitgliedstaaten aufgrund dieser Richtlinie erlassenen Bestimmungen eine Beratungs- und Kontrollfunktion ausüben.

(33) Die vorliegende Richtlinie hindert die Mitgliedstaaten nicht daran, nach ihrem jeweiligen nationalen Recht eine Regelung zur Erhebung und Verarbeitung von PNR-Daten durch Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen — einschließlich Flugbuchungen — erbringen, für die sie PNR-Daten erheben und verarbeiten, oder durch andere als in dieser Richtlinie angegebene Beförderungsunternehmen vorzusehen, sofern dieses nationale Recht mit dem Unionsrecht in Einklang steht.

(34) Diese Richtlinie lässt gegenwärtige Regelungen der Union hinsichtlich der Durchführung von Grenzkontrollen und Regelungen der Union hinsichtlich der Einreise in das Gebiet der Union und der Ausreise aus dem Gebiet der Union unberührt.

(35) Aufgrund der sowohl in rechtlicher als auch in technischer Hinsicht unterschiedlichen nationalen Bestimmungen zur geregelten Verarbeitung von personenbezogenen Daten, und damit auch von PNR-Daten, sind die Fluggesellschaften jetzt und auch künftig mit unterschiedlichen Vorschriften in Bezug auf die Art der zu übermittelnden Informationen und in Bezug auf die Voraussetzungen für die Übermittlung dieser Informationen an die zuständigen einzelstaatlichen Behörden konfrontiert. Diese Unterschiede können einer wirksamen

[1] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

Zusammenarbeit zwischen den zuständigen nationalen Behörden zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität abträglich sein. Daher ist es notwendig, auf Unionsebene einen gemeinsamen Rechtsrahmen für die Übermittlung und Verarbeitung von PNR-Daten zu schaffen.

(36) Die vorliegende Richtlinie wahrt die Grundrechte und Grundsätze der Charta, insbesondere das in den Artikeln 8, 7 und 21 verankerte Recht auf Schutz der personenbezogenen Daten, das Recht auf Achtung der Privatsphäre und das Recht auf Nichtdiskriminierung; sie ist deshalb entsprechend umzusetzen. Diese Richtlinie ist mit den Datenschutzgrundsätzen vereinbar, und ihre Bestimmungen stehen im Einklang mit dem Rahmenbeschluss 2008/977/JI. Um dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen, sieht diese Richtlinie zudem in Bezug auf bestimmte Aspekte Datenschutzbestimmungen vor, die strenger sind als die des Rahmenbeschlusses 2008/977/JI.

(37) Der Anwendungsbereich der Richtlinie wurde möglichst eng gefasst, denn: Sie beschränkt die Speicherfrist für die PNR-Daten bei den PNR-Zentralstellen auf maximal fünf Jahre, nach deren Ablauf die Daten gelöscht werden sollten; sie sieht vor, dass die Daten nach einer ersten Frist von sechs Monaten durch Unkenntlichmachung von Datenelementen depersonalisiert werden, und sie untersagt die Erhebung und Verwendung von sensiblen Daten. Um einen wirksamen und weitreichenden Datenschutz zu gewährleisten, haben die Mitgliedstaaten dafür zu sorgen, dass eine unabhängige nationale Kontrollstelle und insbesondere ein Datenschutzbeauftragter eine Beratungs- und Kontrollfunktion in Bezug auf die Art und Weise der Verarbeitung der PNR-Daten ausübt. Jede Verarbeitung von PNR-Daten sollte zum Zwecke der Überprüfung ihrer Rechtmäßigkeit, zur Selbstkontrolle sowie zur Gewährleistung der Unversehrtheit der Daten und der Sicherheit der Datenverarbeitung protokolliert oder dokumentiert werden. Des Weiteren sollten die Mitgliedstaaten dafür sorgen, dass die Fluggäste klar und präzise über die Erhebung von PNR-Daten und ihre Rechte informiert werden.

(38) Da die Ziele dieser Richtlinie — nämlich die Übermittlung von PNR-Daten durch Fluggesellschaften und deren Verarbeitung zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität — von den Mitgliedstaaten nicht ausreichend verwirklicht werden können sondern vielmehr auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(39) Nach Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts haben diese Mitgliedstaaten mitgeteilt, dass sie sich an der Annahme und Anwendung dieser Richtlinie beteiligen möchten.

(40) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Richtlinie und ist weder durch diese Richtlinie gebunden noch zu ihrer Anwendung verpflichtet

(41) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [1] angehört und hat am 25. März 2011 eine Stellungnahme abgegeben —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Anwendungsbereich

(1) Diese Richtlinie regelt

a) die Übermittlung von Fluggastdatensätzen (PNR-Daten) zu Fluggästen von Drittstaatsflügen durch Fluggesellschaften;

b) die Verarbeitung von Daten gemäß Buchstabe a, unter anderem ihre Erhebung, Verwendung und Speicherung durch Mitgliedstaaten sowie den Austausch dieser Daten zwischen Mitgliedstaaten.

[1] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

(2) Die nach Maßgabe dieser Richtlinie erhobenen PNR-Daten dürfen ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß Artikel 6 Absatz 2 Buchstaben a, b und c verarbeitet werden.

Artikel 2

Anwendung dieser Richtlinie auf EU-Flüge

(1) Ein Mitgliedstaat, der entscheidet, diese Richtlinie auf Flüge innerhalb der Europäischen Union (EU-Flüge) anzuwenden, teilt dies der Kommission schriftlich mit. Ein Mitgliedstaat kann eine solche Mitteilung jederzeit machen oder widerrufen. Die Kommission veröffentlicht diese Mitteilung und eventuelle Widerrufe derselben im *Amtsblatt der Europäischen Union*.

