



EUROPÄISCHE KOMMISSION

Brüssel, den 25.1.2012  
KOM(2012) 11 endgültig

2012/0011 (COD)

Vorschlag für

**VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

**zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und  
zum freien Datenverkehr (Datenschutz-Grundverordnung)**

(Text von Bedeutung für den EWR)

{SEK(2012) 72 endgültig}

{SEK(2012) 73 endgültig}

## BEGRÜNDUNG

### 1. KONTEXT

Der in der Mitteilung KOM(2012) 9<sup>1</sup> skizzierte Vorschlag der Kommission für einen neuen Rechtsrahmen zum Schutz personenbezogener Daten in der EU wird im Folgenden näher erläutert. Die vorgeschlagene neue Datenschutzregelung besteht aus zwei Teilen:

- einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und
- einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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<sup>2</sup>.

Diese Begründung bezieht sich auf den Legislativvorschlag für die Datenschutz-Grundverordnung.

Kernstück der EU-Vorschriften zum Schutz personenbezogener Daten ist die Richtlinie 95/46/EG<sup>3</sup> aus dem Jahr 1995, die auf zweierlei abzielt: Schutz des Grundrechts auf Datenschutz und Garantie des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten. Ergänzt wurde die Richtlinie durch den Rahmenbeschluss 2008/977/JI, der den Schutz personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen regelt.<sup>4</sup>

Der rasche technologische Fortschritt stellt den Datenschutz vor neue Herausforderungen. Das Ausmaß, in dem Daten ausgetauscht und erhoben werden, hat rasant zugenommen. Die Technik macht es möglich, dass Privatwirtschaft und Staat im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend werden auch private Informationen ins weltweite Netz gestellt und damit öffentlich zugänglich gemacht. Die Informationstechnologie hat das wirtschaftliche und gesellschaftliche Leben gründlich verändert.

Die wirtschaftliche Entwicklung setzt Vertrauen in die Online-Umgebung voraus. Verbraucher, denen es an Vertrauen mangelt, scheuen Online-Einkäufe und neue Dienste. Hierdurch könnte sich die Entwicklung innovativer Anwendungen neuer Technologien

---

<sup>1</sup> „Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“, KOM(2012) 9 endgültig.

<sup>2</sup> KOM(2012) 10 endg.

<sup>3</sup> 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).

<sup>4</sup> 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) („Rahmenbeschluss“).

verlangsamten. Der Schutz personenbezogener Daten spielt daher eine zentrale Rolle in der Digitalen Agenda für Europa<sup>5</sup> und allgemein in der Strategie Europa 2020<sup>6</sup>.

In Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der mit dem Vertrag von Lissabon eingeführt wurde, ist der Grundsatz verankert, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Seit dem Vertrag von Lissabon verfügt die Union mit Artikel 16 Absatz 2 AEUV überdies über eine besondere Rechtsgrundlage für den Erlass von Datenschutzvorschriften. Der Schutz personenbezogener Daten ist in Artikel 8 der EU-Grundrechtecharta als Grundrecht ausgestaltet.

Der Europäische Rat hat die Kommission ersucht, die Funktionsweise der verschiedenen Rechtsinstrumente zum Datenschutz zu bewerten und erforderlichenfalls weitere Initiativen legislativer und nicht-legislativer Art vorzulegen.<sup>7</sup> In seiner Entschließung zum Stockholmer Programm begrüßte das Europäische Parlament<sup>8</sup> den Vorschlag, eine umfassende Regelung für den Schutz personenbezogener Daten innerhalb der Europäischen Union zu schaffen, und forderte unter anderem eine Überarbeitung des Rahmenbeschlusses 2008/977/JI. In ihrem Aktionsplan zur Umsetzung des Stockholmer Programms<sup>9</sup> betonte die Kommission die Notwendigkeit, in allen Bereichen der EU-Politik für eine konsequente Anwendung des Grundrechts auf Datenschutz zu sorgen.

Die EU braucht, wie die Kommission in ihrer Mitteilung über ein Gesamtkonzept für den Datenschutz in der Europäischen Union<sup>10</sup> feststellte, ein umfassenderes, kohärenteres Konzept für das Grundrecht auf Schutz personenbezogener Daten.

Die Ziele und Grundsätze der derzeitigen Datenschutzregelung bleiben gültig, aber sie hat eine unterschiedliche Handhabung des Datenschutzes in der Union, Rechtsunsicherheit sowie die weit verbreitete öffentliche Meinung, dass speziell im Internet der Datenschutz nicht immer gewährleistet ist, nicht verhindern können.<sup>11</sup> Deshalb ist es jetzt an der Zeit, eine konsequentere, kohärentere Datenschutzregelung in der EU zu schaffen, die durchsetzbar ist und die Voraussetzungen dafür bietet, dass die digitale Wirtschaft im Binnenmarkt weiter Fuß fasst, die Bürger Kontrolle über ihre eigenen Daten erhalten und die Sicherheit für Wirtschaft und Staat in rechtlicher wie praktischer Hinsicht erhöht wird.

## **2. ERGEBNISSE DER ANHÖRUNGEN UND FOLGENABSCHÄTZUNGEN**

Diese Initiative zur Überarbeitung der derzeitigen Datenschutzbestimmungen ist das Ergebnis umfassender Konsultationen, die über zwei Jahre andauerten und an denen die wichtigsten

---

<sup>5</sup> KOM(2010) 245 endg.

<sup>6</sup> KOM(2010) 2020 endg.

<sup>7</sup> „Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger“ (ABl. C 115 vom 4.5.2010, S. 1).

<sup>8</sup> Entschließung des Europäischen Parlaments vom 25. November 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat – Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger – Stockholm-Programm (P7\_TA(2009)0090).

<sup>9</sup> KOM(2010) 171 endg.

<sup>10</sup> KOM(2010) 609 endg.

<sup>11</sup> Siehe Special Eurobarometer 359 – *Data Protection and Electronic Identity in the EU* (2011): [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

Interessengruppen beteiligt waren. Im Mai 2009<sup>12</sup> wurde eine Konferenz abgehalten, an der hochrangige Vertreter aus den Mitgliedstaaten teilnahmen. Die öffentliche Konsultation fand in zwei Phasen statt:

- 9. Juli bis 31. Dezember 2009 – *Konsultation zum Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten*: Bei der Kommission gingen 168 Antworten ein: 127 von Einzelpersonen, Vereinigungen, Wirtschafts- und Fachverbänden sowie 12 von öffentlicher Seite.<sup>13</sup>
- 4. November 2010 bis 15. Januar 2011 – *Konsultation zum Gesamtkonzept der Kommission für den Datenschutz in der Europäischen Union*. Die Kommission erhielt 305 Antworten: 54 von Bürgern, 31 von staatlicher Seite und 220 von privaten Organisationen, insbesondere von Unternehmensverbänden und Nichtregierungsorganisationen.<sup>14</sup>

Daneben fanden Anhörungen mit wichtigen Interessenträgern zu speziellen Themen statt. Im Juni und Juli 2010 wurden Veranstaltungen für die Behörden der Mitgliedstaaten und private Interessengruppen sowie für Datenschutz- und Verbraucherverbände organisiert.<sup>15</sup> Im November 2010 veranstaltete die Vizepräsidentin der Europäischen Kommission Reding einen Runden Tisch zur Datenschutzreform. Am 28. Januar 2011 (Tag des Datenschutzes) veranstaltete die Europäische Kommission gemeinsam mit dem Europarat eine Konferenz mit hochrangigen Vertretern, auf der Themen im Zusammenhang mit der Datenschutzreform der EU sowie die Notwendigkeit gemeinsamer weltweiter Datenschutzstandards erörtert wurden.<sup>16</sup> Zwei weitere Konferenzen fanden am 16./17. Juni 2011 und 21. September 2011 auf Betreiben der ungarischen bzw. der polnischen Ratspräsidentschaft statt.

Daneben wurden 2011 im Laufe des Jahres Fachseminare und Workshops zu einzelnen Themenschwerpunkten abgehalten. Im Januar veranstaltete die Europäische Agentur für Netz- und Informationssicherheit (ENISA)<sup>17</sup> einen Workshop, der sich mit der Meldung von Datenschutzverstößen in Europa befasste<sup>18</sup>. Im Februar fand ein Workshop der Kommission mit Behörden der Mitgliedstaaten statt, auf dem über Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen und über die Umsetzung des Rahmenbeschlusses gesprochen wurde. Gleichzeitig veranstaltete die Grundrechte-Agentur eine Konsultationssitzung zum Thema „Datenschutz und Schutz der Privatsphäre“. Eine Diskussion mit nationalen Datenschutzbehörden über Kernpunkte der Reform fand am 13. Juli 2011 statt. Die EU-Bürger konnten sich bei einer Eurobarometer-Umfrage äußern, die von November bis Dezember 2010 durchgeführt wurde<sup>19</sup>. Darüber hinaus sind auch eine Reihe von Studien in Auftrag gegeben worden.<sup>20</sup> Von der Artikel-29-Datenschutzgruppe,<sup>21</sup>

---

<sup>12</sup> [http://ec.europa.eu/justice/newsroom/data-protection/events/090519\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm).

<sup>13</sup> Die nichtvertrauliche Fassung der Beiträge kann auf der Website der Kommission eingesehen werden: [http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm).

<sup>14</sup> Die nichtvertrauliche Fassung der Beiträge kann auf der Website der Kommission eingesehen werden: [http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm).

<sup>15</sup> [http://ec.europa.eu/justice/newsroom/data-protection/events/100701\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm).

<sup>16</sup> [http://www.coe.int/t/dghl/standardsetting/dataprotection/Data\\_protection\\_day2011\\_en.asp](http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp).

<sup>17</sup> ENISA befasst sich mit der Datensicherheit in Kommunikationsnetzen und Informationssystemen.

<sup>18</sup> Siehe <http://www.enisa.europa.eu/act/it/data-breach-notification/>.

<sup>19</sup> Siehe Special Eurobarometer 359 – *Data Protection and Electronic Identity in the EU* (2011): [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

<sup>20</sup> Neben der „Study on the economic benefits of privacy enhancing technologies“ siehe auch die Vergleichende Studie über verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den

die mehrere Stellungnahmen abgab, erhielt die Kommission sachdienliche Beiträge<sup>22</sup>. Zu den Fragen, die die Kommission in ihrer Mitteilung vom November 2010 aufgeworfen hatte, nahm auch der Europäische Datenschutzbeauftragte umfassend Stellung.<sup>23</sup>

Mit seiner EntschlieÙung vom 6. Juli 2011 billigte das Europäische Parlament einen Bericht, der das Konzept der Kommission für die Reform des Datenschutzrechts unterstützte.<sup>24</sup> Am 24. Februar 2011 nahm der Rat der Europäischen Union Schlussfolgerungen an, in denen er das Reformvorhaben der Kommission generell befürwortete und der Vorgehensweise der Kommission in vielen Punkten zustimmte. Auch der Europäische Wirtschafts- und Sozialausschuss unterstützte das Ziel der Kommission, durch eine angemessene Überarbeitung der Richtlinie 95/46/EG für eine kohärente Anwendung der EU-Datenschutzregeln in allen Mitgliedstaaten zu sorgen.<sup>25</sup>

Im Zuge der Konsultationen zum Datenschutz-Gesamtkonzept stellte eine breite Mehrheit der Teilnehmer fest, dass die allgemeinen Grundsätze zwar nach wie vor gültig sind, die derzeitige Regelung aber angepasst werden muss, um besser auf die rasante Entwicklung neuer Technologien (vor allem von Online-Technologien) und die zunehmende Globalisierung reagieren zu können. Die Datenschutzregelung sollte allerdings technologieutral bleiben. Die unterschiedliche Handhabung des Datenschutzes in der Union wurde vor allem von der Wirtschaft stark kritisiert. Gefordert wurde mehr Rechtssicherheit und eine stärkere Angleichung der Datenschutzvorschriften. Die komplexen Vorschriften für den internationalen Transfer personenbezogener Daten werden von den Unternehmen, die regelmäßig personenbezogene Daten aus der EU ins Ausland transferieren müssen, als beträchtliches Hemmnis für ihre Tätigkeit angesehen.

Entsprechend ihrer Strategie für eine bessere Rechtsetzung hat die Kommission eine Folgenabschätzung der in Frage kommenden Optionen vorgenommen<sup>26</sup>. Grundlage der Folgenabschätzung waren drei Zielsetzungen: Stärkung der Binnenmarktdimension beim Datenschutz, wirksamere Ausübung der Datenschutzrechte durch den Einzelnen und Schaffung einer umfassenden, kohärenten Regelung für alle Zuständigkeitsbereiche der Union einschließlich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Drei

---

Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen, vom Januar 2010 ([http://ec.europa.eu/justice/policies/privacy/docs/studies/new\\_privacy\\_challenges/final\\_report\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_de.pdf)).

<sup>21</sup> Die Arbeitsgruppe wurde 1996 auf der Grundlage von Artikel 29 der Richtlinie mit beratender Funktion eingesetzt. Ihr gehören die nationalen Datenschutzbehörden an sowie der Europäische Datenschutzbeauftragte und die Kommission. Weitere Informationen zur Tätigkeit der Datenschutzgruppe unter [http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm).

<sup>22</sup> Siehe unter anderem die Stellungnahmen zur Zukunft des Datenschutzes (2009, WP 168), zum Begriff des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters (1/2010, WP 169), zur verhaltensbezogenen Internetwerbung (2/2010, WP 171), zum Rechenschaftsprinzip (3/2010, WP 173), zum anwendbaren Recht (8/2010, WP 179) und zur Einwilligung (15/2011, WP 187). Auf Aufforderung der Kommission erstellte die Gruppe zudem drei Gutachten zur Meldepflicht, zu sensiblen Daten und zur Umsetzung von Artikel 28 Absatz 6 der Datenschutzrichtlinie. Die Arbeiten der Gruppe können eingesehen werden unter: [http://ec.europa.eu/justice/data-protection/article-29/documentation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm).

<sup>23</sup> Abrufbar auf der Website des EDSB: <http://www.edps.europa.eu/EDPSWEB/>.

<sup>24</sup> EntschlieÙung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//DE> (Berichtersteller: MEP Axel Voss (EPP/DE).

<sup>25</sup> CESE 999/2011.

<sup>26</sup> SEK(2012) 72.

Optionen mit unterschiedlicher Eingriffswirkung wurden geprüft: Die erste Option sieht minimale legislative Änderungen und Mitteilungen zu Auslegungsfragen sowie unterstützende Maßnahmen wie Finanzierungsprogramme und technische Hilfsmittel vor. Die zweite Option besteht aus einer punktuellen Regelung der in der Analyse festgestellten Problemstellungen, während die dritte Option eine Verankerung des Datenschutzes auf EU-Ebene durch präzise, detaillierte Vorschriften für alle Sektoren und die Gründung einer EU-Agentur für die Überwachung und Durchsetzung der Vorschriften vorsieht.

Bei jeder Option wurde entsprechend der üblichen Vorgehensweise der Kommission mithilfe einer Lenkungsgruppe mit Vertretern aus den beteiligten Generaldirektionen der Kommission geprüft, inwieweit mit der Option die Zielvorgaben erreicht werden, wie sich die Option wirtschaftlich auswirkt (auch auf den Haushalt der EU-Organe), welche sozialen Auswirkungen mit ihr verbunden sind und welche Auswirkungen auf die Grundrechte zu erwarten sind. Auswirkungen auf die Umwelt wurden nicht festgestellt. Nach Betrachtung der einzelnen Optionen in ihrer Gesamtwirkung wurde die hier favorisierte Option ausgearbeitet, die auf der zweiten Option basiert mit Elementen aus den anderen beiden Optionen. Diese Option wird der Folgenabschätzung zufolge erhebliche Verbesserungen bringen unter anderem durch mehr Rechtssicherheit für die Bürger und für die für die Datenverarbeitung Verantwortlichen, durch einen geringeren Verwaltungsaufwand, eine einheitlichere Anwendung des Datenschutzrechts in der Union, durch die konkrete Möglichkeit für den Einzelnen, seine Rechte auf Schutz seiner personenbezogenen Daten innerhalb der EU wahrzunehmen, und durch eine wirksame Überwachung und Durchsetzung des Datenschutzes. Es wird erwartet, dass die hier bevorzugte Option auch dazu beitragen wird, die Ziele, die sich die Kommission in Bezug auf Verwaltungsvereinfachung und Verringerung des Verwaltungsaufwands gesteckt hat, sowie die Zielvorgaben der Digitalen Agenda für Europa, des Stockholmer Aktionsplans und der Strategie Europa 2020 zu erreichen.

Der Ausschuss für Folgenabschätzung nahm am 9. September 2011 zum Entwurf der Folgenabschätzung Stellung. Die Folgenabschätzung wurde daraufhin wie folgt abgeändert:

- Präzisiert wurde, inwieweit die Ziele der derzeitigen Datenschutzregelung erreicht oder nicht erreicht worden sind. Die Reformziele wurden klarer formuliert.
- Die Dokumentation im Abschnitt „Problemstellung“ wurde ergänzt und es wurden zusätzliche Erläuterungen eingefügt.
- Zum Thema „Verhältnismäßigkeit“ wurde ein neuer Abschnitt aufgenommen.
- Alle Berechnungen und Schätzungen, die den Verwaltungsaufwand im Ausgangsszenario und in der bevorzugten Option betrafen, wurden vollständig überprüft und korrigiert. Das Verhältnis zwischen den Meldekosten und den durch die unterschiedliche Rechtslage bedingten Gesamtkosten wurde präzisiert (einschließlich Anhang 10).
- Die Auswirkungen auf Kleinst-, Klein- und Mittelunternehmen, insbesondere in Bezug auf den Datenschutzbeauftragten und die Datenschutz-Folgenabschätzung, wurden detaillierter beschrieben.

Die Folgenabschätzung und deren Kurzfassung werden zusammen mit den Vorschlägen veröffentlicht.

### **3. RECHTLICHE ASPEKTE**

#### **3.1. Rechtsgrundlage**

Dieser Vorschlag ist auf Artikel 16 AEUV, der neuen durch den Vertrag von Lissabon eingeführten Rechtsgrundlage für den Erlass von Datenschutzvorschriften, gestützt. Danach kann die Union den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten regeln, wenn die Verarbeitung im Rahmen der Ausübung von Tätigkeiten erfolgt, die in den Anwendungsbereich des Unionsrechts fallen. Auch Vorschriften für den freien Verkehr personenbezogener Daten – auch solcher, die von den Mitgliedstaaten oder von nicht-öffentlichen Stellen verarbeitet werden – können auf dieser Grundlage erlassen werden.

Zur Regelung des Schutzes personenbezogener Daten in der Union ist eine Verordnung als Rechtsinstrument am besten geeignet. Aufgrund ihrer unmittelbaren Anwendbarkeit nach Artikel 288 AEUV trägt sie zur Rechtsvereinheitlichung bei und erhöht die Rechtssicherheit durch die Einführung harmonisierter Kernbestimmungen und durch einen besseren Grundrechtsschutz. Auf diese Weise sorgt sie gleichzeitig für einen besser funktionierenden Binnenmarkt.

Die Bezugnahme auf Artikel 114 Absatz 1 AEUV ist für die Änderung der Richtlinie 2002/58/EG nur insoweit notwendig, als diese Richtlinie auch den Schutz der berechtigten Interessen von Teilnehmern vorsieht, bei denen es sich um juristische Personen handelt.

#### **3.2. Subsidiarität und Verhältnismäßigkeit**

Nach dem Subsidiaritätsprinzip (Artikel 5 Absatz 3 EUV) wird die Union nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind. Im Hinblick auf die beschriebene Problematik zeigt die Subsidiaritätsanalyse, dass aus folgenden Gründen Maßnahmen auf EU-Ebene notwendig sind:

- Das Recht auf Schutz personenbezogener Daten, das in Artikel 8 der Grundrechtecharta verankert ist, verlangt ein unionsweit einheitliches Datenschutzniveau. Ohne gemeinsame EU-Vorschriften bestünde die Gefahr, dass der Datenschutz in den Mitgliedstaaten nicht in gleichem Maße gewährleistet ist, was den grenzüberschreitenden Verkehr personenbezogener Daten zwischen Mitgliedstaaten mit unterschiedlichen Datenschutzerfordernissen behindern würde.
- Der Transfer personenbezogener Daten sowohl in andere EU-Staaten als auch in Drittstaaten nimmt rasant zu. Die praktischen Schwierigkeiten bei der Durchsetzung der Datenschutzvorschriften und die hierzu notwendige Zusammenarbeit zwischen den Mitgliedstaaten und ihren Behörden erfordern eine Organisation auf EU-Ebene, um die einheitliche Anwendung des Unionsrechts zu gewährleisten. Die EU ist auch die geeignete Ebene, um sicherzustellen, dass alle Betroffenen bei der Übermittlung personenbezogener Daten in Drittländer effektiv in gleichem Maße geschützt sind.
- Die Mitgliedstaaten können die derzeitigen Probleme – vor allem die durch die Uneinheitlichkeit der nationalen Vorschriften bedingten Probleme – nicht allein

überwinden. Es besteht daher ein besonderer Bedarf an einer harmonisierten, kohärenten Regelung, die einen reibungslosen Transfer personenbezogener Daten innerhalb der EU ermöglicht und gleichzeitig EU-weit allen Betroffenen einen wirksamen Datenschutz garantiert.

- Wegen Art und Umfang der Probleme, die nicht auf einen oder mehrere Mitgliedstaaten beschränkt sind, werden die vorgeschlagenen Legislativmaßnahmen der EU eine größere Wirkung entfalten als vergleichbare Maßnahmen auf Ebene der Mitgliedstaaten.

Nach dem Verhältnismäßigkeitsprinzip muss jedes Handeln zielgerichtet sein und darf nicht über das hinausgehen, was für die Erreichung der angestrebten Ziele notwendig ist. An diesem Grundsatz hat sich die Ausarbeitung dieses Vorschlags von der Feststellung und Analyse der möglichen Optionen bis hin zu seiner Formulierung orientiert.

### **3.3. Zusammenfassung der Grundrechtsaspekte**

Das Recht auf Schutz personenbezogener Daten ist in Artikel 8 der Grundrechtecharta, Artikel 16 AEUV und in Artikel 8 der EMRK verankert. Wie der Gerichtshof der EU betont hat,<sup>27</sup> kann das Recht auf Schutz der personenbezogenen Daten jedoch keine uneingeschränkte Geltung beanspruchen, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden.<sup>28</sup> Datenschutz und Achtung des Privat- und Familienlebens, das durch Artikel 7 der Charta geschützt ist, hängen eng zusammen. Dies geht aus Artikel 1 Absatz 1 der Richtlinie 95/46/EG hervor, wonach die Mitgliedstaaten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten.

Auch andere in der Charta verankerte Grundrechte können betroffen sein: z. B. die Freiheit der Meinungsäußerung (Artikel 11 der Charta), die unternehmerische Freiheit (Artikel 16), das Recht auf Eigentum, insbesondere der Schutz des geistigen Eigentums (Artikel 17 Absatz 2), das Verbot einer Diskriminierung unter anderem wegen der Rasse, der ethnischen Herkunft, der genetischen Merkmale, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, einer Behinderung oder der sexuellen Ausrichtung (Artikel 21), die Rechte des Kindes (Artikel 24), das Recht auf ein hohes Gesundheitsschutzniveau (Artikel 35), das Recht auf Zugang zu Dokumenten (Artikel 42) und das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren (Artikel 47).

### **3.4. Erläuterung des Vorschlags im Einzelnen**

#### *3.4.1. KAPITEL I – ALLGEMEINE BESTIMMUNGEN*

Artikel 1 bestimmt den Gegenstand der Verordnung und – wie Artikel 1 der Richtlinie 95/46/EG – ihre beiden Zielsetzungen.

---

<sup>27</sup> Gerichtshof der Europäischen Union, Urteil vom 9.11.2010, Verbundene Rechtssachen C-92/09 und C-93/09, Volker und Markus Schecke und Eifert, Slg. 2010, I-0000 (noch nicht veröffentlicht).

<sup>28</sup> Im Einklang mit Artikel 52 Absatz 1 der Charta kann die Ausübung der Datenschutzrechte eingeschränkt werden, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Rechte und Freiheiten achten, unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.



Artikel 2 bestimmt den sachlichen Anwendungsbereich der Verordnung.