(2) Im Falle einer Mitteilung gemäß Absatz 1 gelten alle Bestimmungen dieser Richtlinie für EU-Flüge so, als handele es sich um Drittstaatsflüge, und für PNR-Daten zu EU-Flügen so, als handele es sich um PNR-Daten zu Drittstaatsflügen.

(3) Ein Mitgliedstaat kann beschließen, diese Richtlinie nur auf ausgewählte EU-Flüge anzuwenden. Der Mitgliedstaat wählt dabei diejenigen Flüge aus, die er für die Verfolgung der Ziele dieser Richtlinie für erforderlich hält. Der Mitgliedstaat kann jederzeit eine Änderung der von ihm ausgewählten EU-Flüge beschließen.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. „Fluggesellschaft“ ein Luftfahrtunternehmen mit einer gültigen Betriebsgenehmigung oder einer gleichwertigen Genehmigung, die es ihm gestattet, Fluggäste auf dem Luftweg zu befördern;

2. „Drittstaatsflug“ jeden Linien- oder Gelegenheitsflug einer Fluggesellschaft, der von einem Drittstaat aus startet und das Hoheitsgebiet eines Mitgliedstaats zum Ziel hat, oder der vom Hoheitsgebiet eines Mitgliedstaats aus startet und einen Drittstaat zum Ziel hat, wobei in beiden Fällen Flüge mit Zwischenlandungen im Hoheitsgebiet von Mitgliedstaaten oder Drittstaaten eingeschlossen sind;

3. „EU-Flug“ jeden Linien- oder Gelegenheitsflug einer Fluggesellschaft, der vom Hoheitsgebiet eines Mitgliedstaats aus startet und das Hoheitsgebiet eines oder mehrerer anderer Mitgliedstaaten zum Ziel hat, ohne Zwischenlandungen im Hoheitsgebiet eines Drittstaats;

4. „Fluggast“ jede Person, einschließlich Transfer- oder Transitfluggästen, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung der Fluggesellschaft in einem Luftfahrzeug befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung der Person in die Fluggastliste belegt wird;

5. „Fluggastdatensatz“ oder „PNR-Daten“ einen Datensatz mit den für die Reise notwendigen Angaben zu jedem einzelnen Fluggast, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Fluggesellschaften ermöglichen, unabhängig davon, ob er in Buchungssystemen, Abfertigungssystemen (Departure Control Systems) zum Einchecken von Passagieren auf Flüge, oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist;

6. „Buchungssysteme“ das interne System einer Fluggesellschaft, in dem die PNR-Daten für die Bearbeitung von Buchungen erhoben werden;

7. „Push-Methode“ das Verfahren, bei dem die Fluggesellschaft die in Anhang I aufgeführten PNR-Daten in die Datenbank der anfragenden Behörde übermittelt;

8. „terroristische Straftaten“ die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI;

9. „schwere Kriminalität“ die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind;

10. „Depersonalisierung durch Unkenntlichmachung von Datenelementen“ die Vorgehensweise, mit der diejenigen Datenelemente, mit denen die Identität des Fluggastes unmittelbar festgestellt werden könnte, für einen Nutzer unsichtbar gemacht werden.

KAPITEL II

Zuständigkeiten der Mitgliedstaaten

Artikel 4

PNR-Zentralstelle

(1) Jeder Mitgliedstaat errichtet oder benennt eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde, die als seine PNR-Zentralstelle handelt.

(2) Die PNR-Zentralstelle ist verantwortlich für

a) die Erhebung der PNR-Daten bei Fluggesellschaften, für die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung dieser Daten oder der Ergebnisse ihrer Verarbeitung an die zuständigen Behörden nach Artikel 7;

b) den Austausch sowohl von PNR-Daten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten und mit Europol gemäß den Artikeln 9 und 10.

(3) Das Personal der PNR-Zentralstelle kann aus Mitarbeitern zuständiger Behörden bestehen, die zu diesem Zweck abgeordnet wurden. Die Mitgliedstaaten stellen den PNR-Zentralstellen angemessene Ressourcen zur Verfügung, damit sie ihre Aufgaben erfüllen können.

(4) Zwei oder mehr Mitgliedstaaten (die beteiligten Mitgliedstaaten) können gemeinsam eine einzige Behörde errichten oder benennen, die als ihre PNR-Zentralstelle handelt. Diese PNR-Zentralstelle hat ihren Sitz in einem der beteiligten Mitgliedstaaten und gilt als nationale PNR-Zentralstelle aller beteiligten Mitgliedstaaten. Die beteiligten Mitgliedstaaten einigen sich gemeinsam unter Beachtung der Anforderungen dieser Richtlinie über die genauen Modalitäten, unter denen die PNR-Zentralstelle ihrer Tätigkeit nachgeht.

(5) Innerhalb eines Monats nach der Errichtung seiner PNR-Zentralstelle teilt jeder Mitgliedstaat dies der Kommission mit und kann seine Mitteilung jederzeit ändern. Die Kommission veröffentlicht die Mitteilung sowie alle nachfolgenden Änderungen im *Amtsblatt der Europäischen Union*.

Artikel 5

Datenschutzbeauftragter der PNR-Zentralstelle

(1) Die PNR-Zentralstelle ernennt einen Datenschutzbeauftragten, der für die Überwachung der Verarbeitung der PNR-Daten und die Umsetzung der maßgeblichen Sicherheitsvorkehrungen zuständig ist.

(2) Die Mitgliedstaaten stellen den Datenschutzbeauftragten die Mittel zur Verfügung, damit sie ihre Pflichten und Aufgaben gemäß diesem Artikel wirksam und unabhängig wahrnehmen können.

(3) Die Mitgliedstaaten sorgen dafür, dass eine betroffene Person das Recht hat, den Datenschutzbeauftragten als zentrale Kontaktstelle im Zusammenhang mit allen Fragen bezüglich der Verarbeitung der PNR-Daten der betroffenen Person zu kontaktieren.