Artikel 3 bestimmt den räumlichen Anwendungsbereich der Verordnung.

Artikel 4 enthält die Begriffsbestimmungen. Einige Definitionen stammen aus der Richtlinie 95/46/EG, andere wurden abgeändert, ergänzt oder neu eingeführt („Verletzung des Schutzes personenbezogener Daten“ auf der Grundlage von Artikel 2 Buchstabe h der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG<sup>29</sup> in der durch die Richtlinie 2009/136/EG<sup>30</sup> geänderten Fassung, „genetische Daten“, „biometrische Daten“, „Gesundheitsdaten“, „Hauptniederlassung“, „Vertreter“, „Unternehmen“, „Unternehmensgruppe“, „verbindliche unternehmensinterne Vorschriften“, „Kind“ im Sinne der UN-Kinderrechtskonvention<sup>31</sup> und „Aufsichtsbehörde“).

Bei der Definition des Begriffs „Einwilligung“ wurde das Kriterium „explizit“ eingefügt, um eine Verwechslung mit einer „ohne jeden Zweifel“ erteilten Einwilligung zu vermeiden und sicherzustellen, dass der betroffenen Person bewusst ist, dass sie eine Einwilligung erteilt hat und worin sie eingewilligt hat.

### 3.4.2. KAPITEL II – GRUNDSÄTZE

In Artikel 5 sind die Grundsätze für die Verarbeitung personenbezogener Daten niedergelegt, die denen in Artikel 6 der Richtlinie 95/46/EG entsprechen. Neu hinzugekommen ist unter anderem das Transparenzprinzip, der Grundsatz der Datenminimierung wurde klarer gefasst, und es wurde eine umfassende Verantwortung und Haftung des für die Datenverarbeitung Verantwortlichen eingeführt.

Artikel 6, der auf Artikel 7 der Richtlinie 95/46/EG gestützt ist, enthält die Kriterien für eine rechtmäßige Verarbeitung, die weiter konkretisiert werden in Bezug auf die Interessenabwägung und die Erfüllung rechtlicher Verpflichtungen und Aufgaben im öffentlichen Interesse.

Artikel 7 bestimmt, unter welchen Voraussetzung eine Einwilligung eine rechtswirksame Grundlage für eine rechtmäßige Verarbeitung darstellt.

Artikel 8 enthält weitere Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Kindern im Zusammenhang mit Diensten der Informationsgesellschaft, die Kindern direkt angeboten werden.

---

<sup>29</sup> 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).

<sup>30</sup> Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Text von Bedeutung für den EWR) (ABl. L 337 vom 18.12.2009, S. 11). 11.

<sup>31</sup> Die Kinderrechtskonvention wurde von der UN-Generalversammlung mit Resolution 44/25 vom 20.11.1989 angenommen und zur Unterzeichnung, Ratifizierung und zum Beitritt aufgelegt.

Artikel 9 enthält in Anlehnung an Artikel 8 der Richtlinie 95/46/EG das allgemeine Verbot für die Verarbeitung besonderer Kategorien personenbezogener Daten sowie die Ausnahmen von diesem Verbot.

Artikel 10 stellt klar, dass ein für die Verarbeitung Verantwortlicher allein zur Einhaltung einer Vorschrift dieser Verordnung keine zusätzlichen Informationen einholen muss, um die betroffene Person zu identifizieren.

### 3.4.3. KAPITEL III – RECHTE DER BETROFFENEN PERSON

#### 3.4.3.1. Abschnitt 1 – Transparenz und Modalitäten

Artikel 11 führt eine Verpflichtung zur Bereitstellung transparenter, leicht zugänglicher und verständlicher Informationen ein, die sich insbesondere an die Madrider EntschlieÙung zu Internationalen Standards zum Schutz der Privatsphäre<sup>32</sup> anlehnt.

Artikel 12 verpflichtet den für die Verarbeitung Verantwortlichen, Verfahren und Vorkehrungen für die Ausübung der Rechte der betroffenen Personen einschließlich Möglichkeiten für die Antragstellung auf elektronischem Weg vorzusehen, innerhalb einer bestimmten Frist auf den Antrag einer betroffenen Person zu reagieren und eine Ablehnung des Antrags zu begründen.

Artikel 13 erstreckt die auf der Grundlage von Artikel 12 Buchstabe c der Richtlinie 95/46/EG in Bezug auf die Empfänger vorgesehenen Rechte auf alle Empfänger, d. h. auch auf die gemeinsam für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter.

#### 3.4.3.2. Abschnitt 2 – Information und Auskunftsrecht

In Artikel 14 werden die Informationspflichten des für die Verarbeitung Verantwortlichen gegenüber der betroffenen Person weiter ausgeführt, die über die Artikel 10 und 11 der Richtlinie 95/46/EG hinaus über die Speicherfrist, das Beschwerderecht, die Datenübermittlung ins Ausland und die Quelle, aus der die Daten stammen, zu unterrichten ist. Die Ausnahmebestimmungen der Richtlinie 95/46/EG werden beibehalten, d. h. die Informationspflicht besteht nicht, wenn die Erfassung oder Weitergabe der Daten per Gesetz ausdrücklich vorgesehen ist. Beispiele hierfür sind Verfahren der Wettbewerbs-, Steuer- oder Zollbehörden oder von Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind.

Artikel 15, der auf Artikel 12 Buchstabe a der Richtlinie 95/46/EG gestützt ist, regelt das Recht der betroffenen Person auf Auskunft über ihre personenbezogenen Daten und darüber hinaus das Recht, über die Speicherfrist informiert zu werden, das Recht auf Berichtigung, das Recht auf Löschung sowie das Beschwerderecht.

#### 3.4.3.3. Abschnitt 3 – Berichtigung und Löschung

In Artikel 16 ist das Recht der betroffenen Person auf Berichtigung ihrer Daten in Anlehnung an Artikel 12 Buchstabe b der Richtlinie 95/46/EG festgeschrieben.

---

<sup>32</sup> EntschlieÙung der Internationalen Datenschutzkonferenz vom 5. November 2009. Vgl. auch Artikel 13 Absatz 3 des Vorschlags für eine Verordnung über ein Gemeinsames Europäisches Kaufrecht (KOM(2011) 635 endg.).

Artikel 17 garantiert dem Betroffenen das Recht, vergessen zu werden, sowie das Recht auf Löschung. Das in Artikel 12 b der Richtlinie 95/46/EG geregelte Recht auf Löschung wird weiter ausgeführt und präzisiert einschließlich der Bedingungen für das Recht auf Vergessenwerden. Hierzu zählt auch die Pflicht des für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten veröffentlicht hat, Dritte über den Antrag der betroffenen Person auf Löschung aller Verbindungen zu diesen personenbezogenen Daten oder auf Löschung von Kopien oder Replikationen dieser Daten zu informieren. Darüber hinaus wird ein Recht auf Beschränkung der Datenverarbeitung in bestimmten Fällen eingeführt. Der mehrdeutige Ausdruck „Sperrung“ wird dabei vermieden.

In Artikel 18 wird das Recht des Betroffenen auf Datenportabilität eingeführt, d. h. das Recht, seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche ihn daran hindern kann. Als Voraussetzung für die Ausübung dieses Rechts und um den Zugang natürlicher Personen zu ihren Daten weiter zu verbessern, ist vorgesehen, dass der für die Verarbeitung Verantwortliche diese Daten in einem strukturierten, gängigen elektronischen Format zur Verfügung stellen muss.

#### 3.4.3.4. Abschnitt 4 – Widerspruchsrecht und Profiling

Artikel 19 gewährleistet das Widerspruchsrecht der betroffenen Person. Der Artikel ist auf Artikel 14 der Richtlinie 95/46/EG gestützt mit einigen Änderungen unter anderem hinsichtlich der Beweislastregelung und deren Anwendung im Fall der Direktwerbung.

In Artikel 20 geht es um das Recht des Betroffenen, keiner Maßnahme unterworfen zu werden, die auf Profiling basiert. Grundlage dieser Bestimmung ist – mit einigen Änderungen und zusätzlichen Garantien – Artikel 15 Absatz 1 der Richtlinie 95/46/EG über automatisierte Einzelentscheidungen. Berücksichtigt wurde auch die Empfehlung des Europarats zum Profiling<sup>33</sup>.

#### 3.4.3.5. Abschnitt 5 – Beschränkungen

Artikel 21 präzisiert das Recht der EU und ihrer Mitgliedstaaten, Einschränkungen der Grundsätze in Artikel 5 sowie Beschränkungen von Datenschutzrechten im Sinne der Artikel 11 bis 20 und Artikel 32 beizubehalten oder einzuführen. Diese Bestimmung ist auf Artikel 13 der Richtlinie 95/46/EG sowie auf die Anforderungen aus der Grundrechtecharta und der Europäischen Menschenrechtskonvention im Sinne der Auslegung des Gerichtshofs der EU und des Europäischen Menschenrechtsgerichtshofs gestützt.

### 3.4.4. *KAPITEL IV - FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER*

#### 3.4.4.1. Abschnitt 1 – Allgemeine Pflichten

Artikel 22, in den die Diskussion über den Grundsatz der Rechenschaftspflicht eingeflossen ist, enthält eine detaillierte Beschreibung der dem für die Verarbeitung Verantwortlichen obliegenden Verpflichtung, für die Einhaltung der Verordnung zu sorgen und dies

---

<sup>33</sup> CM/Rec (2010)13.

nachzuweisen, unter anderem durch die Einführung hierzu geeigneter interner Maßnahmen und Verfahren.

Artikel 23 regelt die Pflichten, die dem für die Verarbeitung Verantwortlichen aus dem Grundsatz des Datenschutzes durch Technik und dem Gebot datenschutzfreundlicher Voreinstellungen erwachsen.

Artikel 24 präzisiert die Verantwortung der gemeinsam für die Verarbeitung Verantwortlichen in Bezug auf ihr Verhältnis untereinander sowie gegenüber der betroffenen Person.

Artikel 25 schreibt vor, dass jeder für die Verarbeitung Verantwortliche, der keine Niederlassung in der Europäischen Union besitzt und auf dessen Verarbeitungstätigkeit die Verordnung Anwendung findet, in bestimmten Fällen einen Vertreter in der Europäischen Union benennen muss.

Artikel 26, der zum Teil auf Artikel 17 Absatz 2 der Richtlinie 95/46/EG gestützt ist, präzisiert Stellung und Pflichten des Auftragsverarbeiters und bestimmt unter anderem, dass ein Auftragsverarbeiter, der über die Anweisungen des für die Verarbeitung Verantwortlichen hinaus Daten verarbeitet, gemeinsam mit diesem für die Verarbeitung verantwortlich ist.

Artikel 27, der die Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters regelt, ist auf Artikel 16 der Richtlinie 95/46/EG gestützt.

Artikel 28 führt anstelle der allgemeinen Meldepflicht gegenüber der Aufsichtsbehörde gemäß Artikel 18 Absatz 1 und Artikel 19 der Richtlinie 95/46/EG für den für die Verarbeitung Verantwortlichen und für den Auftragsverarbeiter die Pflicht ein, die unter ihrer Verantwortung vollzogenen Verarbeitungsvorgänge zu dokumentieren.

Artikel 29 regelt die Pflicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters zur Zusammenarbeit mit der Aufsichtsbehörde.

#### 3.4.4.2. Abschnitt 2 – Datensicherheit

Artikel 30 verpflichtet den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, geeignete Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung zu ergreifen. Ausgehend von Artikel 17 Absatz 1 der Richtlinie 95/46/EG wird diese Pflicht jetzt auf Auftragsverarbeiter ausgedehnt ungeachtet ihres Vertragsverhältnisses mit dem für die Verarbeitung Verantwortlichen.

Artikel 31 und 32 führen ausgehend von Artikel 4 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG eine entsprechende Meldepflicht für Verstöße gegen den Schutz personenbezogener Daten ein.

#### 3.4.4.3. Abschnitt 3 – Datenschutz-Folgenabschätzung und vorherige Genehmigung

Artikel 33 verpflichtet den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, vor einer risikobehafteten Datenverarbeitung eine datenschutzspezifische Folgenabschätzung durchzuführen.

Artikel 34 betrifft Fälle, in denen vor der Verarbeitung der Daten die Aufsichtsbehörde zurate zu ziehen und deren Genehmigung einzuholen ist. Diese Bestimmung fußt auf dem Prinzip der Vorabkontrolle gemäß Artikel 20 der Richtlinie 95/46/EG.

#### 3.4.4.4. Abschnitt 4 – Datenschutzbeauftragter

Artikel 35 schreibt die Einsetzung eines Datenschutzbeauftragten für den öffentlichen Sektor sowie im privaten Sektor für Großunternehmen und in Fällen vor, in denen die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragverarbeiters aus Verarbeitungsvorgängen besteht, die einer regelmäßigen, systematischen Überwachung bedürfen. Gestützt ist diese Bestimmung auf Artikel 18 Absatz 2 der Richtlinie 95/46/EG, der den Mitgliedstaaten die Möglichkeit bietet, als Ersatz für die allgemeine Meldepflicht die Bestellung eines Datenschutzbeauftragten vorzusehen.

Artikel 36 regelt die Stellung des Datenschutzbeauftragten.

Artikel 37 regelt die Kernaufgaben des Datenschutzbeauftragten.

#### 3.4.4.5. Abschnitt 5 – Verhaltensregeln und Zertifizierung

Artikel 38, der auf Artikel 27 Absatz 1 der Richtlinie 95/46/EG gestützt ist, regelt den Inhalt von Verhaltensregeln und Verfahren und ermächtigt die Kommission, über die allgemeine Gültigkeit der Verhaltensregeln zu entscheiden.

Artikel 39 sieht die Möglichkeit zur Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen vor.

### 3.4.5. *KAPITEL V – ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN*

Artikel 40 bestimmt als allgemeinen Grundsatz, dass personenbezogene Daten nur dann in Drittländer oder an internationale Organisationen übermittelt oder weitergegeben werden dürfen, wenn die in diesem Kapitel festgelegten Bedingungen erfüllt sind.

Artikel 41, der auf Artikel 25 der Richtlinie 95/46/EG gestützt ist, enthält die Kriterien, Bedingungen und Verfahren für den Erlass eines Angemessenheitsbeschlusses der Kommission. Danach beurteilt die Kommission die Angemessenheit des Schutzniveaus unter anderem in Bezug auf die Rechtsstaatlichkeit, den gerichtlichen Rechtsschutz und die Existenz einer unabhängigen Aufsicht. Bestätigt wird in diesem Artikel jetzt ausdrücklich die Möglichkeit für die Kommission, das Schutzniveau zu beurteilen, das in einem Gebiet oder einem Verarbeitungssektor eines Drittlands geboten wird.

Nach Artikel 42 sind für die Übermittlung von Daten in Drittländer in Fällen, in denen die Kommission keinen Angemessenheitsbeschluss erlassen hat, ausreichende Garantien erforderlich, insbesondere in Form von Standard-Datenschutzklauseln, verbindlichen unternehmensinternen Vorschriften und Vertragsklauseln. Die Möglichkeit, auf die Standard-Datenschutzklauseln der Kommission zurückzugreifen, basiert auf Artikel 26 Absatz 4 der Richtlinie 95/46/EG. Neu ist, dass solche Standard-Datenschutzklauseln jetzt auch von einer Aufsichtsbehörde festgelegt und von der Kommission als allgemein gültig erklärt werden können. Als Garantie ausdrücklich genannt werden zudem verbindliche unternehmensinterne Datenschutzregelungen. Die Möglichkeit, auf Vertragsklauseln zurückzugreifen, lässt dem für

die Verarbeitung Verantwortlichen bzw. dem Auftragsverarbeiter einen gewissen Spielraum, muss aber von der Aufsichtsbehörde zuvor genehmigt werden.

In Artikel 43 werden die Bedingungen für den Datentransfer auf der Grundlage verbindlicher unternehmensinterner Datenschutzregelungen weiter ausgeführt. Die Bestimmung ist auf die derzeitigen Praktiken und Anforderungen der Aufsichtsbehörden gestützt.

In Artikel 44, der Artikel 26 der Richtlinie 95/46/EG folgt, sind die Ausnahmen für den Datentransfer in ein Drittland festgeschrieben. Zulässig ist der Datentransfer danach, wenn er zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel für den internationalen Datenaustausch zwischen Wettbewerbsbehörden, Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit oder für die Fischerei zuständig sind. Der Datentransfer kann darüber hinaus unter bestimmten, eng umrissenen Umständen mit einem berechtigten Interesse des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters gerechtfertigt werden. Zuvor müssen die Umstände des Übermittlungsvorgangs allerdings geprüft und dokumentiert worden sein.

In Artikel 45 ist ausdrücklich vorgesehen, dass die Kommission und die Aufsichtsbehörden von Drittländern, insbesondere der Länder, deren Datenschutzniveau als angemessen angesehen wird, ein Verfahren für die internationale Zusammenarbeit zum Schutz personenbezogener Daten unter Berücksichtigung der Empfehlung der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) vom 12. Juni 2007 zur grenzübergreifenden Zusammenarbeit bei der Durchsetzung des Datenschutzrechts (cross-border co-operation in the enforcement of laws protecting privacy) entwickeln.

### 3.4.6. KAPITEL VI – UNABHÄNGIGKEIT DER AUFSICHTSBEHÖRDEN

#### 3.4.6.1. Abschnitt 1 – Unabhängigkeit

Artikel 46 verpflichtet die Mitgliedstaaten in Anlehnung an Artikel 28 Absatz 1 der Richtlinie 95/46/EG, Aufsichtsbehörden einzurichten, zu deren Aufgaben auch die Zusammenarbeit untereinander sowie mit der Kommission gehört.

Artikel 47 präzisiert die Kriterien für die Unabhängigkeit der Aufsichtsbehörden im Einklang mit der Rechtsprechung des Gerichtshofs der Europäischen Union<sup>34</sup> und in Anlehnung an Artikel 44 der Verordnung (EG) Nr. 45/2001<sup>35</sup>.

Artikel 48 regelt in Anlehnung an die einschlägige Rechtsprechung<sup>36</sup> und Artikel 42 Absätze 2 bis 6 der Verordnung (EG) Nr. 45/2001 die allgemeinen Anforderungen an die Mitglieder der Aufsichtsbehörde.

Artikel 49 bestimmt, welche Aspekte in Bezug auf die Aufsichtsbehörden von den Mitgliedstaaten gesetzlich zu regeln sind.

---

<sup>34</sup> Gerichtshof der EU, Urteil vom 9.3.2010, Rs. C-518/07, *Kommission/Deutschland*, Slg. 2010, I-1885.

<sup>35</sup> 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).

<sup>36</sup> Siehe Fußnote 34.

Artikel 50 regelt in Anlehnung an Artikel 28 Absatz 7 der Richtlinie 95/46/EG das Berufsgeheimnis der Mitglieder und Bediensteten der Aufsichtsbehörde.

#### 3.4.6.2. Abschnitt 2 – Aufgaben und Befugnisse

Artikel 51 regelt die örtliche Zuständigkeit der Aufsichtsbehörden. Die allgemeine Zuständigkeit im Hoheitsgebiet des eigenen Mitgliedstaats nach dem Vorbild des Artikels 28 Absatz 6 der Richtlinie 95/46/EG wird ergänzt durch die Zuständigkeit als federführende Behörde, wenn ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter Niederlassungen in mehreren Mitgliedstaaten hat. Auf diese Weise soll eine einheitliche Rechtsanwendung gewährleistet werden (Prinzip einer zentralen Anlaufstelle für den Datenschutz). Gerichte unterliegen dem materiellen Datenschutzrecht, sind aber von der Überwachung durch die Aufsichtsbehörde ausgenommen, wenn sie in ihrer Eigenschaft als Rechtsprechungsorgan tätig sind.

In Artikel 52 sind die Aufgaben der Aufsichtsbehörde aufgeführt, darunter die Untersuchung und Verhandlung von Beschwerden sowie die Aufklärung der Öffentlichkeit über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Artikel 53 regelt – zum Teil gestützt auf Artikel 28 Absatz 3 der Richtlinie 95/46/EG und Artikel 47 der Verordnung (EG) Nr. 45/2001 – die Befugnisse der Aufsichtsbehörde mit einigen neuen Aspekten, darunter die Befugnis zur Verhängung verwaltungsrechtlicher Sanktionen.

Artikel 54 verpflichtet die Aufsichtsbehörden nach dem Vorbild des Artikels 28 Absatz 5 der Richtlinie 95/46/EG zur jährlichen Berichterstattung über ihre Tätigkeit.

### 3.4.7. *KAPITEL VII – ZUSAMMENARBEIT UND KOHÄRENZ*

#### 3.4.7.1. Abschnitt 1 – Zusammenarbeit

Artikel 55, der auf Artikel 28 Absatz 6 Unterabsatz 2 der Richtlinie 95/46/EG gestützt ist, verpflichtet die Aufsichtsbehörden ausdrücklich, einander Amtshilfe zu leisten, und regelt die Folgen, die sich aus der Nichtbeachtung des Ersuchens einer anderen Aufsichtsbehörde ergeben.

Artikel 56 führt in Anlehnung an Artikel 17 des Ratsbeschlusses 2008/615/JI<sup>37</sup> Vorschriften für gemeinsame Maßnahmen sowie das Recht der Aufsichtsbehörden auf Teilnahme an solchen Maßnahmen ein.

#### 3.4.7.2. Abschnitt 2 – Kohärenz

Artikel 57 führt ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) in Bezug auf Verarbeitungsvorgänge ein, die Personen in mehreren Mitgliedstaaten betreffen können.

---

<sup>37</sup> 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).

Artikel 58 legt die Modalitäten für Stellungnahmen des Europäischen Datenschutzausschusses fest.

Artikel 59 betrifft die Stellungnahmen der Kommission zu Angelegenheiten, die im Rahmen des Kohärenzverfahrens behandelt werden, wobei diese Stellungnahmen die Stellungnahmen des Europäischen Datenschutzausschusses entweder bestätigen oder davon abweichen können, sowie die geplante Maßnahme der Aufsichtsbehörde. Wurde die Angelegenheit vom Europäischen Datenschutzausschuss nach Artikel 58 Absatz 3 aufgeworfen, ist zu erwarten, dass die Kommission von ihrem Ermessen Gebrauch macht und gegebenenfalls eine Stellungnahme abgibt.

Artikel 60 regelt die Aussetzung der Annahme der geplanten Maßnahme auf Beschluss der Kommission, soweit dies für die korrekte Anwendung der Verordnung erforderlich ist.

Artikel 61 sieht die Möglichkeit vor, in einem Dringlichkeitsverfahren einstweilige Maßnahmen zu erlassen.

In Artikel 62 sind die Modalitäten festgelegt, nach denen die Kommission Durchführungsrechtsakte im Rahmen des Kohärenzverfahrens erlassen kann.

Artikel 63 schreibt vor, dass Maßnahmen einer Aufsichtsbehörde in allen betroffenen Mitgliedstaaten zu vollstrecken sind. Diese Maßnahmen sind allerdings nur bei Anwendung des Kohärenzverfahrens rechtsgültig und vollstreckbar.

#### 3.4.7.3. Abschnitt 3 – Der Europäische Datenschutzausschuss

Artikel 64 sieht die Einsetzung eines Europäischen Datenschutzausschusses vor, dem die Leiter der Aufsichtsbehörden der Mitgliedstaaten und der Europäische Datenschutzbeauftragte angehören. Der Europäische Datenschutzausschuss tritt an die Stelle der durch Artikel 29 der Richtlinie 95/46/EG eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten. Die Kommission ist nicht Mitglied des Europäischen Datenschutzausschusses, hat aber ein Recht auf Mitwirkung an seinen Arbeiten und auf Teilnahme an den Sitzungen.

Artikel 65 schreibt die Unabhängigkeit des Europäischen Datenschutzausschusses fest.

Artikel 66 listet in Anlehnung an Artikel 30 Absatz 1 der Richtlinie 95/46/EG die Aufgaben des Europäischen Datenschutzausschusses auf, die den erweiterten Tätigkeitsbereich dieses Gremiums innerhalb der Union und darüber hinaus widerspiegeln. Um in dringenden Fällen rasch reagieren zu können, erhält die Kommission die Möglichkeit, dem Datenschutzausschuss eine Frist für seine Stellungnahme zu setzen.