Artikel 6

Verarbeitung der PNR-Daten

(1) Die von den Fluggesellschaften übermittelten PNR-Daten werden von der PNR-Zentralstelle des betreffenden Mitgliedstaats gemäß Artikel 8 erhoben. Wenn die von Fluggesellschaften übermittelten PNR-Daten andere als die in Anhang I genannten Daten beinhalten, werden diese Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht.

(2) Die PNR-Zentralstelle verarbeitet PNR-Daten ausschließlich zu folgenden Zwecken:

a) Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den zuständigen Behörden gemäß Artikel 7 und gegebenenfalls — im Einklang mit Artikel 10 — von Europol genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind;

b) im Einzelfall Beantwortung von auf einer hinreichenden Grundlage gebührend begründeten Anfragen zuständiger Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität, und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden oder gegebenenfalls an Europol, und

c) Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

(3) Bei der Durchführung der in Absatz 2 Buchstabe a genannten Überprüfungen darf die PNR-Zentralstelle

a) die PNR-Daten mit Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften abgleichen; oder

b) die PNR-Daten anhand im Voraus festgelegter Kriterien abgleichen.

(4) Die Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat anhand im Voraus festgelegter Kriterien gemäß Absatz 3 Buchstabe b erfolgt in nichtdiskriminierender Weise. Diese im Voraus festgelegten Kriterien müssen zielgerichtet, verhältnismäßig und bestimmt sein. Die Mitgliedstaaten stellen sicher, dass diese Kriterien von der PNR-Zentralstelle aufgestellt und von ihr in Zusammenarbeit mit den in Artikel 7 genannten zuständigen Behörden regelmäßig überprüft werden. Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen unter keinen Umständen als Grundlage für diese Kriterien dienen.

(5) Die Mitgliedstaaten stellen sicher, dass jeder einzelne Treffer bei der automatisierten Verarbeitung von PNR-Daten nach Maßgabe von Absatz 2 Buchstabe a auf andere, nicht-automatisierte Art individuell überprüft wird, um zu klären, ob die zuständige Behörde gemäß Artikel 7 Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss.

(6) Die PNR-Zentralstelle eines Mitgliedstaats übermittelt die PNR-Daten von nach Absatz 2 Buchstabe a ermittelten Personen oder die Ergebnisse der Verarbeitung dieser Daten zur weiteren Überprüfung an die zuständigen Behörden gemäß Artikel 7 desselben Mitgliedstaats. Derartige Übermittlungen dürfen nur im Einzelfall erfolgen und im Fall einer automatisierten Verarbeitung der PNR-Daten nur nach einer individuellen Überprüfung auf andere, nicht-automatisierte Art.

(7) Die Mitgliedstaaten stellen sicher, dass der Datenschutzbeauftragte Zugang zu sämtlichen von der PNR-Zentralstelle verarbeiteten Daten erhält. Wenn der Datenschutzbeauftragte der Auffassung ist, dass eine Verarbeitung von Daten nicht rechtmäßig war, kann er die Angelegenheit an die nationale Kontrollstelle verweisen.

(8) Die Speicherung, Verarbeitung und Auswertung von PNR-Daten durch die PNR-Zentralstelle erfolgt ausschließlich an einem gesicherten Ort bzw. gesicherten Orten im Hoheitsgebiet der Mitgliedstaaten.

(9) Das Recht zur Einreise von Personen, die im Hoheitsgebiet des betreffenden Mitgliedstaats gemäß der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates ([1]) das Unionsrecht auf freien Personenverkehr genießen, darf von den Auswirkungen der Überprüfungen von Fluggästen gemäß Absatz 2 Buchstabe a dieses Artikels nicht beeinträchtigt werden. Darüber hinaus müssen, wenn Überprüfungen in Bezug auf EU-Flüge zwischen Mitgliedstaaten vorgenommen werden, für die die Verordnung (EG) Nr. 562/2006 des Europäischen Parlaments und des Rates ([2]) gilt, die Auswirkungen solcher Überprüfungen mit der genannten Verordnung im Einklang stehen.

Artikel 7

Zuständige Behörden

(1) Jeder Mitgliedstaat erstellt eine Liste der zuständigen Behörden, die berechtigt sind, zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von den PNR-Zentralstellen anzufordern oder entgegenzunehmen, um sie einer weiteren Prüfung zu unterziehen oder um geeignete Maßnahmen zu veranlassen.

(2) Die in Absatz 1 genannten Behörden sind diejenigen Behörden, die für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständig sind.

(3) Für die Zwecke des Artikels 9 Absatz 3 übermittelt jeder Mitgliedstaat der Kommission bis zum 25. Mai 2017 die Liste seiner zuständigen Behörden und kann seine Mitteilung jederzeit ändern. Die Kommission veröffentlicht die Mitteilung und eventuelle Änderungen derselben im *Amtsblatt der Europäischen Union*.

(4) Die PNR-Daten und die Ergebnisse der Verarbeitung dieser Daten, die aus der PNR-Zentralstelle eingehen, dürfen von den zuständigen Behörden der Mitgliedstaaten ausschließlich zum bestimmten Zweck der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität weiterverarbeitet werden.

(5) Absatz 4 berührt nicht die Befugnisse der Strafverfolgungs- oder Justizbehörden der Mitgliedstaaten in Fällen, in denen im Verlauf von Strafverfolgungsmaßnahmen im Anschluss an eine derartige Verarbeitung andere Straftaten festgestellt werden oder sich Anhaltspunkte für solche Straftaten ergeben.

(6) Die zuständigen Behörden treffen Entscheidungen, aus denen sich eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil für die betroffene Person ergibt, unter keinen Umständen allein auf der Grundlage der automatisierten Verarbeitung der PNR-Daten. Ebenso wenig werden solche Entscheidungen aufgrund der rassischen oder ethnischen Herkunft, der politischen Meinungen, der religiösen oder weltanschaulichen Überzeugungen, der Mitgliedschaft in einer Gewerkschaft, des Gesundheitszustands, des Sexuallebens oder der sexuellen Orientierung einer Person getroffen.

Artikel 8

Datenübermittlungspflichten der Fluggesellschaften

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Fluggesellschaften mittels der „Push-Methode" die in Anhang I aufgelisteten PNR-Daten an die Datenbank der PNR-Zentralstelle des Mitgliedstaats übermitteln, in dessen Hoheitsgebiet der betreffende Flug ankommt oder von dem er abgeht, soweit sie solche Daten im Rahmen ihrer normalen Geschäftstätigkeit bereits erhoben haben. Bei Flügen mit Code-Sharing zwischen mehreren Fluggesellschaften liegt die Pflicht zur Übermittlung der PNR-Daten aller Fluggäste des Fluges bei der Fluggesellschaft, die den Flug durchführt. Erfolgen auf einem Drittstaatsflug eine oder mehrere Zwischenlandungen auf Flughäfen der Mitgliedstaaten, so übermitteln die Fluggesellschaften die PNR-Daten aller Fluggäste an die PNR-Zentralstellen aller betreffenden Mitgliedstaaten. Dies gilt auch, wenn bei einem EU-Flug eine oder mehrere Zwischenlandungen auf den Flughäfen verschiedener Mitgliedstaaten erfolgen, jedoch nur in Bezug auf Mitgliedstaaten, die PNR-Daten zu EU-Flügen erheben.

([1]) Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über das Recht der Unionsbürger und ihrer Familienangehörigen, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten, zur Änderung der Verordnung (EWG) Nr. 1612/68 und zur Aufhebung der Richtlinien 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG und 93/96/EWG (ABl. L 158 vom 30.4.2004, S. 77).

([2]) Verordnung (EG) Nr. 562/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. L 105 vom 13.4.2006, S. 1).

(2) Falls die Fluggesellschaften in Anhang I Nummer 18 aufgelistete erweiterte Fluggastdaten (API-Daten) erhoben haben, diese aber nicht auf die gleiche technische Weise wie andere PNR-Daten vorhalten, treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass die Fluggesellschaften mittels der „Push-Methode" auch diese Daten der PNR-Zentralstelle des in Absatz 1 genannten Mitgliedstaats übermitteln. Im Fall einer solchen Übermittlung gelten sämtliche Bestimmungen dieser Richtlinie in Bezug auf diese API-Daten.

(3) Die Fluggesellschaften übermitteln die PNR-Daten auf elektronischem Wege unter Verwendung der nach dem Prüfverfahren des Artikels 17 Absatz 2 festzulegenden gemeinsamen Protokolle und unterstützten Datenformate oder bei technischen Störungen auf jede andere geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet, und zwar

a) 24 bis 48 Stunden vor der planmäßigen Abflugzeit sowie

b) sofort nach Abfertigungsschluss, d. h., unmittelbar nachdem sich die Fluggäste vor dem Start an Bord des Flugzeugs begeben haben und keine Fluggäste mehr an Bord kommen oder von Bord gehen können.

(4) Die Mitgliedstaaten gestatten den Fluggesellschaften, die Übermittlung nach Absatz 3 Buchstabe b auf Aktualisierungen der gemäß Absatz 3 Buchstabe a übermittelten Daten zu beschränken.

(5) Wenn der Zugriff auf PNR-Daten erforderlich ist, um eine bestimmte und gegenwärtige Bedrohung im Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität abzuwehren, übermitteln die Fluggesellschaften die PNR-Daten in Einzelfällen auf Anfrage einer PNR-Zentralstelle im Einklang mit dem nationalen Recht zu anderen als den in Absatz 3 genannten Zeitpunkten.

Artikel 9

Informationsaustausch zwischen den Mitgliedstaaten

(1) Die Mitgliedstaaten stellen sicher, dass alle relevanten und erforderlichen PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von Personen, die von einer PNR-Zentralstelle nach Artikel 6 Absatz 2 ermittelt wurden, von dieser PNR-Zentralstelle den entsprechenden PNR-Zentralstellen der anderen Mitgliedstaaten übermittelt werden. Die PNR-Zentralstellen der Empfängermitgliedstaaten leiten gemäß Artikel 6 Absatz 6 die erhaltenen Daten an ihre zuständigen Behörden weiter.

(2) Die PNR-Zentralstelle eines Mitgliedstaats ist berechtigt, im Bedarfsfall bei der PNR-Zentralstelle jedes anderen Mitgliedstaats PNR-Daten, die in deren Datenbank vorgehalten werden und noch nicht gemäß Artikel 12 Absatz 2 durch Unkenntlichmachung von Datenelementen depersonalisiert wurden, sowie erforderlichenfalls auch die Ergebnisse jeglicher Verarbeitung dieser Daten, wenn dies bereits gemäß Artikel 6 Absatz 2 Buchstabe a erfolgt ist, anzufordern. Eine solche Anfrage ist gebührend zu begründen. Sie kann ein beliebiges Datenelement oder eine Kombination von Datenelementen betreffen, je nachdem, was die anfordernde PNR-Zentralstelle in dem konkreten Fall im Hinblick auf die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität für erforderlich erachtet. Die PNR-Zentralstellen übermitteln die angeforderten Informationen so rasch wie möglich. Falls die angeforderten Daten gemäß Artikel 12 Absatz 2 durch Unkenntlichmachung von Datenelementen depersonalisiert worden sind, stellt die PNR-Zentralstelle die vollständigen PNR-Daten nur bereit, wenn berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist, und nur, wenn sie durch eine in Artikel 12 Absatz 3 Buchstabe b genannte Behörde dazu ermächtigt ist.