Artikel 67 verpflichtet den Europäischen Datenschutzausschuss nach dem Vorbild des Artikels 30 Absatz 6 der Richtlinie 95/46/EG zur jährlichen Berichterstattung über seine Tätigkeit.

Artikel 68 regelt das Beschlussfassungsverfahren des Europäischen Datenschutzausschusses und schreibt vor, dass sich der Ausschuss eine Geschäftsordnung gibt, in der er auch seine Arbeitsweise festlegt.



Artikel 69 enthält Bestimmungen zum Vorsitz des Europäischen Datenschutzausschusses und zu dessen Stellvertretung.

Artikel 70 präzisiert die Aufgaben des Vorsitzenden.

Artikel 71 bestimmt, dass das Sekretariat des Europäischen Datenschutzausschusses beim Europäischen Datenschutzbeauftragten eingerichtet wird, und legt die Aufgaben des Sekretariats fest.

Artikel 72 regelt die Vertraulichkeit der Arbeiten des Europäischen Datenschutzausschusses.

#### 3.4.8. *KAPITEL VIII – RECHTSBEHELFE, HAFTUNG UND SANKTIONEN*

In Artikel 73 ist das Recht des Betroffenen auf Beschwerde bei einer Aufsichtsbehörde in Anlehnung an Artikel 28 Absatz 4 der Richtlinie 95/46/EG festgeschrieben. Darüber hinaus können auch bestimmte Einrichtungen, Organisationen oder Verbände im Namen der betroffenen Person Beschwerde führen. Im Fall einer Verletzung des Schutzes personenbezogener Daten ist hierzu keine Beschwerde der betroffenen Person erforderlich.

Artikel 74 schreibt das Recht auf einen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde fest. Er ist auf die allgemeine Regelung in Artikel 28 Absatz 3 der Richtlinie 95/46/EG gestützt. In Artikel 74 ist ausdrücklich ein gerichtlicher Rechtsbehelf vorgesehen, um eine Aufsichtsbehörde zu zwingen, im Fall einer Beschwerde tätig zu werden. Zuständig sind in diesem Fall die Gerichte des Mitgliedstaats, in dem die Aufsichtsbehörde ihren Sitz hat. Zudem wird der Aufsichtsbehörde des Mitgliedstaats, in dem die betroffene Person ansässig ist, die Möglichkeit eingeräumt, im Namen der betroffenen Person Klage im Sitzmitgliedstaat der zuständigen Aufsichtsbehörde zu erheben.

Artikel 75 betrifft das Recht auf einen gerichtlichen Rechtsbehelf gegen einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter in Anlehnung an Artikel 22 der Richtlinie 95/46/EG, wobei der Rechtsweg wahlweise in dem Mitgliedstaat eröffnet ist, in dem der Beklagte niedergelassen bzw. die betroffene Person ansässig ist. Ist dieselbe Angelegenheit Gegenstand des Kohärenzverfahrens, kann das Gericht sein Verfahren aussetzen, es sei denn, es ist Eile geboten.

Artikel 76 legt gemeinsame Vorschriften für Gerichtsverfahren fest einschließlich des Rechts von Datenschutzeinrichtungen, -organisationen oder -verbänden, betroffene Personen vor Gericht zu vertreten, des Klagerechts der Aufsichtsbehörden, der Unterrichtung der Gerichte über Parallelverfahren in einem anderen Mitgliedstaat und der Möglichkeit für die Gerichte, bei einem solchen Parallelverfahren das eigene Verfahren auszusetzen.<sup>38</sup> Die Mitgliedstaaten müssen ihrerseits dafür sorgen, dass die Gerichtsverfahren zügig vonstatten gehen.<sup>39</sup>

---

<sup>38</sup> In Anlehnung an Artikel 5 Absatz 1 des Rahmenbeschlusses 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren (ABl. L 328 vom 15.12.2009, S. 42) und Artikel 13 Absatz 1 der Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln (ABl. L 1 vom 4.1.2003, S. 1).

<sup>39</sup> In Anlehnung an Artikel 18 Absatz 1 der 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. 178 vom 17.7.2000, S. 1).

Artikel 77 regelt die Haftung und das Recht auf Schadenersatz. Das Recht auf Schadenersatz, das auf Artikel 23 der Richtlinie 95/46/EG gestützt ist, wird auf Schäden erweitert, die der Auftragsverarbeiter verursacht hat. Näher geregelt wird auch die Haftung in Fällen, in denen an der Datenverarbeitung mehrere Verantwortliche und Auftragsverarbeiter beteiligt sind.

Artikel 78 verpflichtet die Mitgliedstaaten, Vorschriften für Sanktionen einzuführen, Verstöße gegen die Verordnung zu ahnden und dafür zu sorgen, dass diese Vorschriften angewandt werden.

Nach Artikel 79 ist jede Aufsichtsbehörde verpflichtet, die dort aufgelisteten verwaltungsrechtlichen Vergehen unter Beachtung der Umstände des Einzelfalls mit einer Geldbuße bis in Höhe der angegebenen Höchstbeträge zu ahnden.

#### *3.4.9. KAPITEL IX – VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN*

Artikel 81 verpflichtet die Mitgliedstaaten, Freistellungen und Ausnahmen von bestimmten Vorschriften der Verordnung einzuführen, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf freie Meinungsäußerung in Einklang zu bringen. Dieser Artikel ist auf Artikel 9 der Richtlinie 95/46/EG im Sinne der Auslegung des Gerichtshofs der Europäischen Union gestützt.<sup>40</sup>

Artikel 81 verpflichtet die Mitgliedstaaten, über die Verarbeitungsbedingungen für bestimmte Datenkategorien hinaus besondere Garantien für die Verarbeitung zu Gesundheitszwecken vorzusehen.

Artikel 82 bietet den Mitgliedstaaten die Möglichkeit, die Verarbeitung personenbezogener Daten im Beschäftigungskontext gesetzlich zu regeln.

Artikel 83 enthält besondere Vorschriften für die Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken sowie zum Zwecke der wissenschaftlichen Forschung.

Artikel 84 gestattet den Mitgliedstaaten in den Fällen, in denen der für die Verarbeitung Verantwortliche der Geheimhaltung unterliegt, den Zugang der Aufsichtsbehörden zu personenbezogenen Daten und zu Räumlichkeiten gesondert zu regeln.

Artikel 85 gestattet den Kirchen und religiösen Vereinigungen oder Gemeinschaften, die über umfassende Datenschutzregeln verfügen, mit Blick auf Artikel 17 AEUV diese Regeln weiter anzuwenden, sofern sie mit der Verordnung in Einklang gebracht werden.

#### *3.4.10. KAPITEL X – DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE*

Artikel 86 enthält die Standardbestimmung für die Übertragung der Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 290 AEUV. Der Gesetzgeber kann der Kommission danach die Befugnis übertragen, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung

---

<sup>40</sup> Vgl. hierzu u. a. Gerichtshof der EU, Urteil vom 16. Dezember 2008, Rs. C-73/07, *Satakunnan Markkinapörssi und Satamedia*, Slg. 2008, I-9831.

zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften eines Gesetzgebungsakts zu erlassen („quasi-legislative Rechtsakte“).

Artikel 87 regelt das Ausschussverfahren für die Übertragung von Durchführungsbefugnissen auf die Kommission in Fällen, in denen es nach Artikel 291 AEUV einheitlicher Bedingungen für die Durchführung der verbindlichen Rechtsakte der Union bedarf. Es gilt das Prüfverfahren.

#### *3.4.11. KAPITEL XI – SCHLUSSBESTIMMUNGEN*

Die Richtlinie 95/46/EG wird gemäß Artikel 88 aufgehoben.

Artikel 89 regelt das Verhältnis zur Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG und enthält Änderungsvorschriften für diese Richtlinie.

Artikel 90 verpflichtet die Kommission zur Bewertung der Verordnung und zur Vorlage entsprechender Berichte.

Artikel 91 bestimmt den Zeitpunkt des Inkrafttretens der Verordnung und sieht für den Beginn ihrer Anwendbarkeit eine zweijährige Übergangsphase vor.

#### **4. AUSWIRKUNGEN AUF DEN HAUSHALT**

Wie aus dem Finanzbogen zu diesem Vorschlag hervorgeht, ergeben sich die Auswirkungen auf den Haushalt aus den Aufgaben, die dem Europäischen Datenschutzbeauftragten übertragen werden. Dies erfordert eine Anpassung von Rubrik 5 der Finanziellen Vorausschau.

Der Vorschlag hat keine Auswirkungen auf die operativen Ausgaben.

Der Finanzbogen zu diesem Verordnungsvorschlag gibt Aufschluss über die budgetären Auswirkungen nicht nur der Verordnung, sondern auch der Richtlinie über den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit.

Vorschlag für

**VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

**zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (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 Absatz 2 und Artikel 114 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses<sup>41</sup>,

nach Anhörung des Europäischen Datenschutzbeauftragten<sup>42</sup>,

gemäß dem ordentlichen Gesetzgebungsverfahren,

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 sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Die Verarbeitung personenbezogener Daten steht im Dienste des Menschen; die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ungeachtet der Staatsangehörigkeit oder des gewöhnlichen Aufenthaltsorts der natürlichen Personen deren Grundrechte und Grundfreiheiten und insbesondere deren Recht auf Schutz personenbezogener Daten gewahrt bleiben. Die Datenverarbeitung sollte zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und

---

<sup>41</sup> ABl. C , S.

<sup>42</sup> ABl. C , S.

zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen der Menschen beitragen.

- (3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr<sup>43</sup> ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.
- (4) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarktes hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs geführt. Der unionsweite Datenaustausch zwischen wirtschaftlichen und sozialen Akteuren, staatlichen Stellen und Privatpersonen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten zur Zusammenarbeit und zum Austausch personenbezogener Daten, um ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen zu können.
- (5) Der rasche technologische Fortschritt und die Globalisierung stellen den Datenschutz vor neue Herausforderungen. Das Ausmaß, in dem Daten ausgetauscht und erhoben werden, ist dramatisch gestiegen. Die Technik macht es möglich, dass Privatwirtschaft und Staat zur Ausübung ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zugreifen können. Zunehmend werden auch private Informationen ins weltweite Netz gestellt und damit öffentlich zugänglich gemacht. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert, weshalb der Datenverkehr innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtert werden muss, wobei gleichzeitig ein hohes Maß an Datenschutz zu gewährleisten ist.
- (6) Diese Entwicklungen erfordern einen soliden, kohärenteren und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, um eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Jede Person sollte die Kontrolle über ihre eigenen Daten besitzen, und private Nutzer, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.
- (7) Die Ziele und Grundsätze der Richtlinie 95/46/EG besitzen nach wie vor Gültigkeit, doch hat die Richtlinie eine unterschiedliche Handhabung des Datenschutzes in der Union, Rechtsunsicherheit sowie die weit verbreitete öffentliche Meinung, dass speziell im Internet der Datenschutz nicht immer gewährleistet ist, nicht verhindern können. Unterschiede beim Schutz der Rechte und Grundfreiheiten von Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, kann den freien Verkehr solcher Daten in der gesamten Union behindern. Diese Unterschiede im Schutzniveau können 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

---

<sup>43</sup> ABl. L 281 vom 23.11.1995, S. 31.

sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.

- (8) Um ein hohes Maß an Datenschutz für den Einzelnen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten zu beseitigen, sollte der Schutz der Rechte und Freiheiten von 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 kohärent und einheitlich angewandt werden.
- (9) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine Stärkung und Präzisierung der Rechte der betroffenen Personen sowie eine Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, aber ebenso gleiche Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.
- (10) Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union ermächtigt das Europäische Parlament und den Rat, Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten festzulegen.
- (11) Damit jeder in der Union das gleiche Maß an Datenschutz genießt und Unterschiede, die den freien Datenverkehr im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die überall in der Union für Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtsicherheit und Transparenz schafft, den Einzelnen mit denselben durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter vorsieht und eine einheitliche Kontrolle der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten sowie gleiche Sanktionen und eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Um der besonderen Situation von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine Reihe von abweichenden Regelungen. 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 kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs des Kleinstunternehmens sowie kleiner und mittlerer Unternehmen sollte die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 maßgebend sein.
- (12) Der durch diese Verordnung gewährte Schutz betrifft die Verarbeitung personenbezogener Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnorts. Im Falle juristischer Personen und insbesondere von als juristische Person gegründeten Unternehmen, deren Daten, zum Beispiel deren Name, Rechtsform oder Kontaktdaten, verarbeitet werden, sollte eine Berufung auf diese Verordnung nicht möglich sein. Dies sollte auch dann gelten, wenn der Name der juristischen Person die Namen einer oder mehrerer natürlichen Personen enthält.
- (13) Der Schutz natürlicher Personen sollte technologieneutral sein und nicht von den verwendeten Verfahren abhängen, da andernfalls das Risiko einer Umgehung der

Vorschriften groß wäre. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, die in einem Ablagesystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten vom Anwendungsbereich der Verordnung ausgenommen werden.

- (14) Die Verordnung behandelt weder Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Datenverkehrs im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, noch die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union, für die die Verordnung (EG) Nr. 45/2001<sup>44</sup> maßgeblich ist, noch die von den Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchgeführte Verarbeitung personenbezogener Daten.
- (15) Die Verordnung sollte nicht für die von einer natürlichen Person vorgenommene Verarbeitung von personenbezogenen Daten rein persönlicher oder familiärer Natur zu nichtgewerblichen Zwecken und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit gelten, wie zum Beispiel das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen. Ebenfalls nicht ausgenommen werden sollten für die Verarbeitung Verantwortliche oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.
- (16) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden dienen, sowie der freie Verkehr solcher Daten sind in einem eigenen EU-Rechtsinstrument 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 zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung von Straftaten oder der Vollstreckung von Strafurteilen verwendet werden, dem spezifischeren EU-Instrument (Richtlinie XX/YYYY) unterliegen.
- (17) Die vorliegende Verordnung sollte die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste nicht berühren.
- (18) Diese Verordnung ermöglicht es, dass bei der Anwendung ihrer Vorschriften der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten berücksichtigt wird.
- (19) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung 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

---

<sup>44</sup> ABl. L 8 vom 12.1.2001, S. 1.

voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

- (20) Um sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach dieser Verordnung ein Anrecht haben, sollte die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen Produkte und Dienstleistungen anzubieten oder das Verhalten dieser Personen zu beobachten.
- (21) Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten mit Hilfe von Datenverarbeitungstechniken nachvollzogen werden, durch die einer Person ein Profil zugeordnet wird, das die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.
- (22) Ist nach internationalem Recht das innerstaatliche Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, sollte die Verordnung auch auf einen nicht in der EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.
- (23) Die Schutzprinzipien sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Um festzustellen, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden. Die Grundsätze des Datenschutzes sollten nicht für Daten gelten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.
- (24) Bei der Inanspruchnahme von Online-Diensten werden dem Nutzer unter Umständen Online-Kennungen wie IP-Adressen oder Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, zugeordnet. Dies kann Spuren hinterlassen, die zusammen mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der betroffenen Personen zu erstellen und sie zu identifizieren. Hieraus folgt, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente als solche nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind.
- (25) Die Einwilligung sollte explizit mittels einer geeigneten Methode erfolgen, die eine ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer eindeutigen Handlung ermöglicht, die sicherstellt, dass der betreffenden Person bewusst ist, dass sie ihre Einwilligung in die Verarbeitung personenbezogener Daten gibt, etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite und durch jede sonstige Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext klar und deutlich ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Eine stillschweigende Einwilligung ohne Zutun der betroffenen Person stellt daher keine Einwilligung dar.



Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommene Verarbeitungsvorgänge beziehen. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, in dessen Bereitstellung eingewilligt wird, erfolgen.

- (26) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten gezählt werden, die sich auf den Gesundheitszustand eines von der Verarbeitung Betroffenen beziehen, außerdem Informationen über die Vormerkung der betreffenden Person zur Erbringung medizinischer Leistungen, Angaben über Zahlungen oder die Berechtigung zum Empfang medizinischer Dienstleistungen, Nummern, Symbole oder Kennzeichen, die einer bestimmten Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, jede Art von Informationen über die betreffende Person, die im Rahmen der Erbringung von medizinischen Dienstleistungen erhoben wurden, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, darunter biologischer Proben, abgeleitet wurden, die Identifizierung einer Person als Erbringer einer Gesundheitsleistung für die betroffene Person 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, gleich, ob sie von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder einem In-Vitro-Diagnose-Test stammen.
- (27) Zur Bestimmung der Hauptniederlassung eines für die Verarbeitung 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, Bedingungen 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 begründet an sich noch keine Hauptniederlassung und ist daher kein ausschlaggebender Faktor für das Bestehen einer solchen Niederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem sich seine Hauptverwaltung in der Union befindet.
- (28) 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 von Eigentümerschaft, finanzieller Beteiligung oder sonstiger Bestimmungen, die die Tätigkeit des Unternehmens regeln, oder der Befugnis, Datenschutzvorschriften einzuführen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann.
- (29) Die personenbezogenen Daten von Kindern müssen besonderen Schutz genießen, da Kinder sich der Risiken, Folgen, Vorsichtsmaßnahmen und ihrer Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften. Bei der Definition, wann eine Person als Kind gilt, sollte die Definition in der UN-Konvention über die Rechte des Kindes zugrunde gelegt werden.

- (30) Jede Verarbeitung personenbezogener Daten sollte gegenüber den betroffenen Personen nach Recht und Gesetz sowie nach Treu und Glauben und in transparenter Form erfolgen. Insbesondere sollten die besonderen Zwecke, zu denen die Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Datenerfassung feststehen. Die erfassten Daten sollten dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Minimum beschränkt sein; dies heißt vor allem, dass nicht unverhältnismäßig viele Daten erfasst werden und die Speicherfrist auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht durch andere Mittel erreicht werden kann. Es sollten alle vertretbaren Schritte unternommen werden, damit unzutreffende oder unvollständige personenbezogene Daten gelöscht oder berichtigt werden. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für deren Löschung oder regelmäßige Überprüfung vorsehen.
- (31) 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.
- (32) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte die Beweislast, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat, bei dem für die Verarbeitung Verantwortlichen liegen. Vor allem bei Abgabe einer schriftlichen Erklärung in anderem Zusammenhang sollten Vorkehrungen getroffen werden, die sicherstellen, dass die betroffene Person weiß, dass und wozu sie ihre Einwilligung erteilt.
- (33) Um sicherzugehen, dass die Einwilligung ohne Zwang erfolgt, sollte klargestellt werden, dass die Einwilligung keine rechtswirksame Grundlage für die Verarbeitung liefert, wenn die betreffende Person keine echte Wahlfreiheit hat und somit nicht in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden.
- (34) Die Einwilligung liefert keine rechtliche Handhabe für die Verarbeitung personenbezogener Daten, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Dies ist vor allem dann der Fall, wenn sich die betroffene Person in einem Abhängigkeitsverhältnis von dem für die Verarbeitung Verantwortlichen befindet, zum Beispiel dann, wenn personenbezogene Daten von Arbeitnehmern durch den Arbeitgeber im Rahmen von Beschäftigungsverhältnissen verarbeitet werden. Handelt es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, bestünde ein Ungleichgewicht nur bei Verarbeitungsvorgängen, bei denen die Behörde aufgrund ihrer jeweiligen obrigkeitlichen Befugnisse eine Verpflichtung auferlegen kann und deshalb die Einwilligung nicht als ohne Zwang abgegeben gelten kann, wobei die Interessen der betroffenen Person zu berücksichtigen sind.
- (35) Die Verarbeitung von Daten sollte rechtmäßig sein, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.

- (36) Erfolgt die Verarbeitung durch den für die Verarbeitung Verantwortlichen aufgrund einer ihm obliegenden gesetzlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt erforderlich, muss hierfür eine Rechtsgrundlage im Unionsrecht oder im nationalen Recht bestehen, die im Falle einer Beschneidung von Rechten und Freiheiten den Anforderungen der Charta der Grundrechte der Europäischen Union genügt. Desgleichen muss im Unionsrecht oder im nationalen Recht geregelt werden, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln soll.
- (37) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person zu schützen.
- (38) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines für die Verarbeitung Verantwortlichen begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Diese Interessen sind besonders sorgfältig abzuwägen, wenn es sich bei der betroffenen Person um ein Kind handelt, da Kinder besonders schutzwürdig sind. Die betroffene Person sollte das Recht haben, aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Verarbeitung zu widersprechen, ohne dass ihr dadurch Kosten entstehen. Aus Transparenzgründen sollte der für die Verarbeitung Verantwortliche verpflichtet werden, seine berechtigten Interessen gegenüber der betroffenen Person ausdrücklich darzulegen und diese außerdem zu dokumentieren und die betroffene Person über ihr Widerspruchsrecht zu belehren. Da es dem Gesetzgeber obliegt, per Gesetz die Rechtsgrundlage für die Verarbeitung von Daten durch Behörden zu schaffen, greift dieser Rechtfertigungsgrund nicht bei Verarbeitungen durch Behörden, die diese in Erfüllung ihrer Aufgaben vornehmen.
- (39) Die Verarbeitung von 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 für die Verarbeitung Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig ist, d. h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten 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 unberechtigten Zugang zu elektronischen Kommunikationsnetzen, die Verbreitung schädlicher Programmcodes, die Abwehr von Angriffen in Form der gezielten Überlastung von Servern („Denial of access“-Angriffe) sowie Schädigungen von Computer- und elektronischen Kommunikationssystemen zu verhindern.

- (40) Die Verarbeitung personenbezogener Daten für andere Zwecke sollte nur zulässig sein, wenn diese mit den Zwecken, für die sie ursprünglich erhoben wurden, vereinbar sind, beispielsweise dann, wenn die Verarbeitung für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung erforderlich ist. Ist der andere Zweck nicht mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar, muss der für die Verarbeitung Verantwortliche hierfür die Einwilligung der betroffenen Person einholen oder die Verarbeitung auf einen anderen Rechtmäßigkeitsgrund stützen, der sich beispielsweise aus dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, ergibt. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und die betroffene Person über diese anderen Zwecke unterrichtet wird.
- (41) Personenbezogene Daten, die ihrem Wesen nach besonders sensibel und anfällig für eine Verletzung von Grundrechten oder der Privatsphäre sind, bedürfen eines besonderen Schutzes. Derartige Daten dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot sollten im Bedarfsfall jedoch ausdrücklich vorgesehen werden, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.
- (42) Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien sollten auch dann erlaubt sein, wenn es dafür eine gesetzliche Grundlage gibt, und – vorbehaltlich bestimmter Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte – wenn dies durch ein öffentliches Interesse gerechtfertigt ist, speziell wenn es um gesundheitliche Belange geht, wie die Gewährleistung der öffentlichen Gesundheit oder der sozialen Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, vor allem wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sichergestellt werden soll, oder wenn die Verarbeitung historischen oder statistischen Zwecke oder wissenschaftliche Forschungszwecken dient.
- (43) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im internationalen Recht verankerte Ziele von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.
- (44) Wenn es in einem Mitgliedstaat zum Funktionieren des demokratischen Systems gehört, dass die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.
- (45) Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen. Macht die betroffene Person von ihrem Auskunftsrecht Gebrauch, sollte der für die Verarbeitung Verantwortliche das Recht haben, bei der betroffenen Person weitere Informationen einzuholen, die ihn in die Lage versetzen, die von der betreffenden Person gesuchten personenbezogenen Daten zu lokalisieren.