(3) Die zuständigen Behörden eines Mitgliedstaats können bei der PNR-Zentralstelle jedes anderen Mitgliedstaats PNR-Daten, die in deren Datenbank vorgehalten werden, nur dann direkt anfordern, wenn dies in Notfällen erforderlich ist; dabei gelten die in Absatz 2 festgelegten Bedingungen. Die Anfragen der zuständigen Behörden müssen begründet sein. Der PNR-Zentralstelle des anfordernden Mitgliedstaats ist stets eine Kopie der Anfrage zu übermitteln. In allen übrigen Fällen richten die zuständigen Behörden ihre Anfrage zuerst an die PNR-Zentralstelle ihres Mitgliedstaats, die sie anschließend weiterleitet.

(4) Ist ausnahmsweise ein Zugriff auf PNR-Daten erforderlich, um eine bestimmte und gegenwärtige Bedrohung im Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität abwehren zu können, so ist die PNR-Zentralstelle eines Mitgliedstaats berechtigt, von der PNR-Zentralstelle eines anderen Mitgliedstaats zu verlangen, PNR-Daten gemäß Artikel 8 Absatz 5 anzufordern und sie der PNR-Zentralstelle, die die Anfrage gestellt hat, bereitzustellen.

(5) Der Austausch von Informationen nach Maßgabe dieses Artikels kann über alle Kanäle erfolgen, die für die Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten verfügbar sind. Für die Anfrage und den

Informationsaustausch ist die Sprache zu verwenden, die der jeweils gewählte Kommunikationsweg erfordert. Die Mitgliedstaaten teilen der Kommission zusammen mit ihren Angaben gemäß Artikel 4 Absatz 5 die Daten einer Kontaktstelle für Anfragen in Notfällen mit. Die Kommission leitet diese Daten an die Mitgliedstaaten weiter.

Artikel 10

Bedingungen für den Zugang von Europol zu PNR-Daten

(1) Europol ist berechtigt, im Rahmen seiner Zuständigkeiten und zur Ausübung seiner Aufgaben PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von den PNR-Zentralstellen der Mitgliedstaaten anzufordern.

(2) Europol kann im Einzelfall über die nationale Europol-Stelle eine gebührend begründete Anfrage an die PNR-Zentralstelle eines Mitgliedstaats zwecks Übermittlung bestimmter PNR-Daten oder der Ergebnisse der Verarbeitung dieser Daten auf elektronischem Wege richten. Europol kann eine solche Anfrage stellen, wenn dies für die Unterstützung und Verstärkung von Maßnahmen der Mitgliedstaaten zur Verhütung, Aufdeckung oder Ermittlung einer bestimmten terroristischen Straftat oder schwerer Kriminalität unbedingt notwendig ist und die Straftat gemäß dem Beschluss 2009/371/JI in die Zuständigkeit von Europol fällt. In dieser Anfrage sind hinreichende Gründe dafür anzugeben, dass Europol davon ausgeht, dass die Übermittlung der PNR-Daten oder der Ergebnisse der Verarbeitung von PNR-Daten wesentlich zur Verhütung, Aufdeckung oder Ermittlung der betreffenden Straftat beitragen wird.

(3) Europol benachrichtigt den gemäß Artikel 28 des Beschlusses 2009/371/JI ernannten Datenschutzbeauftragten über jeden Informationsaustausch gemäß diesem Artikel.

(4) Der Informationsaustausch gemäß diesem Artikel erfolgt über SIENA und in Einklang mit dem Beschluss 2009/371/JI. Für die Anfrage und den Informationsaustausch ist die Sprache zu verwenden, die für SIENA Anwendung findet.

Artikel 11

Übermittlungen von Daten an Drittstaaten

(1) Die Mitgliedstaaten dürfen die PNR-Daten und die Ergebnisse der Verarbeitung dieser Daten, die durch die PNR-Zentralstelle nach Artikel 12 gespeichert werden, nur im Einzelfall und nur dann an einen Drittstaat übermitteln, wenn

a) die Bedingungen des Artikels 13 des Rahmenbeschlusses 2008/977/JI erfüllt sind;

b) die Übermittlung für die in Artikel 1 Absatz 2 genannten Zwecke dieser Richtlinie erforderlich ist;

c) der Drittstaat sich bereit erklärt, die Daten nur dann an einen anderen Drittstaat zu übermitteln, wenn dies für die in Artikel 1 Absatz 2 genannten Zwecke dieser Richtlinie unbedingt notwendig ist und nur wenn der jeweilige Mitgliedstaat ausdrücklich zustimmt, und

d) die gleichen Bedingungen wie in Artikel 9 Absatz 2 erfüllt sind.

(2) Ungeachtet des Artikels 13 Absatz 2 des Rahmenbeschlusses 2008/977/JI sind Übermittlungen von PNR-Daten ohne vorherige Zustimmung des Mitgliedstaats, von dem die Daten eingeholt wurden, nur unter außergewöhnlichen Umständen und nur dann zulässig, wenn

a) eine solche Übermittlung unerlässlich ist, um eine bestimmte und gegenwärtige Bedrohung durch terroristische Straftaten oder schwere Kriminalität in einem Mitgliedstaat oder einem Drittstaat abzuwehren, und

b) die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann.

Die für die Erteilung der Zustimmung zuständige Behörde wird unverzüglich unterrichtet und die Übermittlung wird ordnungsgemäß aufgezeichnet und einer Ex-Post-Überprüfung unterzogen.

(3) Die Mitgliedstaaten übermitteln PNR-Daten nur unter Bedingungen im Einklang mit dieser Richtlinie und nach Vergewisserung, dass die von den Empfängern beabsichtigte Verwendung der PNR-Daten mit diesen Bedingungen und Sicherheitsvorkehrungen in Einklang steht, an die zuständigen Behörden von Drittstaaten.