- (46) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information leicht zugänglich sowie in einfacher und verständlicher Sprache abgefasst ist. Dies gilt ganz besonders für bestimmte Situationen wie etwa Werbung im Internet, 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 seine Daten erfasst werden. Wenn sich die Verarbeitung speziell an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer kindgerechten Sprache erfolgen.
- (47) Es gilt, die Modalitäten festzulegen, die es einer betroffenen Person ermöglichen, die ihr nach diese Verordnung zustehenden Rechte wahrzunehmen, etwa dass sie ein kostenfreies Auskunftsrecht oder ein Recht auf Berichtigung oder Löschung von Daten besitzt oder von ihrem Widerspruchsrecht Gebrauch machen kann. Der für die Verarbeitung Verantwortliche sollte verpflichtet werden, innerhalb einer bestimmten Frist auf das Ansuchen der betroffenen Person zu antworten und eine etwaige Ablehnung des Ansuchens zu begründen.
- (48) Die Grundsätze von Treu und Glauben und Transparenz bei der Verarbeitung setzen voraus, dass die betroffene Person insbesondere über die Existenz des Verarbeitungsvorgangs und seine Zwecke, die Speicherfrist, das Recht auf Auskunft sowie das Recht auf Berichtigung und Löschung der Daten und das Beschwerderecht informiert wird. Werden die Daten bei der betroffenen Person erhoben, sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde.
- (49) Die Unterrichtung einer betroffenen Person, dass sie betreffende personenbezogene Daten verarbeitet werden, sollte zum Zeitpunkt der Erhebung erfolgen oder für den Fall, dass die Daten nicht bei ihr erhoben werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die Daten rechtmäßig an einen anderen Empfänger weitergegeben werden dürfen, sollte die betroffene Person bei der erstmaligen Weitergabe der Daten an diesen Empfänger darüber aufgeklärt werden.
- (50) Diese Pflicht erübrigt sich jedoch, wenn die betroffene Person bereits informiert ist oder wenn die Speicherung oder Weitergabe ausdrücklich gesetzlich 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 historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung der Fall sein; als Anhaltspunkt können dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige Ausgleichsmaßnahmen dienen.
- (51) Jede Person sollte ein Auskunftsrecht hinsichtlich der Daten, die bei ihr erhoben worden sind, besitzen und dieses Recht problemlos wahrnehmen können, um sich von der Rechtmäßigkeit ihrer Verarbeitung überzeugen zu können. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie gespeichert werden, wer die Empfänger der Daten sind, nach welcher Logik die Daten verarbeitet werden und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling basiert. Dabei dürfen die Grundrechte und Grundfreiheiten anderer Personen, etwa das Geschäftsgeheimnis oder die Rechte an geistigem Eigentum und

insbesondere das Urheberrecht an Software, nicht angetastet werden. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

- (52) Der für die Verarbeitung Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Falle von Online-Kennungen. Ein für die Verarbeitung Verantwortlicher sollte personenbezogene Daten nicht nur deshalb speichern, um auf mögliche Ansuchen reagieren zu können.
- (53) Jede Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein ‚Recht auf Vergessenwerden‘, wenn die Speicherung ihrer Daten unter Verstoß gegen die Verordnung erfolgt ist. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht weiter verarbeitet werden, wenn sich die Zwecke, für die die Daten erhoben wurden, erübrigt haben, 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 unter Verstoß gegen die Verordnung erfolgt ist. Dieses Recht ist besonders 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 Daten – besonders die im Internet gespeicherten – später löschen möchte. Die weitere Speicherung der Daten sollte jedoch zulässig sein, wenn dies für historische oder statistische Zwecke, zum Zwecke der wissenschaftlichen Forschung, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zur Ausübung des Rechts auf freie Meinungsäußerung erforderlich ist, wenn es hierfür eine gesetzliche Grundlage gibt oder wenn eine beschränkte Verarbeitung der Daten anstatt ihrer Löschung gerechtfertigt ist.
- (54) Um dem ‚Recht auf Vergessenwerden‘ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung so weit gehen, dass ein für die Verarbeitung Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, die Pflicht hat, Dritten, die diese Daten verarbeiten, mitzuteilen, dass eine betroffene Person die Löschung von Links zu diesen Daten oder von Kopien oder Reproduktionen dieser Daten verlangt. Der für die Verarbeitung Verantwortliche sollte im Hinblick auf Daten, für deren Veröffentlichung er die Verantwortung trägt, alle vertretbaren Schritte, auch technischer Art, unternehmen, damit diese Information die betroffenen Dritten auch tatsächlich erreicht. Werden personenbezogene Daten von Dritten veröffentlicht, sollte der für die Verarbeitung Verantwortliche für die Veröffentlichung in die Pflicht genommen werden, wenn er die Veröffentlichung gestattet hat.
- (55) Damit die betroffenen Personen eine bessere Kontrolle über ihre eigenen Daten haben und ihr Auskunftsrecht besser ausüben können, sollten sie im Falle einer elektronischen Verarbeitung ihrer personenbezogenen Daten in einem strukturierten gängigen Format ebenfalls Anspruch auf Erhalt einer Kopie der sie betreffenden Daten in einem gängigen elektronischen Format haben. Die betroffene Person sollte auch befugt sein, die von ihr zur Verfügung gestellten Daten von einer automatisierten Anwendung, etwa einem sozialen Netzwerk, auf eine andere Anwendung zu übertragen. Dies sollte dann möglich sein, wenn die betroffene Person die Daten dem automatisierten Verarbeitungssystem mit ihrer ausdrücklichen Einwilligung oder im Zuge der Erfüllung eines Vertrags zur Verfügung gestellt hat.

- (56) In Fällen, in denen die personenbezogenen Daten zum Schutz der lebenswichtigen Interessen der betroffenen Person oder im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder aufgrund der berechtigten Interessen des für die Verarbeitung Verantwortlichen rechtmäßig verarbeitet werden dürfen, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sie betreffenden Daten einzulegen. Die Beweislast sollte bei dem für die Verarbeitung Verantwortlichen liegen, der darlegen muss, dass seine berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.
- (57) Werden personenbezogene Daten verarbeitet, um Direktwerbung für nichtkommerzielle Zwecke zu betreiben, sollte die betroffene Person unentgeltlich, einfach und effektiv Widerspruch gegen eine solche Verarbeitung einlegen können.
- (58) Eine natürliche Person braucht sich keiner Maßnahme unterwerfen lassen, die auf Profiling im Wege der automatischen Datenverarbeitung basiert. Eine solche Maßnahme sollte allerdings erlaubt sein, wenn sie ausdrücklich per Gesetz genehmigt wurde, bei Abschluss oder in Erfüllung eines Vertrags durchgeführt wird oder wenn die betroffene Person ihre Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden werden wie der Unterrichtung der betroffenen Person oder dem Anspruch auf direkten persönlichen Kontakt sowie dem generellen Ausschluss von Kindern von einer solchen Maßnahme.
- (59) Im Unionsrecht oder im Recht der Mitgliedstaaten können Beschränkungen bestimmter Grundsätze sowie des Rechts auf Unterrichtung, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch, von Maßnahmen, die auf der Erstellung von Profilen beruhen, und von Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person sowie von bestimmten damit zusammenhängenden Pflichten der für die Verarbeitung 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 bei Naturkatastrophen oder vom Menschen verursachten Katastrophen sowie die Verhütung, Aufdeckung und strafrechtliche Verfolgung von Straftaten und von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen gehört, und um sonstige öffentliche Interessen der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen zu schützen. Diese Beschränkungen müssen mit der Charta der Grundrechte der Europäischen Union und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.
- (60) Die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen für jedwede durch diesen oder in dessen Auftrag erfolgende Verarbeitung personenbezogener Daten sollte umfassend geregelt werden. Insbesondere sollte der für die Verarbeitung Verantwortliche dafür Sorge tragen, dass jeder Verarbeitungsvorgang im Einklang mit dieser Verordnung steht, und er sollte dies auch nachweisen müssen.
- (61) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten der betroffenen Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen sowohl bei der Konzipierung der

Verarbeitungsvorgänge als auch zum Zeitpunkt der Verarbeitung getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Anforderungen sicherzustellen und nachzuweisen, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und geeignete Maßnahmen ergreifen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

- (62) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie zur Klärung der Verantwortung und der Haftung der für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, insbesondere für Fälle, in denen ein für die Verarbeitung Verantwortlicher die Verarbeitungszwecke, -bedingungen und -mittel gemeinsam mit anderen für die Verarbeitung Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführt wird.
- (63) Jeder für die Verarbeitung Verantwortliche ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf in der Union ansässige betroffene Personen beziehen und dazu dienen, diesen Personen Waren oder Dienstleistungen anzubieten oder deren Verhalten zu beobachten, sollte einen Vertreter benennen müssen, es sei denn, dieser für die Verarbeitung Verantwortliche ist in einem Drittland niedergelassen, das einen angemessenen Schutz bietet, oder es handelt sich um ein kleines oder mittleres Unternehmen, um eine Behörde oder um eine öffentliche Einrichtung oder der betreffende für die Verarbeitung Verantwortliche bietet den betroffenen Personen nicht nur gelegentlich Waren oder Dienstleistungen an. Der Vertreter sollte im Namen des für die Verarbeitung Verantwortlichen tätig werden und den Aufsichtsbehörden als Ansprechpartner dienen.
- (64) Zur Klärung der Frage, ob ein für die Verarbeitung Verantwortlicher in der Union ansässigen betroffenen Personen nur gelegentlich Waren und Dienstleistungen anbietet, sollte jeweils geprüft werden, ob aus dem allgemeinen Tätigkeitsprofil des für die Verarbeitung Verantwortlichen ersichtlich ist, dass das Anbieten der betreffenden Waren und Dienstleistungen lediglich eine zusätzlich zu seinen Haupttätigkeiten hinzukommende Tätigkeit darstellt.
- (65) Zum Nachweis der Einhaltung der in dieser Verordnung festgelegten Bestimmungen sollte der für die Verarbeitung Verantwortliche jeden Verarbeitungsvorgang dokumentieren. Jeder für die Verarbeitung Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Verlangen die entsprechende Dokumentation vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Unterlagen kontrolliert werden können.
- (66) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu deren Eindämmung ergreifen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der dabei anfallenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und



der Art der zu schützenden personenbezogenen Daten angemessen ist. Die Kommission sollte bei der Festlegung technischer Standards und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung die technologische Neutralität, die Interoperabilität sowie Innovationen fördern und gegebenenfalls mit Drittländern zusammenarbeiten.

- (67) Eine Verletzung des Schutzes personenbezogener Daten kann erhebliche wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs für die betroffene Person nach sich ziehen, wenn nicht rechtzeitig und angemessen reagiert wird. Deshalb sollte der für die Verarbeitung Verantwortliche nach Bekanntwerden einer derartigen Verletzung die Aufsichtsbehörde ohne unangemessene Verzögerung – falls möglich binnen 24 Stunden – davon in Kenntnis setzen. Falls die Benachrichtigung nicht binnen 24 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen. Natürliche Personen, für die eine derartige Verletzung des Schutzes ihrer personenbezogenen Daten nachteilige Auswirkungen haben könnte, sollten ohne unangemessene Verzögerung benachrichtigt werden, damit sie die erforderlichen Sicherheitsvorkehrungen treffen können. Die Auswirkungen einer solchen Verletzung sollten als nachteilig für den Schutz der personenbezogenen Daten oder der Privatsphäre einer natürlichen Person angesehen werden, wenn sie zum Beispiel einen Identitätsdiebstahl oder -betrug, eine physische Schädigung, eine erhebliche Demütigung oder Rufschädigung zur Folge haben. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung beinhalten. 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 (z.B. Strafverfolgungsbehörden) erteilten Weisungen erfolgen. Damit eine betroffene Person das Risiko eines unmittelbaren Schadens für sich klein halten kann, bedarf es beispielsweise ihrer sofortigen Benachrichtigung, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen der Datensicherheit zu ergreifen.
- (68) Um bestimmen zu können, ob eine gegebene Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde und der betroffenen Person ohne unangemessene Verzögerung gemeldet wurde, sollte jeweils überprüft werden, ob der für die Verarbeitung Verantwortliche ausreichende technische Vorkehrungen und organisatorische Maßnahmen getroffen hat, 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, noch bevor persönliche oder wirtschaftliche Interessen Schaden nehmen können, wobei die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren negative Folgen für die betroffene Person zu berücksichtigen sind.
- (69) 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 der Verletzung durch ein frühzeitiges Bekanntwerden in unnötiger Weise behindert würde.

- (70) 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 doch keineswegs in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslose allgemeine Meldepflicht sollte daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit jenen Verarbeitungsvorgängen befassen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können. In derartigen Fällen sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen.
- (71) Dies sollte insbesondere für neu geschaffene umfangreiche Dateien gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, und die eine große Zahl von Personen betreffen könnten.
- (72) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten sinnvoll sein, eine Datenschutz-Folgenabschätzung nicht auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen – beispielsweise wenn Behörden oder öffentliche Einrichtungen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere für die Verarbeitung Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.
- (73) Datenschutz-Folgeabschätzungen sollten von einer Behörde oder öffentlichen Einrichtung durchgeführt werden, sofern eine solche Folgenabschätzung nicht schon anlässlich des Erlasses des Gesetzes erfolgt ist, auf dessen Grundlage die Behörde oder Einrichtung ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt.
- (74) In Fällen, in denen die Datenschutz-Folgenabschätzung ergibt, dass bestimmte Verarbeitungsvorgänge große konkrete Risiken für die Rechte und Freiheiten von betroffenen Personen bergen, zum Beispiel das Risiko, infolge des Rückgriffs auf neue Technologien von dem Recht auf Datenschutz nicht Gebrauch machen zu können, sollte die Aufsichtsbehörde vor Beginn dieser Vorgänge zu der Frage, ob die geplante risikobehaftete Verarbeitung gegen die Bestimmungen dieser Verordnung verstößt, zu Rate gezogen werden müssen und Abhilfeschläge unterbreiten dürfen. Eine solche Konsultation sollte auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer darauf basierenden Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

- (75) In Fällen, in denen die Verarbeitung im öffentlichen Sektor oder durch ein privates Großunternehmen erfolgt oder in denen die Kerntätigkeit eines Unternehmens ungeachtet seiner Größe Verarbeitungsvorgänge einschließt, die einer regelmäßigen und systematischen Überwachung bedürfen, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person unterstützt werden. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich um Angestellte des für die Verarbeitung Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.
- (76) Verbände oder andere Vertreter bestimmter Kategorien von für die Verarbeitung Verantwortlichen sollten ermutigt werden, im Einklang mit dieser Verordnung stehende Verhaltenskodizes zu erstellen, um eine wirksame Anwendung dieser Verordnung zu erleichtern, bei der den Eigenheiten der in bestimmten Sektoren erfolgenden Verarbeitungen Rechnung getragen wird.
- (77) Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und –prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen.
- (78) Der grenzüberschreitende Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels und der grenzübergreifenden Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Der durch diese Verordnung unionsweit garantierte Schutz natürlicher Personen sollte jedoch bei der Übermittlung von personenbezogenen Daten aus der Union in Drittländer oder an internationale Organisationen nicht unterminiert werden. In jedem Fall sollten derartige Datenübermittlungen an Drittländer nur unter strikter Einhaltung dieser Verordnung zulässig sein.
- (79) 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.
- (80) Die Kommission kann mit Wirkung für die gesamte Union beschließen, dass bestimmte Drittländer oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation einen angemessenen Datenschutz bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, einen solchen Schutz zu bieten, in der gesamten Union für Rechtssicherheit und eine einheitliche Rechtsanwendung sorgen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an diese Länder übermittelt werden.
- (81) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Inaugenscheinnahme eines Drittlandes berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, ein Rechtsschutz existiert und die internationalen Menschenrechtsbestimmungen eingehalten werden.

- (82) Die Kommission kann ebenso per Beschluss feststellen, dass bestimmte Drittländer oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation keinen angemessenen Datenschutz bieten. Die Übermittlung personenbezogener Daten an derartige Drittländer sollte daher verboten werden. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden.
- (83) Bei Fehlen eines Angemessenheitsbeschlusses sollte der für die Verarbeitung 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 Garantien können darin bestehen, dass auf verbindliche unternehmensinterne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, von einer Aufsichtsbehörde genehmigte Vertragsklauseln oder auf sonstige geeignete, angemessene, aufgrund der Umstände einer Datenübermittlung oder einer Kategorie von Datenübermittlungen gerechtfertigte und von einer Aufsichtsbehörde gebilligte Maßnahmen zurückgegriffen wird.
- (84) Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter offen stehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln zurückzugreifen, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter keinesfalls daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen zu verwenden oder ihnen weitere Klauseln hinzuzufügen, solange letztere weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Freiheiten der betroffenen Personen beschneiden.
- (85) Jede Unternehmensgruppe sollte für ihre grenzüberschreitenden Datenübermittlungen aus der Union an Organisationen der gleichen Unternehmensgruppe genehmigte verbindliche unternehmensinterne Datenschutzvorschriften anwenden dürfen, sofern in diesen unternehmensinternen Vorschriften Grundprinzipien und durchsetzbare Rechte enthalten sind, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.
- (86) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre Einwilligung erteilt hat, wenn die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaates festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn die Übermittlung aus einem gesetzlich vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In diesem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.
- (87) Diese Ausnahmeregelung sollte insbesondere für Datenübermittlungen gelten, die zur Wahrung eines wichtigen öffentlichen Interesses erforderlich sind, beispielsweise für den grenzüberschreitenden Datenaustausch zwischen Wettbewerbs-, Steuer-, Zoll-

oder Finanzaufsichtsbehörden, zwischen für Angelegenheiten der sozialen Sicherheit zuständigen Diensten oder zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten zuständigen Behörden.

- (88) Übermittlungen, die weder als häufig noch als massiv gelten können, sollten auch im Falle berechtigter Interessen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters möglich sein, wenn letztere sämtliche Umstände der Datenübermittlung geprüft haben. Bei der Verarbeitung zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden.
- (89) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Schutzes vorliegt, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, durch die sichergestellt wird, dass die betroffenen Personen die für die Verarbeitung ihrer personenbezogenen Daten in der Union geltenden Rechte und Garantien genießen, sobald die Daten übermittelt sind.
- (90) Manche Drittländer erlassen Gesetze, Verordnungen und sonstige Rechtsakte, durch die die Datenverarbeitungstätigkeiten von natürlichen und juristischen Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar reguliert werden. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets derartiger 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 in dieser Verordnung festgelegten Bedingungen für Datenübermittlungen in Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Weitergabe aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist. Die Bedingungen für das Bestehen eines wichtigen öffentlichen Interesses sollten von der Kommission in einem delegierten Rechtsakt näher festgelegt werden.
- (91) Bei der Übermittlung personenbezogener Daten über Grenzen hinweg ist der Einzelne womöglich weniger in der Lage, seine Datenschutzrechte wahrzunehmen und sich insbesondere gegen die unrechtmäßige Nutzung oder Weitergabe dieser Informationen zu schützen. Zugleich können die Aufsichtsbehörden unter Umständen nicht in der Lage sein, Beschwerden nachzugehen oder Untersuchungen in Bezug auf Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats durchzuführen. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, nicht übereinstimmende rechtliche Regelungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Daher bedarf es der Förderung einer engeren Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können.
- (92) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die ihre Aufgabe völlig unabhängig erfüllen, ist ein wesentliches Element des Schutzes des Einzelnen im Hinblick auf die Verarbeitung personenbezogener Daten. Die Mitgliedstaaten können

mehr als eine Aufsichtsbehörde errichten, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.

- (93) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er durch ein Rechtsinstrument sicherstellen, dass diese Aufsichtsbehörden am Kohärenz-Verfahren 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 Europäischen Datenschutzausschuss und der Kommission gewährleistet.
- (94) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, die für die Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig und angemessen sind.
- (95) Die allgemeinen Anforderungen an die Mitglieder der Aufsichtsbehörde sollten gesetzlich von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung des Mitgliedstaats ernannt werden; ferner sollten sie Bestimmungen über die persönliche Eignung der Mitglieder und ihre Stellung enthalten.
- (96) 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 bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.
- (97) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat statt, sollte eine einzige Aufsichtsbehörde für die Überwachung der Tätigkeit des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der gesamten Union zuständig sein und die entsprechenden Beschlüsse fassen, damit die einheitliche Anwendung der Vorschriften verbessert, Rechtssicherheit gewährleistet und der Verwaltungsaufwand der für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verringert wird.
- (98) Die zuständige Aufsichtsbehörde, die die Aufgaben einer solchen zentralen Kontaktstelle übernimmt, sollte die Aufsichtsbehörde des Mitgliedstaats sein, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung hat.
- (99) Obgleich diese Verordnung auch für die Tätigkeit der nationalen Gerichte gilt, sollten - damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben unangetastet bleibt - die Aufsichtsbehörden nicht für personenbezogene Daten zuständig sein, die von Gerichten in ihrer gerichtlichen Eigenschaft verarbeitet werden. Diese Ausnahme sollte allerdings streng begrenzt werden auf rein justizielle Tätigkeiten in Gerichtsverfahren und sich nicht auf andere Tätigkeiten beziehen, mit denen je nach dem nationalen Recht Richter betraut sein können.

- (100) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und Befugnisse haben, darunter, insbesondere im Fall von Beschwerden Einzelner, Untersuchungsbefugnisse sowie rechtsverbindliche Interventions-, Beschluss- und Sanktionsbefugnisse sowie die Befugnis, Gerichtsverfahren anzustrengen. Die Aufsichtsbehörden sollten ihre Untersuchungsbefugnisse, was den Zugang zu Räumlichkeiten anbelangt, im Einklang mit dem Unionsrecht und dem einzelstaatlichen Recht ausüben. Dies betrifft vor allem das Erfordernis einer vorherigen richterlichen Genehmigung.
- (101) Jede Aufsichtsbehörde sollte Beschwerden von betroffenen Personen entgegennehmen und die Angelegenheit untersuchen. 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 vonnöten sein, sollte die betroffene Person auch hierüber informiert werden.
- (102) Die Aufklärungsmaßnahmen der Aufsichtsbehörden für die breite Öffentlichkeit sollten an die für die Verarbeitung Verantwortlichen, die Auftragsverarbeiter einschließlich Kleinst-, Klein- und Mittelunternehmen und die betroffenen Personen gerichtete spezifische Maßnahmen einschließen.
- (103) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist.
- (104) Jede Aufsichtsbehörde sollte berechtigt sein, an gemeinsamen Maßnahmen von Aufsichtsbehörden teilzunehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer festgelegten Frist antworten müssen.
- (105) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenz-Verfahren) eingeführt werden, das die Aufsichtsbehörden verpflichtet, untereinander und mit der Kommission zusammenzuarbeiten. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme in Bezug auf Verarbeitungsvorgänge zu treffen, die mit dem Angebot von Waren oder Dienstleistungen für Personen in mehreren Mitgliedstaaten oder der Beobachtung des Verhaltens dieser Personen im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten erheblich beeinträchtigen könnten. Ferner sollte es zur Anwendung kommen, wenn eine Aufsichtsbehörde oder die Kommission beantragen, 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.
- (106) Bei Anwendung des Kohärenzverfahrens sollte der Europäische Datenschutzausschuss, falls von der einfachen Mehrheit seiner Mitglieder so entschieden wird oder falls eine andere Aufsichtsbehörde oder die Kommission darum ersuchen, binnen einer festgelegten Frist eine Stellungnahme abgeben.

- (107) Um die Übereinstimmung mit dieser Verordnung zu gewährleisten, kann die Kommission eine Stellungnahme in der Angelegenheit abgeben oder einen Beschluss fassen, der die Aufsichtsbehörde verpflichtet, die geplante Maßnahme auszusetzen.
- (108) Es kann dringender Handlungsbedarf zum Schutz der Interessen von betroffenen Personen bestehen, insbesondere wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht. Daher sollten die Aufsichtsbehörden bei der Anwendung des Kohärenzverfahrens einstweilige Maßnahmen mit einer festgelegten Geltungsdauer treffen können.
- (109) Die Anwendung dieses Verfahrens sollte eine Bedingung für die rechtliche Gültigkeit und die Durchsetzung des entsprechenden Beschlusses durch eine Aufsichtsbehörde sein. In anderen Fällen von grenzübergreifender Relevanz können die betroffenen Aufsichtsbehörden auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Untersuchungen durchführen, ohne auf das Kohärenz-Verfahren zurückzugreifen.
- (110) Auf Unionsebene sollte ein Europäischer Datenschutzausschuss eingerichtet werden. Dieser ersetzt die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten gebildet werden. Die Kommission sollte sich an seinen Tätigkeiten beteiligen. Der Europäische Datenschutzausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Europäische Datenschutzausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.
- (111) Jede betroffene Person, die sich in ihren Rechten verletzt sieht, die ihr aufgrund dieser Verordnung zustehen, sollte das Recht auf Beschwerde bei einer Aufsichtsbehörde in einem Mitgliedstaat sowie das Recht auf einen gerichtlichen Rechtsbehelf haben, wenn die Aufsichtsbehörde auf die Beschwerde nicht reagiert oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist.
- (112) Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Datenschutzes zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, sollten das Recht haben, im Namen der betroffenen Person Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder unabhängig von der Beschwerde einer betroffenen Person eine eigene Beschwerde zu erheben, wenn ihrer Ansicht nach der Schutz personenbezogener Daten verletzt wurde.
- (113) Jede natürliche oder juristische Person sollte das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde haben. Für Verfahren gegen eine Aufsichtsbehörde sollten die Gerichte des Mitgliedstaats zuständig sein, in dem die Aufsichtsbehörde ihren Sitz hat.
- (114) Um den gerichtlichen Schutz der betroffenen Person in Situationen zu stärken, in denen die zuständige Aufsichtsbehörde ihren Sitz in einem anderen Mitgliedstaat als dem Mitgliedstaat hat, in dem die betroffene Person ansässig ist, sollte die betroffene Person eine Einrichtung, Organisation oder einen Verband, die sich den Schutz der



Rechte und Interessen der betroffenen Personen im Bereich des Datenschutzes zum Ziel gesetzt haben, darum ersuchen können, in ihrem Namen vor dem zuständigen Gericht in dem anderen Mitgliedstaat Klage gegen die Aufsichtsbehörde zu erheben.

- (115) In Fällen, in denen die zuständige Aufsichtsbehörde mit Sitz in einem anderen Mitgliedstaat nicht tätig wird oder unzureichende Maßnahmen in Bezug auf eine Beschwerde getroffen hat, sollte die betroffene Person die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen können, vor dem zuständigen Gericht im anderen Mitgliedstaat Klage gegen die dortige Aufsichtsbehörde zu erheben. Die ersuchte Aufsichtsbehörde sollte entscheiden können, ob es angemessen ist, dem Ersuchen stattzugeben; diese Entscheidung sollte von einem Gericht nachgeprüft werden können.
- (116) Bei Verfahren gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter sollte es dem Kläger überlassen bleiben, ob er die Gerichte des Mitgliedstaats anruft, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat oder in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat; dies gilt nicht, wenn es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.
- (117) Gibt es Hinweise auf in verschiedenen Mitgliedstaaten anhängige Parallelverfahren, sollten die Gerichte verpflichtet sein, sich miteinander in Verbindung zu setzen. Die Gerichte sollten die Möglichkeit haben, ein Verfahren auszusetzen, wenn in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist. Die Mitgliedstaaten sollten sicherstellen, dass effiziente Klagemöglichkeiten vorhanden sind, mit denen rasch Maßnahmen zur Abstellung oder Verhinderung eines Verstoßes gegen diese Verordnung erwirkt werden können.
- (118) Schäden, die einer Person aufgrund einer rechtswidrigen Verarbeitung entstehen, sollten von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter ersetzt werden, die von ihrer Haftung befreit werden können, wenn sie nachweisen, dass ihnen der Schaden nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt.
- (119) Gegen jede – privatem oder öffentlichem Recht unterliegende – Person, die gegen diese Verordnung verstößt, sollten Sanktionen verhängt werden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sind, und alle Maßnahmen zu ihrer Anwendung treffen.
- (120) Um die verwaltungsrechtlichen Sanktionen, die bei Verstößen gegen diese Verordnung verhängt werden können, zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, verwaltungsrechtliche Vergehen zu ahnden. Diese Vergehen sollten in dieser Verordnung zusammen mit der Obergrenze der entsprechenden Geldbußen aufgeführt werden, die in jedem Einzelfall im Verhältnis zu den besonderen Umständen des Falls und unter Berücksichtigung insbesondere der Art, Schwere und Dauer des Verstoßes festzusetzen sind. Abweichungen bei der Anwendung verwaltungsrechtlicher Sanktionen können im Kohärenzverfahren behandelt werden.

- (121) Für die Verarbeitung personenbezogener Daten zu ausschließlich journalistischen Zwecken oder zu künstlerischen oder literarischen Zwecken sind Ausnahmen von bestimmten Vorschriften dieser Verordnung vorzusehen, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf freie Meinungsäußerung und insbesondere dem Recht, Informationen zu empfangen und weiterzugeben, wie es unter anderem in Artikel 11 der Charta der Grundrechte der Europäischen Union 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 deshalb Rechtsvorschriften 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 für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von Daten in Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden sowie in Bezug auf die Zusammenarbeit und die einheitliche Rechtsanwendung regeln. Die Mitgliedstaaten sollten dies jedoch nicht zum Anlass nehmen, Ausnahmeregelungen für die anderen Bestimmungen dieser Verordnung vorzusehen. 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. Die Mitgliedstaaten sollten deshalb für die nach dieser Verordnung zu regelnden Abweichungen und Ausnahmen Tätigkeiten als „journalistisch“ einstufen, wenn das Ziel dieser Tätigkeit in der Weitergabe von Informationen, Meinungen und Vorstellungen an die Öffentlichkeit besteht, unabhängig davon, auf welchem Wege dies geschieht. Diese Tätigkeiten sind mit oder ohne Erwerbszweck möglich und sollten nicht auf Medienunternehmen beschränkt werden.
- (122) Für die Verarbeitung von personenbezogenen Gesundheitsdaten als besonderer Datenkategorie, die eines höheren Schutzes bedarf, lassen sich häufig berechtigte Gründe zugunsten des Einzelnen wie der Gesellschaft insgesamt anführen, insbesondere wenn es darum geht, die Kontinuität der Gesundheitsversorgung über die Landesgrenzen hinaus zu gewährleisten. Diese Verordnung sollte daher vorbehaltlich besonderer und geeigneter Garantien zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen die Bedingungen für die Verarbeitung personenbezogener Gesundheitsdaten harmonisieren. Dies schließt das Recht natürlicher 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.
- (123) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, personenbezogene Gesundheitsdaten auch ohne Einwilligung der betroffenen Person zu verarbeiten. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der 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 ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen

Mittel, die Bereitstellung von und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung personenbezogener Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitnehmer, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.

- (124) Die allgemeinen Grundsätze des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten sollten auch im Beschäftigungskontext gelten. Die Mitgliedstaaten sollten daher in den Grenzen dieser Verordnung die Verarbeitung personenbezogener Daten im Beschäftigungskontext gesetzlich regeln können.
- (125) Die Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung sollte, um rechtmäßig zu sein, auch anderen einschlägigen Rechtsvorschriften unter anderem zu klinischen Versuchen genügen.
- (126) Wissenschaftliche Forschung im Sinne dieser Verordnung sollte Grundlagenforschung, angewandte Forschung und privat finanzierte Forschung einschließen und darüber hinaus dem in Artikel 179 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen.
- (127) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem für die Verarbeitung 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 gesetzlich regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen.
- (128) Im Einklang mit Artikel 17 des Vertrags über die Arbeitsweise der Europäischen Union achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht. Wendet eine Kirche in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, sollten diese Regeln weiter gelten, wenn sie mit dieser Verordnung in Einklang gebracht werden. Kirchen und religiöse Vereinigungen oder Gemeinschaften sollten verpflichtet werden, eine völlig unabhängige Datenschutzaufsicht einzurichten.
- (129) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, Rechtsakte nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union zu erlassen. Delegierte Rechtsakte sollten insbesondere erlassen werden in Bezug auf die Rechtmäßigkeit der Verarbeitung, zur Festlegung der Kriterien und Bedingungen für die Einwilligung eines Kindes, für die Verarbeitung besonderer Kategorien personenbezogener Daten, zur Beurteilung offensichtlich

unverhältnismäßiger Anträge und Gebühren für die Ausübung der Rechte der betroffenen Person, zur Festlegung der Kriterien und Anforderungen im Hinblick auf die Unterrichtung der betroffenen Person sowie in Bezug auf deren Auskunftsrecht, in Bezug auf das Recht auf Vergessenwerden und auf Löschung, betreffend auf Profiling basierende Maßnahmen, zur Festlegung der Kriterien und Anforderungen betreffend die Pflichten des für die Verarbeitung Verantwortlichen in Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, in Bezug auf Auftragsverarbeiter, zur Festlegung der Kriterien und Anforderungen betreffend die Dokumentation und die Sicherheit der Verarbeitung, zur Festlegung der Kriterien und Anforderungen für die Feststellung einer Verletzung des Schutzes personenbezogener Daten und für deren Meldung bei der Aufsichtsbehörde sowie für die Umstände, unter denen anzunehmen ist, dass sich eine solche Verletzung negativ auf die betroffene Person auswirken wird, zur Festlegung der Kriterien und Bedingungen für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung erforderlich ist, zur Festlegung der Kriterien und Anforderungen für die Bestimmung hoher konkreter Risiken, die eine vorherige Zurateziehung der Aufsichtsbehörde erfordern, für die Bestimmung des Datenschutzbeauftragten und dessen Aufgaben, in Bezug auf Verhaltensregeln, zur Festlegung der Kriterien und Anforderungen für Zertifizierungsverfahren und für die Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften, zur Regelung der Ausnahmen für Datenübermittlungen, zur Festlegung der verwaltungsrechtlichen Sanktionen, in Bezug auf die Datenverarbeitung für Gesundheitszwecke, im Beschäftigungskontext und zu historischen und statistischen Zwecken sowie zum Zwecke der wissenschaftlichen Forschung. Es ist besonders wichtig, dass die Kommission im Rahmen ihrer Vorarbeiten auch auf Sachverständigenebene geeignete Konsultationen durchführt. Die Kommission sollte bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte dafür sorgen, dass das Europäische Parlament und der Rat die entsprechenden Dokumente gleichzeitig, rechtzeitig und in geeigneter Form erhalten.

- (130) Um einheitliche Bedingungen für die Anwendung dieser Verordnung sicherzustellen, sollten der Kommission Durchführungsbefugnisse übertragen werden zur Festlegung von: Standardvorlagen für die Verarbeitung personenbezogener Daten von Kindern, Standardverfahren und -vorlagen für die Ausübung der Rechte der betroffenen Person, Standardvorlagen für die Unterrichtung der betroffenen Person, Standardverfahren und -vorlagen für das Auskunftsrecht und das Recht auf Datenübertragbarkeit, Standardvorlagen betreffend die Pflichten des für die Verarbeitung Verantwortlichen in Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie in Bezug auf Dokumentation, besonderen Anforderungen für die Sicherheit der Verarbeitung, Standardformat und Verfahren für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und für die Benachrichtigung der betroffenen Person, Standards und Verfahren für Datenschutz-Folgenabschätzungen, Verfahren und Vorlagen für die vorherige Genehmigung und vorherige Zurateziehung der Aufsichtsbehörde, technischen Standards und Verfahren für die Zertifizierung, Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder Verarbeitungssektor dieses Drittlands oder in einer internationalen Organisation, Fällen der Datenweitergabe, die nicht im Einklang mit dem Unionsrecht stehen, Vorschriften für die Amtshilfe, gemeinsamen Maßnahmen und Beschlüssen im Rahmen des Kohärenzverfahrens. Diese Befugnisse sollten nach Maßgabe der 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,<sup>45</sup> ausgeübt werden. Die Kommission sollte besondere Maßnahmen für Kleinst-, Klein- und Mittelunternehmen erwägen.

- (131) Die Standardvorlagen für die Einwilligung im Falle von Kindern, die Standardverfahren und -vorlagen für die Ausübung der Rechte der betroffenen Person, die Standardvorlagen für die Unterrichtung der betroffenen Person, die Standardverfahren und -vorlagen für das Auskunftsrecht und das Recht auf Datenübertragbarkeit, die Standardvorlagen betreffend die Pflichten des für die Verarbeitung Verantwortlichen in Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie in Bezug auf Dokumentation, die besonderen Anforderungen für die Sicherheit der Verarbeitung, Standardformat und Verfahren für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und für die Benachrichtigung der betroffenen Person, die Standards und Verfahren für Datenschutz-Folgenabschätzungen, die Verfahren und Vorlagen für die vorherige Genehmigung und vorherige Zurateziehung der Aufsichtsbehörde, die technischen Standards und Verfahren für die Zertifizierung, die Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder Verarbeitungssektor dieses Drittlands oder in einer internationalen Organisation, die Fälle der Datenweitergabe, die nicht im Einklang mit dem Unionsrecht stehen, die Vorschriften für die Amtshilfe, für gemeinsame Maßnahmen und Beschlüsse im Rahmen des Kohärenzverfahrens sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.
- (132) Die Kommission sollte in hinreichend begründeten Fällen äußerster Dringlichkeit, die ein Drittland oder ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder eine internationale Organisation betreffen, die kein angemessenes Schutzniveau gewährleisten, und sich auf Angelegenheiten beziehen, die von Aufsichtsbehörden im Rahmen des Kohärenzverfahrens mitgeteilt wurden, sofort geltende Durchführungsrechtsakte erlassen.
- (133) Da die Ziele dieser Verordnung, nämlich ein gleiches Maß an Datenschutz für den Einzelnen und freier Datenverkehr in der Union, auf Ebene der 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 Subsidiaritätsprinzip gemäß Artikel 5 des Vertrags über die Europäische Union tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht diese Verordnung nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.
- (134) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Die Genehmigungen der Aufsichtsbehörden und die Beschlüsse der Kommission auf der Grundlage der Richtlinie 95/46/EG sollten jedoch in Kraft bleiben.

---

<sup>45</sup> 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).

- (135) 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 festgelegten spezifischen Pflichten, die dasselbe Ziel verfolgen, unterliegen einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Um das Verhältnis zwischen dieser Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden.
- (136) Für Island und Norwegen stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses 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<sup>46</sup> dar.
- (137) Für die Schweiz stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses 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<sup>47</sup> dar.
- (138) Für Lichtenstein stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses 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<sup>48</sup> dar.
- (139) Diese Verordnung steht, in Anbetracht des Umstands, dass, wie der Gerichtshof der Europäischen Union betont hat, das Recht auf Schutz der personenbezogenen Daten keine uneingeschränkte Geltung beanspruchen kann, sondern im Hinblick auf seine gesellschaftliche Funktion gesehen werden und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss, im Einklang mit allen Grundrechten und Grundsätzen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere mit dem Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, dem Recht auf Schutz personenbezogener Daten, der Gedanken-, Gewissens- und Religionsfreiheit, der Freiheit der Meinungsäußerung und der Informationsfreiheit, der unternehmerischen

---

<sup>46</sup> ABl. L 176 vom 10.7.1999, S. 36.

<sup>47</sup> ABl. L 53 vom 27.2.2008, S. 52.

<sup>48</sup> ABl. L 160 vom 18.6.2011, S. 19.

Freiheit, dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren sowie mit der Achtung der Vielfalt der Kulturen, Religionen und Sprachen –

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. Die 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 oder 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 einer Datei gespeichert sind oder gespeichert werden sollen.
2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird
  - a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit,
  - b) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union,
  - c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Kapitel 2 des Vertrags über die Europäische Union fallen,
  - d) durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht,
  - e) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.

3. Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit von Anbietern von Vermittlungsdiensten unberührt.

### *Artikel 3*

#### ***Räumlicher Anwendungsbereich***

1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.
2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung
  - a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder
  - b) der Beobachtung ihres Verhaltens dient.
3. Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

### *Artikel 4*

#### ***Begriffsbestimmungen***

Im Sinne dieser Verordnung bezeichnet der Ausdruck

- (1) „betroffene Person“ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
- (2) „personenbezogene Daten“ alle Informationen, die sich auf eine betroffene Person beziehen;
- (3) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede 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 Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung sowie das Löschen oder Vernichten der Daten;



- (4) „Datei“ 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;
- (5) "für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten durch einzelstaatliches oder Unionsrecht vorgegeben, können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach einzelstaatlichem oder Unionsrecht bestimmt werden;
- (6) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- (7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden;
- (8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
- (9) "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
- (10) „genetische Daten“ Daten jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen;
- (11) „biometrische Daten“ Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten;
- (12) „Gesundheitsdaten“ Informationen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die betreffende Person beziehen;
- (13) „Hauptniederlassung“ im Falle des für die Verarbeitung Verantwortlichen der Ort seiner Niederlassung in der Union, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten getroffen werden; wird über die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten nicht in der Union entschieden, ist die Hauptniederlassung der Ort, an dem die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen in der Union hauptsächlich stattfinden. Im Falle des Auftragsverarbeiters bezeichnet

„Hauptniederlassung“ den Ort, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat;

- (14) „Vertreter“ jede in der Union niedergelassene natürliche oder juristische Person, die von dem für die Verarbeitung Verantwortlichen ausdrücklich bestellt wurde und in Bezug auf die diesem nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle handelt und gegenüber den Aufsichtsbehörden oder sonstigen Stellen in der Union als Ansprechpartner fungiert;
- (15) „Unternehmen“ jedes Gebilde, das eine wirtschaftliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, das heißt vor allem natürliche und juristische Personen sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
- (16) „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
- (17) „verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet;
- (18) „Kind“ jede Person bis zur Vollendung des achtzehnten Lebensjahres;
- (19) „Aufsichtsbehörde“ eine von einem Mitgliedstaat nach Maßgabe von Artikel 46 eingerichtete staatliche Stelle.

## **KAPITEL II GRUNDSÄTZE**

### *Artikel 5*

#### ***Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten***

Personenbezogene Daten müssen

- a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- b) für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- c) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein; sie dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht

durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können;

- d) sachlich richtig und auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden;
- e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Realisierung der Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten ausschließlich zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke im Einklang mit den Vorschriften und Modalitäten des Artikels 83 verarbeitet werden und die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen überprüft wird;
- f) unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen verarbeitet werden, der dafür haftet, dass bei jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den Nachweis hierfür erbringen muss.

#### *Artikel 6*

#### ***Rechtmäßigkeit der Verarbeitung***

1. Die Verarbeitung personenbezogener Daten 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 genau festgelegte Zwecke gegeben.
  - b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.
  - c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.
  - d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.
  - e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.
  - f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen 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. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.
3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e müssen eine Rechtsgrundlage haben im
  - a) Unionsrecht oder
  - b) Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.

Die einzelstaatliche Regelung muss ein im öffentlichen Interesse liegendes Ziel verfolgen oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem mit der Verarbeitung verfolgten legitimen Zweck stehen.

4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Absatz 1 Buchstabe f für verschiedene Bereiche und Verarbeitungssituationen einschließlich Situationen, die die Verarbeitung personenbezogener Daten von Kindern betreffen, näher zu regeln.

#### *Artikel 7* **Einwilligung**

1. Der für die Verarbeitung Verantwortliche trägt die Beweislast dafür, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für eindeutig festgelegte Zwecke erteilt hat.
2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.
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.
4. Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht.

*Artikel 8*  
***Verarbeitung personenbezogener Daten eines Kindes***

1. Für die Zwecke dieser Verordnung ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Dienste der Informationsgesellschaft angeboten werden, nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um eine nachprüfbare Einwilligung zu erhalten.
2. Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind, unberührt.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.
4. Die Kommission kann Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

*Artikel 9*  
***Verarbeitung besonderer Kategorien von personenbezogenen Daten***

1. Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Überzeugungen, die Religions- oder Glaubenszugehörigkeit oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie von genetischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßnahmen ist untersagt.
2. Absatz 1 gilt nicht in folgenden Fällen:
  - a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten vorbehaltlich der in den Artikeln 7 und 8 genannten Bedingungen eingewilligt, es sei denn, nach den Rechtsvorschriften der Union oder eines Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, oder
  - b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche seine ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen arbeitsrechtlichen Pflichten nachkommen kann, soweit dies nach den Vorschriften der Union oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist, oder
  - c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich und die betroffene Person ist aus

physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder

- d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Erwerbszweck im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur 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 Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder
  - e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder
  - f) die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich oder
  - g) die Verarbeitung ist erforderlich, um auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, eine im öffentlichen Interesse liegende Aufgabe zu erfüllen, oder
  - h) die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Artikels 81 für Gesundheitszwecke erforderlich oder
  - i) die Verarbeitung ist vorbehaltlich der Bedingungen und Garantien des Artikels 83 für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung erforderlich oder
  - j) die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßnahmen erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung einer Aufgabe, der ein wichtiges öffentliches Interesse zugrunde liegt, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist. Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten sowie angemessene Garantien für die Verarbeitung der in Absatz 1 genannten besonderen Kategorien von personenbezogenen Daten und die in Absatz 2 genannten Ausnahmen näher zu regeln.

*Artikel 10*  
***Verarbeitung, ohne dass die betroffene Person bestimmt werden kann***

Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, ist er nicht verpflichtet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen.

**KAPITEL III**  
**RECHTE DER BETROFFENEN PERSON**  
**ABSCHNITT 1**  
**TRANSPARENZ UND MODALITÄTEN**

*Artikel 11*  
***Transparente Information und Kommunikation***

1. Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine nachvollziehbare und für jedermann leicht zugängliche Strategie.
2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache zur Verfügung, besonders dann, wenn die Information an ein Kind gerichtet ist.

*Artikel 12*  
***Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann***

1. Der für die Verarbeitung Verantwortliche legt fest, mittels welcher Verfahren er die Informationen gemäß Artikel 14 bereitstellt und den betroffenen Personen die Ausübung der ihnen gemäß Artikel 13 sowie den Artikeln 15 bis 19 zustehenden Rechte ermöglicht. Er trifft insbesondere Vorkehrungen, um die Beantragung der in Artikel 13 sowie in den Artikeln 15 bis 19 genannten Maßnahmen zu erleichtern. Im Falle der automatischen Verarbeitung personenbezogener Daten sorgt der für die Verarbeitung Verantwortliche dafür, dass die Maßnahme elektronisch beantragt werden kann.
2. Der für die Verarbeitung Verantwortliche kommt seiner Informationspflicht gegenüber der betroffenen Person umgehend nach und teilt ihr spätestens innerhalb eines Monats nach Eingang eines Antrags mit, ob eine Maßnahme nach Artikel 13 oder den Artikeln 15 bis 19 ergriffen wurde, und erteilt die erbetene Auskunft. Diese Frist kann um einen Monat verlängert werden, wenn mehrere betroffene Personen von ihren Rechten Gebrauch machen und ihre Zusammenarbeit bis zu einem vertretbaren Maß notwendig ist, um einen unnötigen und unverhältnismäßig hohen Aufwand seitens des für die Verarbeitung Verantwortlichen zu vermeiden. Die Unterrichtung hat schriftlich zu erfolgen. Stellt die betroffene Person den Antrag in

elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

3. Weigert sich der für die Verarbeitung Verantwortliche, auf Antrag der betroffenen Person tätig zu werden, unterrichtet er die betroffene Person über die Gründe für die Weigerung und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.
4. Die Unterrichtung und die auf Antrag ergriffenen Maßnahmen gemäß Absatz 1 sind kostenlos. Bei offenkundig unverhältnismäßigen Anträgen und besonders im Fall ihrer Häufung kann der für die Verarbeitung Verantwortliche ein Entgelt für die Unterrichtung oder die Durchführung der beantragten Maßnahme verlangen oder die beantragte Maßnahme unterlassen. In diesem Fall trägt der für die Verarbeitung Verantwortliche die Beweislast für den offenkundig unverhältnismäßigen Charakter des Antrags.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Voraussetzungen für offenkundig unverhältnismäßige Anträge sowie die in Absatz 4 genannten Entgelte näher zu regeln.
6. Die Kommission kann Standardvorlagen und Standardverfahren für die Mitteilungen gemäß Absatz 2, auch für solche in elektronischer Form, festlegen. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

#### *Artikel 13*

#### ***Rechte gegenüber Empfängern***

Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung, die aufgrund von Artikel 16 beziehungsweise 17 vorgenommen wird, mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

## **ABSCHNITT 2 INFORMATIONSPFLICHT UND AUSKUNFTSRECHT**

#### *Artikel 14*

#### ***Information der betroffenen Person***

1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche zumindest Folgendes mit:
  - a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters und des Datenschutzbeauftragten,
  - b) die Zwecke, für die Daten verarbeitet werden, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, beziehungsweise die von dem für die



Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,

- c) die Dauer, für die die personenbezogenen Daten gespeichert werden,
  - d) das Bestehen eines Rechts auf Auskunft sowie Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,
  - e) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
  - f) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,
  - g) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das dort geltende Datenschutzniveau unter Bezugnahme auf einen Angemessenheitsbeschluss der Kommission,
  - h) sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.
2. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem mit, ob die Bereitstellung der Daten obligatorisch oder fakultativ ist und welche mögliche Folgen die Verweigerung der Daten hätte.
  3. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem die Herkunft der personenbezogenen Daten mit.
  4. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1, 2 und 3
    - a) zum Zeitpunkt der Erhebung der personenbezogenen Daten bei der betroffenen Person oder
    - b) falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, zum Zeitpunkt ihrer Erfassung oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen, unter denen die Daten erhoben oder auf sonstige Weise verarbeitet wurden, Rechnung trägt, oder, falls die Weitergabe an einen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.
  5. Die Absätze 1 bis 4 finden in folgenden Fällen keine Anwendung:
    - a) Die betroffene Person verfügt bereits über die Informationen gemäß den Absätzen 1, 2 und 3 oder

- b) die Daten werden nicht bei der betroffenen Person erhoben und die Unterrichtung erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohen Aufwand verbunden oder
  - c) die Daten werden nicht bei der betroffenen Person erhoben und die Erfassung oder Weitergabe ist ausdrücklich per Gesetz geregelt oder
  - d) die Daten werden nicht bei der betroffenen Person erhoben und die Bereitstellung der Informationen greift nach Maßgabe des Unionsrechts oder des Rechts der Mitgliedstaaten gemäß Artikel 21 in die Rechte und Freiheiten anderer Personen ein.
6. Im Fall des Absatzes 5 Buchstabe b ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person.
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kategorien von Empfängern gemäß Absatz 1 Buchstabe f, den Anforderungen an Informationen gemäß Absatz 1 Buchstabe g, den Kriterien für die Erteilung sonstiger Informationen im Sinne von Absatz 1 Buchstabe h für verschiedene Bereiche und Verarbeitungssituationen und zu den Bedingungen und geeigneten Garantien im Hinblick auf die Ausnahmen gemäß Absatz 5 Buchstabe b zu regeln. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst und Kleinstunternehmen sowie mittlere Unternehmen.
8. Die Kommission kann Standardvorlagen für die Bereitstellung der Informationen gemäß den Absätzen 1 bis 3 festlegen, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

#### *Artikel 15*

#### ***Auskunftsrecht der betroffenen Person***

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht. Werden personenbezogene Daten verarbeitet, teilt der für die Verarbeitung Verantwortliche Folgendes mit:
- a) die Verarbeitungszwecke,
  - b) die Kategorien personenbezogener Daten, die verarbeitet werden,
  - c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden müssen oder weitergegeben worden sind, speziell bei Empfängern in Drittländern,
  - d) die Dauer, für die die personenbezogenen Daten gespeichert werden,
  - e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung

Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,

- f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
  - g) diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,
  - h) die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen, zumindest im Fall der Maßnahmen gemäß Artikel 20.
2. Die betroffene Person hat Anspruch darauf, dass ihr von dem für die Verarbeitung Verantwortlichen mitgeteilt wird, welche personenbezogenen Daten verarbeitet werden. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.
  3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kriterien und Anforderungen in Bezug auf die Mitteilung über den Inhalt der personenbezogenen Daten gemäß Absatz 1 Buchstabe g an die betroffene Person festzulegen.
  4. Die Kommission kann Standardvorlagen und -verfahren für Auskunftsgesuche und die Erteilung der Auskünfte gemäß Absatz 1 festlegen, darunter auch für die Überprüfung der Identität der betroffenen Person und die Mitteilung der personenbezogenen Daten an die betroffene Person, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

### **ABSCHNITT 3**

## **BERICHTIGUNG UND LÖSCHUNG**

#### *Artikel 16*

#### ***Recht auf Berichtigung***

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung von unzutreffenden personenbezogenen Daten zu verlangen. Die betroffene Person hat das Recht, die Vervollständigung unvollständiger personenbezogener Daten, auch in Form eines Korrigendums, zu verlangen.