(4) Der Datenschutzbeauftragte der PNR-Zentralstelle des Mitgliedstaats, der die PNR-Daten übermittelt hat, wird über jede Übermittlung von PNR-Daten durch den Mitgliedstaat gemäß diesem Artikel unterrichtet.

Artikel 12

Speicherfrist und Depersonalisierung

(1) Die Mitgliedstaaten stellen sicher, dass die von den Fluggesellschaften an die PNR-Zentralstelle übermittelten PNR-Daten für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen beziehungsweise von dem er abgegangen ist, in einer bei dieser PNR-Zentralstelle angesiedelten Datenbank vorgehalten werden.

(2) Nach Ablauf einer Frist von sechs Monaten ab Übermittlung der PNR-Daten gemäß Absatz 1 werden alle PNR-Daten durch Unkenntlichmachung der folgenden Datenelemente, mit denen die Identität des Fluggasts, auf den sich die PNR-Daten beziehen, unmittelbar festgestellt werden könnte, depersonalisiert:

a) Name(n), auch die Namen und die Zahl der im PNR-Datensatz verzeichneten mitreisenden Personen;

b) Anschrift und Kontaktdaten;

c) alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Fluggasts, zu dem die PNR-Daten erstellt wurden, oder anderer Personen beitragen könnten;

d) Vielflieger-Eintrag;

e) allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten, zu dem die PNR-Daten erstellt wurden, und

f) jedwede erhobenen API-Daten.

(3) Nach Ablauf der in Absatz 2 genannten Frist von sechs Monaten ist die Offenlegung der vollständigen PNR-Daten nur zulässig, wenn

a) berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist und

b) dies genehmigt wird durch

   i) eine Justizbehörde oder

   ii) eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten.

(4) Die Mitgliedstaaten stellen sicher, dass die PNR-Daten nach Ablauf der Frist nach Absatz 1 dauerhaft gelöscht werden. Diese Verpflichtung lässt Fälle unberührt, in denen bestimmte PNR-Daten an eine zuständige Behörde übermittelt wurden und im Zusammenhang mit einem konkreten Fall zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität verwendet werden; in diesem Fall richtet sich die Frist für die Speicherung dieser Daten durch die zuständige Behörde nach nationalem Recht.

(5) Die Ergebnisse der Verarbeitung nach Artikel 6 Absatz 2 Buchstabe a werden von der PNR-Zentralstelle nur so lange vorgehalten, wie dies erforderlich ist, um die zuständigen Behörden und die PNR-Zentralstellen anderer Mitgliedstaaten gemäß Artikel 9 Absatz 1 über einen Treffer zu informieren. Fällt die in Artikel 6 Absatz 5 genannte anschließende individuelle nicht-automatisierte Überprüfung eines Treffers bei der automatisierten Verarbeitung negativ aus, so kann dieses Ergebnis dennoch gespeichert werden, um künftige „falsche“ Treffer zu vermeiden, solange die dazugehörigen Daten nicht gemäß Absatz 4 dieses Artikels gelöscht sind.

Artikel 13

Schutz personenbezogener Daten

(1) Jeder Mitgliedstaat sorgt im Zusammenhang mit der Verarbeitung personenbezogener Daten nach dieser Richtlinie dafür, dass die Rechte jedes Fluggasts in Bezug auf Schutz personenbezogener Daten, Zugang, Berichtigung, Löschung und Einschränkung der Verarbeitung sowie Schadenersatz und Rechtsbehelfe den Rechten entsprechen, die nach Unionsrecht und nationalem Recht sowie zur Umsetzung der Artikel 17, 18, 19 und 20 des Rahmenbeschlusses 2008/977/JI festgelegt sind. Diesbezüglich gelten daher jene Artikel.

(2) Jeder Mitgliedstaat sorgt dafür, dass die nach nationalem Recht erlassenen Bestimmungen zur Umsetzung der Artikel 21 und 22 des Rahmenbeschlusses 2008/977/JI betreffend die Vertraulichkeit der Verarbeitung und die Datensicherheit ebenfalls auf jede Verarbeitung personenbezogener Daten nach dieser Richtlinie Anwendung finden.

(3) Diese Richtlinie berührt nicht die Anwendbarkeit der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates ([1]) auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften, insbesondere deren Pflichten, geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der personenbezogenen Daten zu treffen.

(4) Die Mitgliedstaaten untersagen die Verarbeitung von PNR-Daten, die die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben oder ihre sexuelle Orientierung erkennen lassen. Bei der PNR-Zentralstelle eingehende PNR-Daten, aus denen derartige Informationen hervorgehen, werden umgehend gelöscht.

(5) Die Mitgliedstaaten sorgen dafür, dass die PNR-Zentralstellen alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren dokumentieren. Diese Dokumentation muss zumindest folgende Unterlagen enthalten:

a) den Namen und die Kontaktinformationen der Organisation und des Personals der PNR-Zentralstelle, die mit der Verarbeitung der PNR-Daten beauftragt sind, und die verschiedenen Ebenen der Zugangsberechtigungen;

b) die Anfragen von zuständigen Behörden und PNR-Zentralstellen anderer Mitgliedstaaten;

c) jede Anfrage und jede Übermittlung von PNR-Daten durch bzw. an Drittstaaten.

Die PNR-Zentralstelle stellt der nationalen Kontrollstelle auf Anfrage alle verfügbare Dokumentation zur Verfügung.

(6) Die Mitgliedstaaten stellen sicher, dass die PNR-Zentralstelle mindestens über folgende Verarbeitungsvorgänge Aufzeichnungen führt: Erhebung, Abfrage, Offenlegung und Löschung. Den Aufzeichnungen über Abfragen und Offenlegung müssen der Zweck, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person zu entnehmen sein, die die PNR-Daten abgefragt oder offengelegt hat, sowie die Identität der Empfänger dieser Daten. Die Aufzeichnungen werden ausschließlich zu Zwecken der Überprüfung, der Eigenüberwachung, der Sicherstellung der Datenintegrität und der Datensicherheit oder des Audits verwendet. Die PNR-Zentralstelle stellt der nationalen Kontrollstelle auf Anfrage die Aufzeichnungen zur Verfügung.