#### *Artikel 17*

#### ***Recht auf Vergessenwerden und auf Löschung***

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen, speziell wenn es sich um

personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft:

- a) Die 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 stützte, oder die Speicherfrist, für die die Einwilligung gegeben wurde, ist abgelaufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.
  - c) Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.
  - d) Die Verarbeitung der Daten ist aus anderen Gründen nicht mit der Verordnung vereinbar.
2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen.
3. Der für die Verarbeitung Verantwortliche sorgt für eine umgehende Löschung der personenbezogenen Daten, soweit deren Speicherung nicht erforderlich ist
- (a) zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80;
  - (b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81;
  - (c) für historische und statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83;
  - (d) zur Erfüllung einer gesetzlichen Pflicht zur Vorhaltung der personenbezogenen Daten, der der für die Verarbeitung Verantwortliche nach dem Unionsrecht oder dem Recht eines Mitgliedstaats unterliegt, wobei das mitgliedstaatliche Recht ein im öffentlichen Interesse liegendes Ziel verfolgen, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen muss;
  - (e) in den in Absatz 4 genannten Fällen.
4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung beschränken, wenn

- a) ihre Richtigkeit von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen;
  - b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Erfüllung seiner Aufgabe nicht länger benötigt, sie aber für Beweiszwecke weiter aufbewahrt werden müssen;
  - c) die Verarbeitung unrechtmäßig ist, die betroffene Person aber Einspruch gegen ihre Löschung erhebt und stattdessen deren eingeschränkte Nutzung fordert;
  - d) die betroffene Person gemäß Artikel 18 Absatz 2 die Übertragung der personenbezogenen Daten auf ein anderes automatisiertes Verarbeitungssystem fordert.
5. Die in Absatz 4 genannten personenbezogenen Daten dürfen mit Ausnahme ihrer Speicherung nur verarbeitet werden, wenn sie für Beweiszwecke erforderlich sind, wenn die betroffene Person ihre Einwilligung gegeben hat oder die Rechte einer anderen natürlichen oder juristischen Person geschützt werden müssen oder wenn dies im öffentlichen Interesse liegt.
6. Unterliegt die Verarbeitung personenbezogener Daten gemäß Absatz 4 einer Beschränkung, teilt der für die Verarbeitung Verantwortliche der betroffenen Person im Voraus mit, dass die Beschränkung aufgehoben werden soll.
7. Der für die Verarbeitung Verantwortliche trifft Vorkehrungen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden.
8. Wird eine Löschung vorgenommen, darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht auf sonstige Weise verarbeiten.
9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf
- a) die Kriterien und Anforderungen im Hinblick auf die Anwendung von Absatz 1 für bestimmte Bereiche und spezielle Verarbeitungssituationen,
  - b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten,
  - c) die Kriterien und Bedingungen für die Beschränkung der Verarbeitung personenbezogener Daten gemäß Absatz 4.

*Artikel 18*  
***Recht auf Datenübertragbarkeit***

1. Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das Recht, von dem für

die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen.

2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.
3. Die Kommission kann das elektronische Format gemäß Absatz 1 festlegen sowie die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten gemäß Absatz 2. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

## **ABSCHNITT 4**

### **WIDERSPRUCHSRECHT UND PROFILING**

#### *Artikel 19*

#### ***Widerspruchsrecht***

1. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben d, e und f erfolgt, Widerspruch einzulegen, sofern der für die Verarbeitung Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, dagegen unentgeltlich Widerspruch einzulegen. Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.
3. Im Falle eines Widerspruchs gemäß den Absätzen 1 und 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht weiter nutzen oder anderweitig verarbeiten.

#### *Artikel 20*

#### ***Auf Profiling basierende Maßnahmen***

1. Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen

Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.

2. Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person einer Maßnahme nach Absatz 1 nur unterworfen werden, wenn die Verarbeitung
  - a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags vorgenommen wird und der Abschluss oder die Erfüllung des Vertrags auf Wunsch der betroffenen Person erfolgt ist oder geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, beispielsweise durch das Recht auf direkten persönlichen Kontakt, oder
  - b) ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person enthalten oder
  - c) mit Einwilligung der betroffenen Person nach Maßgabe von Artikel 7 und vorbehaltlich entsprechender Garantien erfolgt.
3. Die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Merkmale einer natürlichen Person darf sich nicht ausschließlich auf die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten stützen.
4. In Fällen gemäß Absatz 2 müssen die von dem für die Verarbeitung Verantwortlichen gemäß Artikel 14 erteilten Auskünfte auch Angaben zu einer etwaigen Verarbeitung für die unter Absatz 1 beschriebenen Zwecke und die damit angestrebten Auswirkungen auf die betroffene Person beinhalten.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen, die für geeignete Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 gelten sollen, näher zu regeln.

## **ABSCHNITT 5 BESCHRÄNKUNGEN**

### *Artikel 21 Beschränkungen*

1. Die Union oder die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5 Buchstaben a bis e und den Artikeln 11 bis 20 sowie gemäß Artikel 32 beschränken, sofern eine solche Beschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist
  - a) zum Schutz der öffentlichen Sicherheit
  - b) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten

- c) zum Schutz sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats etwa im Währungs-, Haushalts- und Steuerbereich und zum Schutz der Marktstabilität und Marktintegrität
  - d) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe
  - e) für Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a, b, c und d genannten Zwecke verbunden sind
  - f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.
2. Jede Legislativmaßnahme im Sinne des Absatzes 1 muss spezifische Vorschriften zumindest zu den mit der Verarbeitung verfolgten Zielen und zur Bestimmung des für die Verarbeitung Verantwortlichen enthalten.

## **KAPITEL IV**

# **FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER**

### **ABSCHNITT 1**

### **ALLGEMEINE PFLICHTEN**

#### *Artikel 22*

#### *Pflichten des für die Verarbeitung Verantwortlichen*

1. Der für die Verarbeitung Verantwortliche stellt durch geeignete Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann.
2. Die in Absatz 1 genannten Maßnahmen umfassen insbesondere
  - (f) die Dokumentation nach Maßgabe von Artikel 28;
  - (g) die Umsetzung der in Artikel 30 vorgesehenen Vorkehrungen für die Datensicherheit;
  - (h) die Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 33;
  - (i) die Umsetzung der nach Artikel 34 Absätze 1 und 2 geltenden Anforderungen in Bezug auf die vorherige Genehmigung oder Zurateziehung der Aufsichtsbehörde;
  - (j) die Benennung eines Datenschutzbeauftragten gemäß Artikel 35 Absatz 1.



3. Der für die Verarbeitung Verantwortliche setzt geeignete Verfahren zur Überprüfung der Wirksamkeit der in den Absätzen 1 und 2 genannten Maßnahmen ein. Die Überprüfung wird von unabhängigen internen oder externen Prüfern durchgeführt, wenn dies angemessen ist.
4. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für die in Absatz 1 genannten Maßnahmen, die Bedingungen für die in Absatz 3 genannten Überprüfungs- und Auditverfahren und die Kriterien für die in Absatz 3 angesprochene Angemessenheitsprüfung festzulegen und spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen zu prüfen.

#### *Artikel 23*

#### ***Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen***

1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.
2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.
4. Die Kommission kann technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.

#### *Artikel 24*

#### ***Gemeinsam für die Verarbeitung Verantwortliche***

In allen Fällen, in denen ein für die Verarbeitung Verantwortlicher die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten gemeinsam mit anderen Personen festlegt, vereinbaren diese gemeinsam für die Verarbeitung Verantwortlichen, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die

Verfahren und Mechanismen betrifft, die den betroffenen Person die Wahrnehmung ihrer Rechte ermöglichen.

#### *Artikel 25*

##### ***Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen***

1. Jeder für die Verarbeitung Verantwortliche, der sich in der in Artikel 3 Absatz 2 beschriebenen Situation befindet, benennt einen Vertreter in der Union.
2. Diese Pflicht gilt nicht für
  - a) für die Verarbeitung Verantwortliche, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz im Sinne von Artikel 41 bietet; oder
  - b) Unternehmen, die weniger als 250 Mitarbeiter beschäftigen; oder
  - c) Behörden oder öffentliche Einrichtungen; oder
  - d) für die Verarbeitung Verantwortliche, die in der Union ansässigen betroffenen Personen nur gelegentlich Waren oder Dienstleistungen anbieten.
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, ansässig sind.
4. Die Benennung eines Vertreters durch den für die Verarbeitung Verantwortlichen erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen.

#### *Artikel 26*

##### ***Auftragsverarbeiter***

1. Der für die Verarbeitung Verantwortliche wählt für alle in seinem Auftrag durchzuführenden Verarbeitungsvorgänge einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.
2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter

- a) nur auf Weisung des für die Verarbeitung Verantwortlichen tätig wird, insbesondere in Fällen, in denen eine Übermittlung der personenbezogenen Daten nicht zulässig ist;
  - b) ausschließlich Mitarbeiter beschäftigt, die sich zur Vertraulichkeit verpflichtet haben oder der gesetzlichen Verschwiegenheitspflicht unterliegen;
  - c) alle in Artikel 30 genannten erforderlichen Maßnahmen ergreift;
  - d) die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf;
  - e) soweit es verarbeitungsbedingt möglich ist, in Absprache mit dem für die Verarbeitung Verantwortlichen die notwendigen technischen und organisatorischen Voraussetzungen dafür schafft, dass der für die Verarbeitung Verantwortliche seine Pflicht erfüllen kann, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
  - f) den Auftragsverarbeiter bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;
  - g) nach Abschluss der Verarbeitung dem für die Verarbeitung Verantwortlichen sämtliche Ergebnisse aushändigt und die personenbezogenen Daten auf keine andere Weise weiterverarbeitet;
  - (h) dem für die Verarbeitung Verantwortlichen und der Aufsichtsbehörde alle erforderlichen Informationen für die Kontrolle der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt.
3. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dokumentieren die Anweisungen des für die Verarbeitung Verantwortlichen und die in Absatz 2 aufgeführten Pflichten des Auftragsverarbeiters.
  4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.
  5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters in Übereinstimmung mit Absatz 1 festzulegen sowie die Bedingungen, durch die die Verarbeitung personenbezogener Daten in Unternehmensgruppen speziell zu Kontroll- und Berichterstattungszwecken vereinfacht werden kann.

*Artikel 27*  
**Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters**

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, sofern sie keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedstaatlichen Recht erwachsenden Pflichten unterliegen.

*Artikel 28*  
**Dokumentation**

1. Alle für die Verarbeitung Verantwortlichen, alle Auftragsverarbeiter sowie etwaige Vertreter von für die Verarbeitung Verantwortlichen dokumentieren die ihrer Zuständigkeit unterliegenden Verarbeitungsvorgänge.
2. Die Dokumentation enthält mindestens folgende Informationen:
  - a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (oder etwaiger gemeinsam für die Verarbeitung Verantwortlicher) oder des Auftragsverarbeiters sowie eines etwaigen Vertreters;
  - b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;
  - c) Angaben über die Zwecke der Verarbeitung sowie – falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet – über die von dem für die Verarbeitung Verantwortlichen verfolgten legitimen Interessen;
  - d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;
  - e) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten einschließlich der für die Verarbeitung Verantwortlichen, denen personenbezogene Daten aus dem von diesen verfolgtem legitimen Interesse mitgeteilt werden;
  - f) gegebenenfalls Angaben über etwaige Datenübermittlungen in Drittländer oder an internationale Organisationen einschließlich deren Namen sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen ein Beleg dafür, dass geeignete Sicherheitsgarantien vorgesehen wurden;
  - g) eine allgemeine Angabe der Fristen für die Löschung der verschiedenen Datenkategorien;
  - h) eine Beschreibung der in Artikel 22 Absatz 3 genannten Verfahren.
3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen die Dokumentation der Aufsichtsbehörde auf Anforderung zur Verfügung.

4. Die in den Absätzen 1 und 2 genannten Anforderungen gelten nicht für folgende für die Verarbeitung Verantwortliche und Auftragsverarbeiter:
  - a) natürliche Personen, die personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeiten; oder
  - b) Unternehmen oder Organisationen mit weniger als 250 Beschäftigten, die personenbezogene Daten nur als Nebentätigkeit zusätzlich zu ihren Haupttätigkeiten verarbeiten.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannte Dokumentation festzulegen, so dass insbesondere den Verantwortlichkeiten des für die Verarbeitung Verantwortlichen, des Auftragsverarbeiters sowie des etwaigen Vertreters des für die Verarbeitung Verantwortlichen Rechnung getragen wird.
6. Die Kommission kann Standardvorlagen für die in Absatz 1 genannte Dokumentation festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.

#### *Artikel 29*

#### ***Zusammenarbeit mit der Aufsichtsbehörde***

1. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen arbeiten der Aufsichtsbehörde auf Verlangen zu, um ihr die Erfüllung ihrer Pflichten zu erleichtern, indem sie dieser insbesondere die in Artikel 53 Absatz 2 Buchstabe a genannten Informationen übermitteln und ihr den in Artikel 53 Absatz 2 Buchstabe b genannten Zugang gewähren.
2. Auf von der Aufsichtsbehörde im Rahmen der Ausübung ihrer Befugnisse erteilte Anordnungen gemäß Artikel 53 Absatz 2 antworten der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter der Aufsichtsbehörde binnen einer von der Aufsichtsbehörde zu setzenden angemessenen Frist. Die Antwort muss auch eine Beschreibung der im Anschluss an die Bemerkungen der Aufsichtsbehörde getroffenen Maßnahmen und der damit erzielten Ergebnisse beinhalten.

## **ABSCHNITT 2 DATENSICHERHEIT**

#### *Artikel 30*

#### ***Sicherheit der Verarbeitung***

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

2. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen im Anschluss an eine Risikobewertung die in Absatz 1 genannten Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlicher Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für die in den Absätzen 1 und 2 genannten technischen und organisatorischen Maßnahmen festzulegen und den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen, wobei sie die technologische Entwicklung sowie Lösungen für einen Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen berücksichtigt, sofern nicht Artikel 4 gilt.
4. Die Kommission kann erforderlichenfalls Durchführungsbestimmungen zu einer situationsabhängigen Konkretisierung der in den Absätzen 1 und 2 genannten Anforderungen erlassen, um insbesondere
  - a) jedweden unbefugten Zugriff auf personenbezogene Daten zu verhindern;
  - b) jedwede unbefugte Einsichtnahme in personenbezogene Daten sowie jedwede unbefugte Offenlegung, Kopie, Änderung, Löschung oder Entfernung von personenbezogenen Daten zu verhindern;
  - c) sicherzustellen, dass die Rechtmäßigkeit der Verarbeitungsvorgänge überprüft wird.

Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.

#### *Artikel 31*

#### ***Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde***

1. Bei einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde ohne unangemessene Verzögerung und nach Möglichkeit binnen 24 Stunden nach Feststellung der Verletzung. Falls die Meldung an die Aufsichtsbehörde nicht binnen 24 Stunden erfolgt, ist dieser eine Begründung beizufügen.
2. In Übereinstimmung mit Artikel 26 Absatz 2 Buchstabe f alarmiert und informiert der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unmittelbar nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.
3. Die in Absatz 1 genannte Benachrichtigung enthält mindestens folgende Informationen:
  - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Datenkategorien und der Zahl der betroffenen Datensätze;

- b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;
  - c) Empfehlungen für Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen der Verletzung des Schutzes personenbezogener Daten;
  - d) eine Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten;
  - e) eine Beschreibung der vom für die Verarbeitung Verantwortlichen vorgeschlagenen oder ergriffenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten.
4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. Die Dokumentation enthält nur die zu diesem Zweck erforderlichen Informationen.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Feststellung der in den Absätzen 1 und 2 genannten Verletzungen des Schutzes personenbezogener Daten festzulegen sowie die konkreten Umstände, unter denen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben.
6. Die Kommission kann das Standardformat für derartige Meldungen an die Aufsichtsbehörde, die Verfahrensvorschriften für die vorgeschriebene Meldung sowie Form und Modalitäten der in Absatz 4 genannten Dokumentation einschließlich der Fristen für die Löschung der darin enthaltenen Informationen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.

#### *Artikel 32*

#### ***Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten***

1. Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung nach Artikel 31 die betroffene Person ohne unangemessene Verzögerung von der Verletzung des Schutzes personenbezogener Daten, wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person umfasst mindestens die in Artikel 31 Absatz 3 Buchstaben b und c genannten Informationen und Empfehlungen.
3. Die Benachrichtigung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten ist nicht erforderlich, wenn der für die Verarbeitung

Verantwortliche zur Zufriedenheit der Aufsichtsbehörde nachweist, dass er geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Durch diese technischen Sicherheitsvorkehrungen sind die betreffenden Daten für alle Personen zu verschlüsseln, die nicht zum Zugriff auf die Daten befugt sind.

4. Unbeschadet der dem für die Verarbeitung Verantwortlichen obliegenden Pflicht, der betroffenen Person die Verletzung des Schutzes personenbezogener Daten mitzuteilen, kann die Aufsichtsbehörde, falls der für die Verarbeitung Verantwortliche die betroffene Person noch nicht in Kenntnis gesetzt hat, nach Prüfung der zu erwartenden negativen Auswirkungen der Verletzung den für die Verarbeitung Verantwortlichen auffordern, dies zu tun.
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Umstände festzulegen, unter denen sich eine Verletzung des Schutzes personenbezogener Daten negativ auf die in Absatz 1 genannten personenbezogenen Daten auswirken kann.
6. Die Kommission kann das Format für die in Absatz 1 genannte Mitteilung an die betroffene Person und die für die Mitteilung geltenden Verfahrensvorschriften festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.

### **ABSCHNITT 3**

## **DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE GENEHMIGUNG**

#### *Artikel 33*

#### ***Datenschutz-Folgenabschätzung***

1. Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.
2. Die in Absatz 1 genannten Risiken bestehen insbesondere bei folgenden Verarbeitungsvorgängen:
  - a) systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen, die sich auf eine automatisierte Verarbeitung von Daten gründet und ihrerseits als Grundlage für Maßnahmen dient, welche Rechtswirkung gegenüber der betroffenen Person entfalten oder erhebliche Auswirkungen für diese mit sich bringen;



- b) Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten, wenn die betreffenden Daten in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen;
  - c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung;
  - d) Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten;
  - e) sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab die Aufsichtsbehörde zu Rate zu ziehen ist.
3. Die Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung; sie 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 werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden.
4. Der für die Verarbeitung Verantwortliche holt die Meinung der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
5. Falls es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde oder um eine öffentliche Einrichtung handelt und die Verarbeitung aufgrund einer im Unionsrecht festgelegten rechtlichen Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c erfolgt, welche Vorschriften und Verfahren für die betreffenden Verarbeitungsvorgänge vorsieht, gelten die Absätze 1 bis 4 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.
6. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für Verarbeitungsvorgänge, die mit den in den Absätzen 1 und 2 genannten Risiken behaftet sein können, sowie die Anforderungen an die in Absatz 3 genannte Folgenabschätzung einschließlich der Bedingungen für die Skalierbarkeit und für die interne und externe Überprüfbarkeit festzulegen. Dabei berücksichtigt die Kommission spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen.
7. Die Kommission kann Standards und Verfahren für die Durchführung sowie für die interne und externe Überprüfung der in Absatz 3 genannten Folgenabschätzung festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.

*Artikel 34*  
*Vorherige Genehmigung und vorherige Zurateziehung*

1. Der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter holt vor der Verarbeitung personenbezogener Daten eine Genehmigung der Aufsichtsbehörde ein, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die Risiken zu mindern, welche für die betroffenen Personen bestehen, wenn dieser Vertragsklauseln nach Artikel 42 Absatz 2 Buchstabe d vereinbart oder keine geeigneten Garantien für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation in einem rechtsverbindlichen Instrument nach Artikel 42 Absatz 5 vorsieht.
2. Der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter zieht vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die für die betroffenen Personen bestehenden Risiken zu mindern; dies gilt für alle Fälle, in denen
  - a) aus einer Datenschutz-Folgenabschätzung nach Artikel 33 hervorgeht, dass die geplanten Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke hohe konkrete Risiken bergen können; oder
  - b) die Aufsichtsbehörde eine vorherige Zurateziehung bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält.
3. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, untersagt sie die geplante Verarbeitung und unterbreitet geeignete Vorschläge, wie diese Mängel beseitigt werden könnten.
4. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Zurateziehung nach Absatz 2 Buchstabe b sind, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt derartige Listen an den Europäischen Datenschutzausschuss.
5. Wenn auf der in Absatz 4 genannten Liste Verarbeitungsvorgänge aufgeführt werden, die sich auf Waren oder Dienstleistungen beziehen, welche betroffenen Personen in mehreren Mitgliedstaaten angeboten werden, oder die dazu dienen sollen, das Verhalten dieser betroffenen Personen zu beobachten, oder die wesentliche Auswirkungen auf den freien Verkehr personenbezogener Daten in der Union haben können, bringt die Aufsichtsbehörde vor der Annahme der Liste das in Artikel 57 beschriebene Kohärenzverfahren zur Anwendung.
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter legt der Aufsichtsbehörde die Datenschutz-Folgenabschätzung nach Artikel 33 vor und übermittelt ihr auf Aufforderung alle sonstigen Informationen, die sie benötigt, um

die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Risiken und die diesbezüglichen Sicherheitsgarantien bewerten zu können.