Diese Aufzeichnungen sind fünf Jahre lang aufzubewahren.

(7) Die Mitgliedstaaten sorgen dafür, dass ihre PNR-Zentralstelle technische und organisatorische Maßnahmen und Verfahren umsetzt, um ein hohes Sicherheitsniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden PNR-Daten angemessen ist.

(8) Die Mitgliedstaaten sorgen dafür, dass die PNR-Zentralstelle die betroffene Person und die nationale Kontrollstelle unverzüglich von einer Verletzung des Schutzes personenbezogener Daten benachrichtigt, wenn diese Verletzung voraussichtlich ein hohes Risiko für den Schutz der personenbezogenen Daten oder eine Verletzung der Privatsphäre der betroffenen Person zur Folge hat.

Artikel 14

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Vorschriften zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen.

Insbesondere erlassen die Mitgliedstaaten Vorschriften über Sanktionen einschließlich Geldbußen gegen Fluggesellschaften, die die Daten nicht gemäß Artikel 8 übermitteln oder hierzu nicht das vorgeschriebene Format verwenden.

Die vorgesehenen Sanktionen müssen wirksam, angemessen und abschreckend sein.

([1]) 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. L 281 vom 23.11.1995, S. 31).

Artikel 15

Nationale Kontrollstelle

(1) Jeder Mitgliedstaat sorgt dafür, dass die nationale Kontrollstelle gemäß Artikel 25 des Rahmenbeschlusses 2008/977/JI für die Beratung und Kontrolle hinsichtlich der Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen nationalen Vorschriften in seinem Hoheitsgebiet verantwortlich ist. Artikel 25 des Rahmenbeschlusses 2008/977/JI findet Anwendung.

(2) Diese nationalen Kontrollstellen erfüllen ihre Aufgaben gemäß Absatz 1, um die Grundrechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu schützen.

(3) Aufgaben jeder nationalen Kontrollstelle sind

a) die Behandlung von Beschwerden betroffener Personen, die Untersuchung der Angelegenheit und Unterrichtung der betroffenen Personen über den Fortgang und das Ergebnis der Beschwerde innerhalb einer angemessenen Frist;

b) die Prüfung der Rechtmäßigkeit der Datenverarbeitung, die Durchführung von Ermittlungen, Inspektionen und Audits gemäß nationalem Recht entweder aus eigener Initiative oder aufgrund einer Beschwerde gemäß Buchstabe a.

(4) Jede nationale Kontrollstelle berät auf Anfrage eine betroffene Person bei der Wahrnehmung der Rechte, die ihr aufgrund der nach Maßgabe dieser Richtlinie erlassenen Vorschriften zustehen.

KAPITEL III

Durchführungsmassnahmen

Artikel 16

Gemeinsame Protokolle und unterstützte Datenformate

(1) Alle von den Fluggesellschaften für die Zwecke dieser Richtlinie vorgenommenen Übermittlungen von PNR-Daten an die PNR-Zentralstellen erfolgen mittels elektronischer Hilfsmittel, die hinsichtlich der technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen für die vorzunehmende Verarbeitung ausreichende Gewähr bieten. Bei einer technischen Störung werden die PNR-Daten auf jede andere geeignete Weise übermittelt, vorausgesetzt, dass die gleiche Sicherheitsstufe beibehalten und das Datenschutzrecht der Union vollständig eingehalten wird.

(2) Ein Jahr nach der ersten Annahme der gemeinsamen Protokolle und unterstützten Datenformate durch die Kommission gemäß Absatz 3 erfolgen sämtliche von den Fluggesellschaften für die Zwecke dieser Richtlinie vorgenommenen Übermittlungen von PNR-Daten an die PNR-Zentralstellen auf elektronischem Weg unter Verwendung sicherer Übermittlungsmethoden entsprechend diesen gemeinsamen Protokollen. Diese Protokolle sind für alle Übermittlungen identisch, um die Sicherheit der PNR-Daten während der Übermittlung zu gewährleisten. Die PNR-Daten werden unter Verwendung eines unterstützten Datenformats übermittelt, das die Lesbarkeit der Daten für alle Beteiligten garantiert. Alle Fluggesellschaften sind gehalten, das gemeinsame Protokoll und das Datenformat, das sie für ihre Übermittlungen zu verwenden gedenken, auszuwählen und beides der PNR-Zentralstelle mitzuteilen.

(3) Die Liste der gemeinsamen Protokolle und unterstützten Datenformate wird mittels Durchführungsrechtsakten von der Kommission erstellt und im Bedarfsfall angepasst. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 17 Absatz 2 erlassen.

(4) Absatz 1 ist anwendbar, solange die gemeinsamen Protokolle und unterstützten Datenformate gemäß den Absätzen 2 und 3 nicht vorliegen.

(5) Die Mitgliedstaaten stellen sicher, dass innerhalb eines Jahres nach der Annahme der in Absatz 2 genannten gemeinsamen Protokolle und Datenformate die erforderlichen technischen Maßnahmen ergriffen werden, damit die gemeinsamen Protokolle und Datenformate angewendet werden können.

Artikel 17

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.

Gibt der Ausschuss keine Stellungnahme ab, so erlässt die Kommission den Entwurf des Durchführungsrechtsakts nicht und Artikel 5 Absatz 4 Unterabsatz 3 der Verordnung (EU) Nr. 182/2011 findet Anwendung.

KAPITEL IV

Schlussbestimmungen

Artikel 18

Umsetzung

(1) Die Mitgliedstaaten setzen die Rechts- und Verwaltungsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie bis zum 25. Mai 2018 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf die vorliegende Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 19

Überprüfung

(1) Anhand von Informationen der Mitgliedstaaten, einschließlich der statistischen Daten nach Artikel 20 Absatz 2, nimmt die Kommission bis zum 25. Mai 2020 eine Überprüfung aller Elemente dieser Richtlinie vor und legt dem Europäischen Parlament und dem Rat einen Bericht vor und erläutert diesen.

(2) Bei der Vornahme ihrer Überprüfung berücksichtigt die Kommission insbesondere

a) die Einhaltung des einschlägigen Schutzstandards bezüglich personenbezogener Daten;

b) die Erforderlichkeit und Verhältnismäßigkeit der Erhebung und Verarbeitung von PNR-Daten für jeden der in dieser Richtlinie genannten Zwecke;

c) die Datenspeicherungsfristen;

d) die Effektivität des Informationsaustauschs zwischen den Mitgliedstaaten und

e) die Qualität der Prüfungen, einschließlich in Bezug auf die nach Maßgabe von Artikel 20 erhobenen statistischen Daten.

(3) Der Bericht gemäß Absatz 1 enthält zudem eine Überprüfung der Erforderlichkeit, Verhältnismäßigkeit und Wirksamkeit der Aufnahme der obligatorischen Erhebung und Übermittlung von PNR-Daten in Bezug auf sämtliche oder ausgewählte EU-Flüge in den Anwendungsbereich dieser Richtlinie. Die Kommission berücksichtigt dabei die Erfahrungen der Mitgliedstaaten, insbesondere jener Mitgliedstaaten, die gemäß Absatz 2 diese Richtlinie auf EU-Flüge anwenden. In dem Bericht wird auch geprüft, ob es erforderlich ist, Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen — einschließlich Flugbuchungen — erbringen, in den Anwendungsbereich dieser Richtlinie aufzunehmen.

(4) Auf der Grundlage der Überprüfung nach diesem Artikel legt die Kommission dem Europäischen Parlament und dem Rat gegebenenfalls einen Gesetzgebungsvorschlag zur Änderung dieser Richtlinie vor.

Artikel 20

Statistische Daten

(1) Die Mitgliedstaaten stellen der Kommission jährlich Statistiken über die an die PNR-Zentralstellen übermittelten PNR-Daten zur Verfügung. Diese Statistiken dürfen keine personenbezogenen Daten enthalten.

(2) Die Statistiken müssen mindestens Folgendes ausweisen:

a) die Gesamtzahl der Fluggäste, deren PNR-Daten erhoben und ausgetauscht worden sind;

b) die Zahl der Fluggäste, bei denen eine weitere Überprüfung für angezeigt erachtet wurde.

Artikel 21

Verhältnis zu anderen Rechtsakten

(1) Es steht den Mitgliedstaaten frei, am 24. Mai 2016 geltende bilaterale oder multilaterale Übereinkünfte oder Vereinbarungen untereinander über den Austausch von Informationen zwischen zuständigen Behörden auch weiterhin anzuwenden, soweit diese Übereinkünfte oder Vereinbarungen mit dieser Richtlinie vereinbar sind.

(2) Diese Richtlinie berührt nicht die Anwendbarkeit der Richtlinie 95/46/EG auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften.

(3) Diese Richtlinie berührt nicht die Verpflichtungen und Zusagen der Mitgliedstaaten oder der Union aufgrund bilateraler oder multilateraler Übereinkünfte mit Drittstaaten.

Artikel 22

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 27. April 2016.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

ANHANG I

Von Fluggesellschaften erhobene PNR-Daten

1. PNR-Buchungscode (Record Locator)
2. Datum der Buchung/Flugscheinausstellung
3. Planmäßiges Abflugdatum bzw. planmäßige Abflugdaten
4. Name(n)
5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)
6. Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift
7. Gesamter Reiseverlauf für bestimmte PNR-Daten
8. Vielflieger-Eintrag
9. Reisebüro/Sachbearbeiter
10. Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (No show) und Fluggäste mit Flugschein, aber ohne Reservierung (Go show)
11. Angaben über gesplittete/geteilte PNR-Daten
12. Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)
13. Flugscheindaten einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug (One-way), automatische Tarifanzeige (Automated Ticket Fare Quote fields)
14. Sitzplatznummer und sonstige Sitzplatzinformationen
15. Code-Sharing
16. Vollständige Gepäckangaben
17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten
18. Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft)
19. Alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR-Daten.

ANHANG II

Liste der strafbaren Handlungen gemäß Artikel 3 Nummer 9

1. Beteiligung an einer kriminellen Vereinigung
2. Menschenhandel
3. Sexuelle Ausbeutung von Kindern und Kinderpornografie
4. Illegaler Handel mit Drogen und psychotropen Stoffen
5. Illegaler Handel mit Waffen, Munition und Sprengstoffen
6. Korruption
7. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Union
8. Wäsche von Erträgen aus Straftaten und Geldfälschung, einschließlich Euro-Fälschung
9. Computerstraftaten/Cyberkriminalität
10. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten
11. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt
12. Vorsätzliche Tötung, schwere Körperverletzung
13. Illegaler Handel mit menschlichen Organen und menschlichem Gewebe
14. Entführung, Freiheitsberaubung und Geiselnahme
15. Diebstahl in organisierter Form oder mit Waffen
16. Illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen
17. Betrügerische Nachahmung und Produktpiraterie
18. Fälschung von amtlichen Dokumenten und Handel damit
19. Illegaler Handel mit Hormonen und anderen Wachstumsförderern
20. Illegaler Handel mit nuklearen und radioaktiven Substanzen
21. Vergewaltigung
22. Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen
23. Flugzeug- und Schiffsentführung
24. Sabotage
25. Handel mit gestohlenen Kraftfahrzeugen
26. Wirtschaftsspionage

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
2985 Luxemburg
LUXEMBURG

DE