7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung einer von ihren nationalen Parlamenten zu erlassenden Legislativmaßnahme oder einer sich auf eine solche Legislativmaßnahme gründenden Maßnahme, durch die die Art der Verarbeitung definiert wird, zu Rate, damit die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sichergestellt ist und insbesondere die für die betreffenden Personen bestehenden Risiken gemindert werden.
8. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Bestimmung der in Absatz 2 Buchstabe a genannten hohen konkreten Risiken festzulegen.
9. Die Kommission kann Standardvorlagen und Verfahrensvorschriften für die in den Absätzen 1 und 2 genannte vorherige Genehmigung beziehungsweise Zurateziehung sowie für die in Absatz 6 vorgesehene Unterrichtung der Aufsichtsbehörde festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.

## **ABSCHNITT 4**

### **DATENSCHUTZBEAUFTRAGTER**

#### *Artikel 35*

#### ***Benennung eines Datenschutzbeauftragten***

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls
  - a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder
  - b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder
  - c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.
2. Im Fall des Absatzes 1 Buchstabe b darf eine Gruppe von Unternehmen einen gemeinsamen Datenschutzbeauftragten ernennen.
3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann der Datenschutzbeauftragte unter Berücksichtigung der Struktur der Behörde beziehungsweise der öffentlichen Einrichtung für mehrere Bereiche benannt werden.

4. In anderen als den in Absatz 1 genannten Fällen können der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen.
5. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt den Datenschutzbeauftragten nach Maßgabe der beruflichen Qualifikation und insbesondere des Fachwissens, das dieser auf dem Gebiet des Datenschutzrechts und der einschlägigen Praktiken besitzt, sowie nach Maßgabe von dessen Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben. Der Grad des erforderlichen Fachwissens richtet sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten.
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass etwaige sonstige berufliche Pflichten des Datenschutzbeauftragten mit den Aufgaben und Pflichten, die diesem in seiner Funktion als Datenschutzbeauftragter obliegen, vereinbar sind und zu keinen Interessenkonflikten führen.
7. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt einen Datenschutzbeauftragten für einen Zeitraum von mindestens zwei Jahren. Der Datenschutzbeauftragte kann für weitere Amtszeiten wiederernannt werden. Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt.
8. Der Datenschutzbeauftragte kann durch den für die Verarbeitung Verantwortlichen oder durch den Auftragsverarbeiter beschäftigt werden oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
9. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter teilt der Aufsichtsbehörde und der Öffentlichkeit den Namen und die Kontaktdaten des Datenschutzbeauftragten mit.
10. Betroffene Personen haben das Recht, den Datenschutzbeauftragten zu allen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehenden Fragen zu Rate zu ziehen und die Wahrnehmung ihrer Rechte gemäß dieser Verordnung zu beantragen.
11. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 Buchstabe c genannte Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie die Kriterien für die berufliche Qualifikation des in Absatz 5 genannten Datenschutzbeauftragten festzulegen.

*Artikel 36*  
***Stellung des Datenschutzbeauftragten***

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
2. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte seinen Pflichten und Aufgaben unabhängig nachkommen kann und keine Anweisungen bezüglich der Ausübung seiner Tätigkeit erhält. Der Datenschutzbeauftragte berichtet unmittelbar der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und stellt das erforderliche Personal, die erforderlichen Räumlichkeiten, die erforderliche Ausrüstung und alle sonstigen Ressourcen, die für die Erfüllung der in Artikel 37 genannten Pflichten und Aufgaben erforderlich sind, zur Verfügung.

*Artikel 37*  
***Aufgaben des Datenschutzbeauftragten***

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter betraut den Datenschutzbeauftragten mit mindestens folgenden Aufgaben:
  - a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters über dessen aus dieser Verordnung erwachsenden Pflichten sowie Dokumentation dieser Tätigkeit und der erhaltenen Antworten;
  - b) Überwachung der Umsetzung und Anwendung der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
  - c) Überwachung der Umsetzung und Anwendung dieser Verordnung, insbesondere ihrer Anforderungen an einen Datenschutz durch Technik und an datenschutzfreundliche Voreinstellungen, an die Datensicherheit, an die Benachrichtigung der betroffenen Personen und an die Anträge der betroffenen Personen zur Wahrnehmung der ihnen nach dieser Verordnung zustehenden Rechte;
  - d) Sicherstellung, dass die in Artikel 28 genannte Dokumentation vorgenommen wird;
  - e) Überwachung der Dokumentation und Meldung von Verletzungen des Schutzes personenbezogener Daten sowie die Benachrichtigung davon gemäß den Artikeln 31 und 32;
  - f) Überwachung der von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter durchgeführten Datenschutz-Folgenabschätzung sowie der

Beantragung einer vorherigen Genehmigung beziehungsweise Zurateziehung gemäß den Artikeln 33 und 34;

- g) Überwachung der auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutzbeauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;
  - (h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen sowie gegebenenfalls Zurateziehung der Aufsichtsbehörde auf eigene Initiative.
2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Aufgaben, die Zertifizierung, die Stellung, die Befugnisse und die Ressourcen des in Absatz 1 genannten Datenschutzbeauftragten festzulegen.

## **ABSCHNITT 5 VERHALTENSREGELN UND ZERTIFIZIERUNG**

### *Artikel 38 Verhaltensregeln*

1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen:
- a) faire und transparente Datenverarbeitung,
  - b) Datenerhebung,
  - c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;
  - d) von betroffenen Personen in Ausübung ihrer Rechte gestellte Anträge;
  - e) Unterrichtung und Schutz von Kindern;
  - f) Datenübermittlung in Drittländer oder an internationale Organisationen;
  - g) Mechanismen zur Überwachung und zur Sicherstellung der Einhaltung der Verhaltensregeln durch die diesen unterliegenden für die Verarbeitung Verantwortlichen;
  - (h) außergerichtliche Verfahren und sonstige Streitschlichtungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der den betroffenen Personen aus den Artikeln 73 und 75 erwachsenden Rechte.

2. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten und beabsichtigen, eigene Verhaltensregeln aufzustellen oder bestehende Verhaltensregeln zu ändern oder zu erweitern, können diesbezügliche Vorschläge der Aufsichtsbehörde in dem betreffenden Mitgliedstaat zur Stellungnahme vorlegen. Die Aufsichtsbehörde kann zu der Frage Stellung nehmen, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde hört die betroffenen Personen oder ihre Vertreter zu diesen Vorschlägen an.
3. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von Verhaltensregeln sowie Vorschläge zur Änderung oder Ausweitung bestehender Verhaltensregeln vorlegen.
4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.
5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

#### *Artikel 39* **Zertifizierung**

1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.
2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen.
3. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.

# **KAPITEL V**

## **ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN**

### *Artikel 40*

#### *Allgemeine Grundsätze der Datenübermittlung*

Jedwede Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung 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 Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.

### *Artikel 41*

#### *Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses*

1. Eine Datenübermittlung darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner weiteren Genehmigung.
2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission
  - a) die Rechtsstaatlichkeit, die geltenden allgemeinen und sektorspezifischen Vorschriften, insbesondere über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, die in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation geltenden Landesregeln und Sicherheitsvorschriften sowie die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen und insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden;
  - b) die Existenz und die Wirksamkeit einer oder mehrerer in dem betreffenden Drittland beziehungsweise in der betreffenden internationalen Organisation tätiger unabhängiger Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind, und
  - c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation eingegangenen internationalen Verpflichtungen.



3. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.
4. In jedem Durchführungsrechtsakt werden der geografische und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben.
5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bietet; dies gilt insbesondere für Fälle, in denen die in dem betreffenden Drittland beziehungsweise der betreffenden internationalen Organisation geltenden allgemeinen und sektorspezifischen Vorschriften keine wirksamen und durchsetzbaren Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für in der Union ansässige betroffene Personen und insbesondere für betroffene Personen, deren personenbezogene Daten übermittelt werden, garantieren. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 oder – in Fällen, in denen es äußerst dringlich ist, das Recht natürlicher Personen auf den Schutz ihrer personenbezogenen Daten zu wahren – nach dem in Artikel 87 Absatz 3 genannten Verfahren angenommen.
6. Wenn die Kommission die in Absatz 5 genannte Feststellung trifft, wird dadurch jedwede Übermittlung personenbezogener Daten an das betreffende Drittland beziehungsweise an ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder an die betreffende internationale Organisation unbeschadet der Bestimmungen der Artikel 42 bis 44 untersagt. Die Kommission nimmt zu geeigneter Zeit Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation auf, um Abhilfe für die Situation, die aus dem gemäß Absatz 5 erlassenen Beschluss entstanden ist, zu schaffen.
7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren von Drittländern und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese einen beziehungsweise keinen angemessenen Schutz personenbezogener Daten bieten.
8. Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission geändert, ersetzt oder aufgehoben werden.

#### *Artikel 42*

#### ***Datenübermittlung auf der Grundlage geeigneter Garantien***

1. Hat die Kommission keinen Beschluss nach Artikel 41 erlassen, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermitteln, sofern er in

einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.

2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere bestehen in Form
  - a) verbindlicher unternehmensinterner Vorschriften nach Artikel 43;
  - b) von der Kommission angenommener Standarddatenschutzklauseln, diese Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen;
  - c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommener Standarddatenschutzklauseln, sofern diesen von der Kommission allgemeine Gültigkeit gemäß Artikel 62 Absatz 1 Buchstabe b zuerkannt wurde, oder
  - d) von Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden.
3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, b und c genannten unternehmensinternen Vorschriften und Standarddatenschutzklauseln erfolgen, bedürfen keiner weiteren Genehmigung.
4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d dieses Artikels genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung der Aufsichtsbehörde gemäß Artikel 34 Absatz 1 Buchstabe a ein. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.
5. Wenn keine geeigneten Garantien für den Schutz personenbezogener Daten in einem rechtsverbindlichen Instrument vorgesehen werden, holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung für die Übermittlung oder Kategorie von Übermittlungen oder für die Aufnahme von entsprechenden Bestimmungen in die Verwaltungsvereinbarungen ein, die die Grundlage für eine solche Übermittlung bilden. Derartige vorherige Genehmigungen der Aufsichtsbehörde müssen im Einklang mit Artikel 34 Absatz 1 Buchstabe a stehen. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung. Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben so lange in Kraft, bis sie von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden.

### Artikel 43

#### *Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften*

1. Eine Aufsichtsbehörde kann nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens verbindliche unternehmensinterne Vorschriften genehmigen, sofern diese
  - a) rechtsverbindlich sind, für alle Mitglieder der Unternehmensgruppe des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden;
  - b) den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen;
  - c) die in Absatz 2 festgelegten Anforderungen erfüllen.
2. Alle verbindlichen unternehmensinternen Vorschriften enthalten mindestens folgende Informationen:
  - a) Struktur und Kontaktdaten der Unternehmensgruppe und ihrer Mitglieder;
  - b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Kategorien 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 unternehmensinternen Vorschriften;
  - d) die allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, die Datenqualität, die Rechtsgrundlage für die Verarbeitung sowie die Bestimmungen für etwaige Verarbeitungen sensibler personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese Vorschriften gebundene Organisationen;
  - e) die Rechte der betroffenen Personen und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 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 unternehmensinternen Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;
  - f) die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße von nicht in der Union niedergelassenen Mitgliedern der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Vorschriften; der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, 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 gemäß Artikel 11 über die verbindlichen unternehmensinternen Vorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;
  - h) die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;
  - i) die innerhalb der Unternehmensgruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften;
  - j) die Verfahren für die Meldung und Erfassung von Änderungen der Unternehmenspolitik und ihre Meldung an die Aufsichtsbehörde;
  - k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe gewährleisten, wie insbesondere die Offenlegung der Ergebnisse der Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.
4. Die Kommission kann das Format und Verfahren für den auf elektronischem Wege erfolgenden Informationsaustausch über verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

#### *Artikel 44* **Ausnahmen**

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 vorliegt noch geeignete Garantien nach Artikel 42 bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur zulässig, wenn
- a) die betroffene Person der vorgeschlagenen Datenübermittlung zugestimmt hat, nachdem sie über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführter Datenübermittlungen informiert wurde,

- b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist,
  - c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist,
  - d) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist,
  - e) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist,
  - f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
  - g) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder
  - (h) die Übermittlung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter wahrgenommen wird, erforderlich ist und nicht als häufig oder massiv bezeichnet werden kann, und falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.
2. Datenübermittlungen gemäß Absatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.
3. Bei Datenverarbeitungen gemäß Absatz 1 Buchstabe h berücksichtigt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter insbesondere die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland sowie erforderlichenfalls etwaige vorgesehene geeignete Garantien zum Schutz personenbezogener Daten.

4. Absatz 1 Buchstaben b, c und h gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.
5. Das in Absatz 1 Buchstabe d genannte öffentliche Interesse muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die in Absatz 1 Buchstabe h dieses Artikels genannten geeigneten Garantien in der Dokumentation gemäß Artikel 28 und setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis.
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die in Absatz 1 Buchstabe d genannten „wichtigen Gründe des öffentlichen Interesses“ zu präzisieren und die Kriterien und Anforderungen für die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h festzulegen.

#### *Artikel 45*

#### ***Internationale Zusammenarbeit zum Schutz personenbezogener Daten***

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur
  - a) Entwicklung wirksamer Mechanismen der internationalen Zusammenarbeit, durch die die 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 Mitteilungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,
  - c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,
  - d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten.
2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen und insbesondere zu deren Aufsichtsbehörden, wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese einen angemessenen Schutz bieten.

# KAPITEL VI

## UNABHÄNGIGE AUFSICHTSBEHÖRDEN

### ABSCHNITT 1

#### UNABHÄNGIGKEIT

##### *Artikel 46*

##### *Aufsichtsbehörde*

1. Jeder Mitgliedstaat trägt dafür Sorge, dass eine oder mehrere Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind und einen Beitrag zur ihrer einheitlichen Anwendung in der gesamten Union leisten, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten geschützt und der freie Verkehr dieser Daten in der Union erleichtert werden. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.
2. Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die als zentrale Kontaktstelle für die wirksame Beteiligung dieser Behörden im Europäischen Datenschutzausschuss fungiert und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 57 einhalten.
3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

##### *Artikel 47*

##### *Unabhängigkeit*

1. Die Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben und Befugnisse völlig unabhängig.
2. Die Mitglieder der Aufsichtsbehörde ersuchen in Ausübung ihres Amtes weder um Weisung noch nehmen sie Weisungen entgegen.
3. 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. Die Mitglieder der Aufsichtsbehörde verhalten sich nach Ablauf ihrer Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen ehrenhaft und zurückhaltend.
5. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde mit angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und mit der erforderlichen Infrastruktur ausgestattet wird, um ihre Aufgaben und Befugnisse

auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.

6. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde über eigenes Personal verfügt, das vom Leiter der Aufsichtsbehörde ernannt wird und seiner Leitung untersteht.
7. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörde über einen eigenen jährlichen Haushalt verfügt. Die Haushaltspläne werden veröffentlicht.

#### *Artikel 48*

#### ***Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde***

1. Die Mitgliedstaaten tragen dafür Sorge, dass die Mitglieder der Aufsichtsbehörde entweder vom Parlament oder von der Regierung des betreffenden Mitgliedstaats ernannt werden.
2. Die Mitglieder werden aus einem Kreis von Personen ausgewählt, an deren Unabhängigkeit kein Zweifel besteht, und die nachweislich über die für die Erfüllung ihrer Aufgaben erforderliche 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 seiner Enthebung aus dem Amt gemäß Absatz 4.
4. Ein Mitglied kann vom zuständigen nationalen Gericht seines Amtes enthoben oder seiner Ruhegehaltsansprüche oder an ihrer Stelle gewährten Vergünstigungen für verlustig erklärt werden, wenn es die Voraussetzungen für die Ausübung seines Amtes nicht mehr erfüllt oder eine schwere Verfehlung begangen hat.
5. Endet die Amtszeit des Mitglieds oder tritt es zurück, übt es sein Amt so lange weiter aus, bis ein neues Mitglied ernannt ist.

#### *Artikel 49*

#### ***Errichtung der Aufsichtsbehörde***

Jeder Mitgliedstaat regelt durch Gesetz in den Grenzen dieser Verordnung

- a) die Errichtung der Aufsichtsbehörde und ihre Stellung,
- b) die Qualifikation, Erfahrung und fachliche Eignung, die für die Wahrnehmung der Aufgaben eines Mitglieds der Aufsichtsbehörde notwendig ist,
- c) die Vorschriften und Verfahren für die Ernennung der Mitglieder der Aufsichtsbehörde und zur Bestimmung der Handlungen und Tätigkeiten, die mit dem Amt unvereinbar sind,



- d) die Amtszeit der Mitglieder der Aufsichtsbehörde, die mindestens vier Jahre beträgt; dies gilt nicht für die erste Amtszeit nach Inkrafttreten dieser Verordnung, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;
- e) ob die Mitglieder der Aufsichtsbehörde wiederernannt werden können,
- f) die Regelungen und allgemeinen Bedingungen für das Amt eines Mitglieds und die Aufgaben der Bediensteten der Aufsichtsbehörde,
- g) die Regeln und Verfahren für die Beendigung der Amtszeit der Mitglieder der Aufsichtsbehörde, auch für den Fall, dass sie die Voraussetzungen für die Ausübung ihres Amtes nicht mehr erfüllen oder eine schwere Verfehlung begangen haben.

#### *Artikel 50*

#### ***Verschwiegenheitspflicht***

Die Mitglieder und Bediensteten der Aufsichtsbehörde sind während ihrer Amtsbeziehungsweise Dienstzeit und auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben bekannt geworden sind, Verschwiegenheit zu bewahren.

## **ABSCHNITT 2 AUFGABEN UND BEFUGNISSE**

#### *Artikel 51*

#### ***Zuständigkeit***

1. Jede Aufsichtsbehörde übt im Hoheitsgebiet ihres Mitgliedstaats die ihr mit dieser Verordnung übertragenen Befugnisse aus.
2. Findet die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der Union statt, wobei der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, so ist die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, unbeschadet der Bestimmungen von Kapitel VII dieser Verordnung für die Aufsicht über dessen Verarbeitungstätigkeit in allen Mitgliedstaaten zuständig.
3. Die Aufsichtsbehörde ist nicht zuständig für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen.

*Artikel 52*  
*Aufgaben*

1. Aufgaben der Aufsichtsbehörde sind
  - a) die Überwachung und Gewährleistung der Anwendung dieser Verordnung,
  - b) die Befassung mit Beschwerden betroffener Personen oder von Verbänden, die diese Personen gemäß Artikel 73 vertreten, die Untersuchung der Angelegenheit in angemessenem Umfang und Unterrichtung der betroffenen Personen oder Verbände über den Fortgang und das Ergebnis der Beschwerde innerhalb einer angemessenen Frist, vor allem, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,
  - c) der Informationsaustausch mit anderen Aufsichtsbehörden und die Amtshilfe sowie die Gewährleistung der einheitlichen Anwendung und Durchsetzung dieser Verordnung,
  - d) die Durchführung von Untersuchungen auf eigene Initiative, aufgrund einer Beschwerde oder auf Ersuchen einer anderen Aufsichtsbehörde und, falls die betroffene Person eine Beschwerde bei dieser Aufsichtsbehörde eingereicht hat, deren Unterrichtung über die Ergebnisse der Untersuchungen innerhalb einer angemessenen Frist,
  - e) die Verfolgung relevanter Entwicklungen, soweit als sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere der Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,
  - f) die Beratung der Organe und Einrichtungen der Mitgliedstaaten im Hinblick auf Rechts- und Verwaltungsmaßnahmen, die den Schutz der Rechte und Freiheiten der natürlichen Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand haben,
  - g) die Beratung in Bezug auf die in Artikel 34 genannten Verarbeitungsvorgänge und deren Genehmigung,
  - h) die Abgabe von Stellungnahmen zu den Entwürfen von Verhaltensregeln gemäß Artikel 38 Absatz 2,
  - i) die Genehmigung verbindlicher unternehmensinterner Vorschriften gemäß Artikel 43,
  - j) die Mitwirkung im Europäischen Datenschutzausschuss.
2. Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.

3. Die Aufsichtsbehörde berät auf Antrag jede betroffene Person bei der Wahrnehmung der ihr nach dieser Verordnung zustehenden Rechte und arbeitet zu diesem Zweck gegebenenfalls mit den Aufsichtsbehörden anderer Mitgliedstaaten zusammen.
4. Für die in Absatz 1 Buchstabe b genannten Beschwerden stellt die Aufsichtsbehörde ein Beschwerdeformular zur Verfügung, das elektronisch oder auf anderem Wege ausgefüllt werden kann.
5. Die Leistungen der Aufsichtsbehörde sind für die betroffene Person kostenlos.
6. Bei offensichtlich missbräuchlichen Anträgen, insbesondere bei wiederholt gestellten Anträgen, kann die Aufsichtsbehörde eine Gebühr verlangen oder davon absehen, die von der betroffenen Person beantragte Maßnahme zu treffen. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offensichtlich missbräuchlichen Charakter des Antrags.

*Artikel 53*  
**Befugnisse**

1. Jede Aufsichtsbehörde ist befugt,
  - a) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter auf einen behaupteten Verstoß gegen die Vorschriften zum Schutz personenbezogener Daten hinzuweisen und ihn gegebenenfalls anzuweisen, diesem Verstoß in einer bestimmten Weise abzuwehren, um den Schutz der betroffenen Person zu verbessern,
  - b) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
  - c) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben zweckdienlich sind,
  - d) die Befolgung der Genehmigungen und Auskünfte im Sinne von Artikel 34 sicherzustellen,
  - e) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter zu ermahnen oder zu verwarnen,
  - f) die Berichtigung, Löschung oder Vernichtung aller Daten, die unter Verletzung der Bestimmungen dieser Verordnung verarbeitet wurden, anzuordnen, und solche Maßnahmen Dritten, an die diese Daten weitergegeben wurden, mitzuteilen,
  - g) die Verarbeitung vorübergehend oder endgültig zu verbieten,
  - h) die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation zu unterbinden,

- i) Stellungnahmen zu allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten abzugeben,
  - j) das nationale Parlament, die Regierung oder sonstige politische Institutionen sowie die Öffentlichkeit über Fragen im Zusammenhang mit dem Schutz personenbezogener Daten zu informieren.
2. Jede Aufsichtsbehörde kann kraft ihrer Untersuchungsbefugnis vom für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter Folgendes verlangen:
- a) Zugriff auf alle personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind,
  - b) Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte, sofern Grund zu der Annahme besteht, dass dort Tätigkeiten ausgeführt werden, die gegen diese Verordnung verstoßen.

Die Befugnisse nach Buchstabe b werden im Einklang mit dem Unionsrecht und dem Recht der Mitgliedstaaten ausgeübt.

3. Jede Aufsichtsbehörde ist insbesondere gemäß Artikel 74 Absatz 4 und Artikel 75 Absatz 2 befugt, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Klage zu erheben.
4. Jede Aufsichtsbehörde ist befugt, verwaltungsrechtliche Vergehen, insbesondere solche nach Artikel 79 Absätze 4, 5 und 6, zu ahnden.

#### *Artikel 54* **Tätigkeitsbericht**

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit. Der Bericht wird dem nationalen Parlament vorgelegt und der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

## **KAPITEL VII** **ZUSAMMENARBEIT UND KOHÄRENZ**

### **ABSCHNITT 1** **ZUSAMMENARBEIT**

#### *Artikel 55* **Amtshilfe**

1. Die Aufsichtsbehörden übermitteln einander zweckdienliche 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 Auskunftersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Zurateziehung, die Vornahme von Nachprüfungen und die zügige Unterrichtung über die Befassung mit einer Angelegenheit und über weitere Entwicklungen in Fällen, in denen Personen in mehreren Mitgliedstaaten voraussichtlich von Verarbeitungsvorgängen betroffen sind.

2. Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu können insbesondere auch die Übermittlung zweckdienlicher Informationen über den Verlauf einer Untersuchung oder Durchsetzungsmaßnahmen gehören, um die Einstellung oder das Verbot von Verarbeitungsvorgängen zu erwirken, die gegen diese Verordnung verstoßen.
3. Das Amtshilfeersuchen enthält alle erforderlichen Informationen, darunter Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für die Angelegenheit verwendet, für die sie angefordert wurden.
4. Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn
  - a) sie für das Ersuchen nicht zuständig ist oder
  - b) das Ersuchen gegen die Bestimmungen dieser Verordnung verstoßen würde.
5. Die Aufsichtsbehörde, an die das Ersuchen gerichtet wurde, informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen.
6. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, auf elektronischem Wege und so schnell wie möglich unter Verwendung eines standardisierten Formats.
7. Maßnahmen, die aufgrund eines Amtshilfeersuchens getroffen werden, sind gebührenfrei.
8. Wird eine ersuchte Aufsichtsbehörde nicht binnen eines Monats auf das Amtshilfeersuchen einer anderen Aufsichtsbehörde hin tätig, so ist die ersuchende Aufsichtsbehörde befugt, einstweilige Maßnahmen im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen und die Angelegenheit dem Europäischen Datenschutzausschuss gemäß dem Verfahren von Artikel 57 vorzulegen.
9. Die Aufsichtsbehörde legt fest, wie lange diese einstweilige Maßnahme gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission unverzüglich unter Angabe aller Gründe von diesen Maßnahmen in Kenntnis.
10. Die Kommission kann Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere das in Absatz 6 genannte standardisierte

Format, festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

#### *Artikel 56*

#### ***Gemeinsame Maßnahmen der Aufsichtsbehörden***

1. Zur Stärkung der Zusammenarbeit und Amtshilfe erfüllen die Aufsichtsbehörden gemeinsame untersuchungsspezifische Aufgaben, führen gemeinsame Durchsetzungsmaßnahmen und andere gemeinsame Maßnahmen durch, an denen benannte Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.
2. In Fällen, in denen voraussichtlich Personen in mehreren Mitgliedstaaten von Verarbeitungsvorgängen betroffen sind, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, an den gemeinsamen untersuchungsspezifischen Aufgaben oder den gemeinsamen Maßnahmen teilzunehmen. Die zuständige Aufsichtsbehörde lädt die Aufsichtsbehörde jedes dieser Mitgliedstaaten zur Teilnahme an den betreffenden gemeinsamen untersuchungsspezifischen Aufgaben oder gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme.
3. Jede Aufsichtsbehörde kann als einladende Aufsichtsbehörde gemäß ihren nationalen Rechtsvorschriften und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde Durchführungsbefugnisse einschließlich untersuchungsspezifischer Aufgaben übertragen oder, soweit dies nach dem Recht der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Durchführungsbefugnisse nach dem Recht der unterstützenden Aufsichtsbehörde auszuüben. Diese Durchführungsbefugnisse können nur unter der Leitung und in der Regel in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem nationalen Recht der einladenden Aufsichtsbehörde. Die einladende Aufsichtsbehörde haftet für ihre Handlungen.
4. Die Aufsichtsbehörden regeln die praktischen Aspekte spezifischer Kooperationsmaßnahmen.
5. Kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 nach, so sind die anderen Aufsichtsbehörden befugt, eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen.
6. Die Aufsichtsbehörde legt fest, wie lange die einstweilige Maßnahme nach Absatz 5 gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde teilt dem Europäischen Datenschutzausschuss und der Kommission diese Maßnahmen unverzüglich unter Angabe aller Gründe mit und nimmt für diese Sache das in Artikel 57 genannte Verfahren in Anspruch.

## **ABSCHNITT 2 KOHÄRENZ**

### *Artikel 57 Kohärenzverfahren*

Zu den in Artikel 46 Absatz 1 genannten Zwecken arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und mit der Kommission zusammen.

### *Artikel 58 Stellungnahme des Europäischen Datenschutzausschusses*

1. Bevor eine Aufsichtsbehörde eine Maßnahme nach Absatz 2 erlässt, übermittelt sie die geplante Maßnahme dem Europäischen Datenschutzausschuss und der Kommission.
2. Die in Absatz 1 genannte Verpflichtung gilt für Maßnahmen, die Rechtswirkung entfalten sollen und
  - a) sich auf Verarbeitungstätigkeiten beziehen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen in mehreren Mitgliedstaaten oder mit der Beobachtung des Verhaltens dieser Personen im Zusammenhang stehen, oder
  - b) den freien Verkehr personenbezogener Daten in der Union wesentlich beeinträchtigen können oder
  - c) der Annahme einer Liste der Verarbeitungsvorgänge dienen, die der vorherigen Zurateziehung gemäß Artikel 34 Absatz 5 unterliegen oder
  - d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dienen oder
  - e) der Genehmigung von Vertragsklauseln gemäß Artikel 42 Absatz 2 Buchstabe d dienen oder
  - f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dienen.
3. Jede Aufsichtsbehörde und der Europäische Datenschutzausschuss können beantragen, dass eine Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird, insbesondere, wenn eine Aufsichtsbehörde die in Absatz 2 genannte geplante Maßnahme nicht vorlegt oder den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht nachkommt.
4. Um die ordnungsgemäße und kohärente Anwendung dieser Verordnung sicherzustellen, kann die Kommission beantragen, dass eine Sache im Rahmen des Kohärenzverfahrens behandelt wird.

5. Die Aufsichtsbehörden und die Kommission übermitteln auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme und die Gründe, warum eine solche Maßnahme ergriffen werden muss.
6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats die Mitglieder des Datenschutzausschusses und die Kommission über zweckdienliche Informationen, die ihm zugegangen sind. Soweit erforderlich stellt der Vorsitz des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung.
7. Wenn der Europäische Datenschutzausschuss dies mit der einfachen Mehrheit seiner Mitglieder entscheidet oder eine Aufsichtsbehörde oder die Kommission dies binnen einer Woche nach Übermittlung der zweckdienlichen Informationen nach Absatz 5 beantragen, gibt der Europäische Datenschutzausschuss eine Stellungnahme zu der Angelegenheit ab. Die Stellungnahme wird binnen einem Monat mit der einfachen Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet je nach Fall die in Absatz 1 oder Absatz 3 genannte Aufsichtsbehörde, die Kommission und die gemäß Artikel 51 zuständige Aufsichtsbehörde unverzüglich über die Stellungnahme und veröffentlicht sie.
8. Die in Absatz 1 genannte Aufsichtsbehörde und die gemäß Artikel 51 zuständige Aufsichtsbehörde tragen der Stellungnahme des Europäischen Datenschutzausschusses Rechnung und teilen dessen Vorsitz und der Kommission binnen zwei Wochen nach ihrer Unterrichtung über die Stellungnahme elektronisch unter Verwendung eines standardisierten Formats mit, ob sie die geplante Maßnahme beibehält oder ändert; gegebenenfalls übermittelt sie die geänderte geplante Maßnahme.

*Artikel 59*  
***Stellungnahme der Kommission***

1. Binnen zehn Wochen, nachdem eine Angelegenheit nach Artikel 58 vorgebracht wurde, oder spätestens binnen sechs Wochen im Fall des Artikels 61, kann die Kommission hierzu eine Stellungnahme abgeben, um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung sicherzustellen.
2. Hat die Kommission eine Stellungnahme gemäß Absatz 1 angenommen, so trägt die betroffene Aufsichtsbehörde dieser so weit wie möglich Rechnung und teilt der Kommission und dem Europäischen Datenschutzausschuss mit, ob sie ihre geplante Maßnahme beizubehalten oder abzuändern beabsichtigt.
3. Während des in Absatz 1 genannten Zeitraums erlässt die Aufsichtsbehörde nicht die geplante Maßnahme.
4. Beabsichtigt die Aufsichtsbehörde, der Stellungnahme der Kommission nicht zu folgen, teilt sie dies der Kommission und dem Europäischen Datenschutzausschuss innerhalb des in Absatz 1 genannten Zeitraums mit und begründet dies. In diesem



Fall darf die geplante Maßnahme während eines weiteren Monats nicht angenommen werden.

#### *Artikel 60*

#### ***Aussetzung einer geplanten Maßnahme***

1. Binnen einem Monat nach der Mitteilung nach Artikel 59 Absatz 4 kann die Kommission, wenn sie ernsthaft bezweifelt, dass die geplante Maßnahme die ordnungsgemäße Anwendung dieser Verordnung sicherstellt, oder befürchtet, dass sie zu einer uneinheitlichen Anwendung der Verordnung führt, unter Berücksichtigung der Stellungnahme des Europäischen Datenschutzausschusses gemäß Artikel 58 Absatz 7 oder Artikel 61 Absatz 2 einen begründeten Beschluss erlassen, mit dem die Aufsichtsbehörde aufgefordert wird, die Annahme der geplanten Maßnahme auszusetzen, sofern dies erforderlich ist, um
  - a) voneinander abweichende Meinungen der Aufsichtsbehörde und des Europäischen Datenschutzausschusses miteinander in Einklang zu bringen, falls dies möglich erscheint oder
  - b) eine Maßnahme gemäß Artikel 62 Absatz 1 Buchstabe zu erlassen.
2. Die Kommission legt fest, wie lange die Maßnahme ausgesetzt wird, wobei die Aussetzung 12 Wochen nicht überschreiten darf.
3. Während des in Absatz 2 genannten Zeitraums darf die Aufsichtsbehörde die geplante Maßnahme nicht annehmen.

#### *Artikel 61*

#### ***Dringlichkeitsverfahren***

1. Unter außergewöhnlichen Umständen kann eine Aufsichtsbehörde abweichend vom Verfahren nach Artikel 58 sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer treffen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um die Interessen von betroffenen Personen, vor allem, wenn die Durchsetzung ihrer Rechte durch eine Veränderung der bestehenden Lage erheblich behindert zu werden droht, zu schützen, um größere Nachteile abzuwenden oder aus anderen Gründen. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission unverzüglich unter Angabe aller Gründe von diesen Maßnahmen 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, auch für die Dringlichkeit der endgültigen Maßnahmen, im Dringlichkeitsverfahren um eine Stellungnahme des Europäischen Datenschutzausschusses ersuchen.
3. Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme ersuchen, wenn die zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine

geeignete Maßnahme getroffen hat, um die Interessen von betroffenen Personen zu schützen.

4. Abweichend von Artikel 58 Absatz 7 wird die Stellungnahme im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen durch einfache Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen.

#### *Artikel 62* **Durchführungsrechtsakte**

1. Die Kommission kann zu folgenden Zwecken Durchführungsrechtsakte erlassen:
  - a) Beschluss über die ordnungsgemäße Anwendung dieser Verordnung gemäß ihren Zielen und Anforderungen im Hinblick auf Angelegenheiten, die ihr gemäß Artikel 58 oder Artikel 61 von einer Aufsichtsbehörde übermittelt wurden, zu denen gemäß Artikel 60 Absatz 1 ein begründeter Beschluss erlassen wurde oder zu denen eine Aufsichtsbehörde keine geplante Maßnahme übermittelt und mitgeteilt hat, dass sie der Stellungnahme der Kommission gemäß Artikel 59 nicht zu folgen beabsichtigt,
  - b) Beschluss innerhalb des in Artikel 59 Absatz 1 genannten Zeitraums darüber, ob Standard-Datenschutzklauseln nach Artikel 58 Absatz 2 Buchstabe d allgemeine Gültigkeit zuerkannt wird,
  - c) Festlegung der Form und der Verfahren für die Anwendung des in diesem Abschnitt beschriebenen Kohärenzverfahrens,
  - d) Festlegung der Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere des standardisierten Formats nach Artikel 58 Absätze 5, 6 und 8.

Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

2. In hinreichend begründeten Fällen äußerster Dringlichkeit im Zusammenhang mit den Interessen betroffener Personen gemäß Absatz 1 Buchstabe a erlässt die Kommission gemäß dem Verfahren von Artikel 87 Absatz 3 sofort geltende Durchführungsrechtsakte. Diese gelten für einen Zeitraum von höchstens 12 Monaten.
3. Unabhängig davon, ob die Kommission eine Maßnahme nach Maßgabe dieses Abschnitts erlassen hat, kann sie auf der Grundlage der Verträge andere Maßnahmen erlassen.

*Artikel 63*  
**Durchsetzung**

1. Für die Zwecke dieser Verordnung wird eine durchsetzbare Maßnahme der Aufsichtsbehörde eines Mitgliedstaats in allen anderen betroffenen Mitgliedstaaten durchgesetzt.
2. Nimmt eine Aufsichtsbehörde für eine geplante Maßnahme entgegen Artikel 58 Absätze 1 bis 5 nicht das Kohärenzverfahren in Anspruch, so ist die Maßnahme der Aufsichtsbehörde nicht rechtsgültig und durchsetzbar.

**ABSCHNITT 3**  
**EUROPÄISCHER DATENSCHUTZAUSSCHUSS**

*Artikel 64*  
**Europäischer Datenschutzausschuss**

1. Hiermit wird ein Europäischer Datenschutzausschuss eingerichtet.
2. Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten.
3. Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Richtlinie erlassenen Vorschriften zuständig, so wird der Leiter einer dieser Aufsichtsbehörden zum gemeinsamen Vertreter ernannt.
4. Die Kommission ist berechtigt, an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen und bestimmt einen Vertreter. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die Kommission unverzüglich von allen Tätigkeiten des Europäischen Datenschutzausschusses.

*Artikel 65*  
**Unabhängigkeit**

1. Der Europäische Datenschutzausschuss handelt bei der Erfüllung seiner Aufgaben gemäß den Artikeln 66 und 67 unabhängig.
2. Unbeschadet der Ersuchen der Kommission gemäß Artikel 66 Absatz 1 Buchstabe b und Artikel 67 Absatz 2 ersucht der Europäische Datenschutzausschuss bei der Erfüllung seiner Aufgaben weder um Weisung noch nimmt er Weisungen entgegen.

*Artikel 66*  
**Aufgaben des Europäischen Datenschutzausschusses**

1. Der Europäische Datenschutzausschuss stellt sicher, dass diese Verordnung einheitlich angewandt wird. Zu diesem Zweck geht der Europäische

Datenschutzausschuss von sich aus oder auf Ersuchen der Kommission insbesondere folgenden Tätigkeiten nach:

- a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, darunter auch etwaige Vorschläge zur Änderung dieser Verordnung;
  - b) von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission vorgenommene Prüfung von die Anwendung dieser Verordnung betreffenden Fragen und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Praktiken für die Aufsichtsbehörden zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;
  - c) Überprüfung der praktischen Anwendung der unter Buchstabe b genannten Leitlinien, Empfehlungen und bewährten Praktiken und regelmäßige Berichterstattung über diese an die Kommission;
  - d) Abgabe von Stellungnahmen zu Beschlussentwürfen von Aufsichtsbehörden gemäß dem in Artikel 57 genannten Kohärenzverfahren;
  - e) Förderung der Zusammenarbeit und eines effizienten bilateralen und multilateralen Austausches von Informationen und Praktiken zwischen den Aufsichtsbehörden;
  - f) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit Aufsichtsstellen internationaler Organisationen;
  - g) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und –praktiken mit Datenschutzaufsichtsbehörden in aller Welt.
2. Die Kommission kann, wenn sie den Europäischen Datenschutzausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist setzen.
  3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken an die Kommission und an den in Artikel 87 genannten Ausschuss weiter und veröffentlicht sie.
  4. Die Kommission setzt den Europäischen Datenschutzausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die vom Europäischen Datenschutzausschuss herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken ergriffen hat.

#### *Artikel 67* **Berichterstattung**

1. Der Europäische Datenschutzausschuss informiert die Kommission regelmäßig und zeitnah über die Ergebnisse seiner Tätigkeiten. Er erstellt einen jährlichen Bericht

über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union und in Drittländern.

Der Bericht enthält eine Überprüfung der praktischen Anwendung der in Artikel 66 Absatz 1 Buchstabe c genannten Leitlinien, Empfehlungen und bewährten Praktiken.

2. Der Bericht wird veröffentlicht und dem Europäischen Parlament, dem Rat und der Kommission übermittelt.

### ***Artikel 68*** ***Verfahrensweise***

1. Der Europäische Datenschutzausschuss trifft seine Beschlüsse mit der einfachen Mehrheit seiner Mitglieder.
2. Der Europäische Datenschutzausschuss gibt sich eine Geschäftsordnung und legt seine Arbeitsweise fest. Er sieht insbesondere vor, dass bei Ablauf der Amtszeit oder Rücktritt eines seiner Mitglieder die Aufgaben kontinuierlich weiter erfüllt werden, dass für spezifische Fragen oder Sektoren Untergruppen eingesetzt werden, und dass seine Verfahrensvorschriften im Einklang mit dem in Artikel 57 genannten Kohärenzverfahren stehen.

### ***Artikel 69*** ***Vorsitz***

1. Der Europäische Datenschutzausschuss wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und zwei stellvertretende Vorsitzende. Der Europäische Datenschutzbeauftragte, bekleidet, sofern er nicht zum Vorsitzenden gewählt wurde, einen der beiden Stellvertreterposten.
2. Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre Wiederwahl ist zulässig.

### ***Artikel 70*** ***Aufgaben des Vorsitzenden***

1. Der Vorsitzende hat folgende Aufgaben:
  - a) Einberufung der Sitzungen des Europäischen Datenschutzausschusses und Erstellung der Tagesordnungen;
  - b) Sicherstellung einer rechtzeitigen Erfüllung der Aufgaben des Europäischen Datenschutzausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 57.
2. Der Europäische Datenschutzausschuss legt die Verteilung der Aufgaben auf den Vorsitzenden und dessen zwei Stellvertreter in seiner Geschäftsordnung fest.

*Artikel 71*  
**Sekretariat**

1. Der Europäische Datenschutzausschuss erhält ein Sekretariat. Dieses wird vom Europäischen Datenschutzbeauftragten gestellt.
2. Das Sekretariat leistet dem Europäischen Datenschutzausschuss unter Leitung von dessen Vorsitzendem analytische, administrative und logistische Unterstützung.
3. Das Sekretariat ist insbesondere verantwortlich für
  - a) das Tagesgeschäft des Europäischen Datenschutzausschusses;
  - b) die Kommunikation zwischen den Mitgliedern des Europäischen Datenschutzausschusses, seinem Vorsitz und der Kommission sowie die Kommunikation mit anderen Organen und mit der Öffentlichkeit;
  - c) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation;
  - d) die Übersetzung sachdienlicher Informationen;
  - e) die Vor- und Nachbereitung der Sitzungen des Europäischen Datenschutzausschusses;
  - f) Vorbereitung, Entwurf und Veröffentlichung von Stellungnahmen und sonstigen vom Europäischen Datenschutzausschuss angenommenen Dokumenten.

*Artikel 72*  
**Vertraulichkeit**

1. Die Beratungen des Europäischen Datenschutzausschusses sind vertraulich.
2. Den Mitgliedern des Europäischen Datenschutzausschusses, Sachverständigen und den Vertretern von Dritten vorgelegte Dokumente sind vertraulich, sofern sie nicht gemäß der Verordnung (EG) Nr. 1049/2001 offengelegt oder auf andere Weise vom Europäischen Datenschutzausschuss der Öffentlichkeit zugänglich gemacht werden.
3. Die Mitglieder des Europäischen Datenschutzausschusses, die Sachverständigen und die Vertreter von Dritten beachten die Verpflichtung zur Wahrung der Vertraulichkeit gemäß diesem Artikel. Der Vorsitzende stellt sicher, dass die Sachverständigen und die Vertreter von Dritten von der ihnen auferlegten Vertraulichkeitspflicht in Kenntnis gesetzt werden.

## **KAPITEL VIII**

### **RECHTSBEHELFE, HAFTUNG UND SANKTIONEN**

#### *Artikel 73*

#### ***Recht auf Beschwerde bei einer Aufsichtsbehörde***

1. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.
2. Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, haben das Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte infolge der Verarbeitung personenbezogener Daten verletzt wurden.
3. Unabhängig von der Beschwerde einer betroffenen Person haben Einrichtungen, Organisationen oder Verbände im Sinne des Absatzes 2 das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht sind, dass der Schutz personenbezogener Daten verletzt wurde.

#### *Artikel 74*

#### ***Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde***

1. Jede natürliche oder juristische Person hat das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde.
2. Jede betroffene Person hat das Recht auf einen gerichtlichen Rechtsbehelf, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden, wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist oder wenn die Aufsichtsbehörde sie nicht gemäß Artikel 52 Absatz 1 Buchstabe b innerhalb von drei Monaten über den Stand oder das Ergebnis der 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. Eine betroffene Person, die von einer Entscheidung einer Aufsichtsbehörde betroffen ist, die ihren Sitz in einem anderen Mitgliedstaat hat als dem, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, kann die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen, in ihrem Namen gegen die zuständige Aufsichtsbehörde in dem anderen Mitgliedstaat Klage zu erheben.

5. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.

#### *Artikel 75*

#### ***Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter***

1. Jede natürliche Person hat unbeschadet eines verfügbaren administrativen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 73 das Recht auf einen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden.
2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung 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 gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.
3. Ist dieselbe Maßnahme, Entscheidung oder Vorgehensweise Gegenstand des Kohärenzverfahrens gemäß Artikel 58, kann das Gericht das Verfahren, mit dem es befasst wurde, aussetzen, es sei denn, es ist aufgrund der Dringlichkeit des Schutzes der Rechte der betroffenen Person nicht möglich, den Ausgang des Kohärenzverfahrens abzuwarten.
4. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.

#### *Artikel 76*

#### ***Gemeinsame Vorschriften für Gerichtsverfahren***

1. Einrichtungen, Organisationen oder Verbände im Sinne des Artikels 73 Absatz 2 haben das Recht, die in Artikel 74 und 75 genannten Rechte im Namen einer oder mehrerer betroffenen Personen wahrzunehmen.
2. Jede Aufsichtsbehörde hat das Recht, Klage zu erheben, um die Bestimmungen dieser Verordnung durchzusetzen oder um einen einheitlichen Schutz der personenbezogenen Daten innerhalb der Union sicherzustellen.
3. Hat ein zuständiges mitgliedstaatliches Gericht Grund zu der Annahme, dass in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist, setzt es sich mit dem zuständigen Gericht in diesem anderen Mitgliedstaat in Verbindung, um sich zu vergewissern, ob ein solches Parallelverfahren besteht.
4. Betrifft das Parallelverfahren in dem anderen Mitgliedstaat dieselbe Maßnahme, Entscheidung oder Vorgehensweise, kann das Gericht sein Verfahren aussetzen.



5. Die Mitgliedstaaten stellen sicher, dass mit den nach innerstaatlichem Recht verfügbaren Klagemöglichkeiten rasch Maßnahmen einschließlich einstweilige Maßnahmen erwirkt werden können, um mutmaßliche Rechtsverletzungen abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht.

#### *Artikel 77*

#### ***Haftung und Recht auf Schadenersatz***

1. Jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit dieser Verordnung nicht zu vereinbarenden Handlung ein Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.
2. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter gesamtschuldnerisch für den gesamten Schaden.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.

#### *Artikel 78*

#### ***Sanktionen***

1. Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen diese Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen; dies gilt auch für den Fall, dass der für die Verarbeitung Verantwortliche seiner Pflicht zur Benennung eines Vertreters nicht nachgekommen ist. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.
2. Hat der für die Verarbeitung Verantwortliche einen Vertreter benannt, wirken die Sanktionen gegen den Vertreter unbeschadet etwaiger Sanktionen, die gegen den für die Verarbeitung Verantwortlichen verhängt werden könnten.
3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

#### *Artikel 79*

#### ***Verwaltungsrechtliche Sanktionen***

1. Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen.
2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Die Höhe der Geldbuße bemisst sich nach

der Art, Schwere und Dauer des Verstoßes, seinem vorsätzlichen oder fahrlässigen Charakter, dem Grad der Verantwortung der natürlichen oder juristischen Person und früheren Verstößen dieser Person, den nach Artikel 23 eingeführten technischen und organisatorischen Maßnahmen und Verfahren und dem Grad der Zusammenarbeit mit der Aufsichtsbehörde zur Abstellung des Verstoßes.

3. Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen in Fällen, in denen
  - (a) eine natürliche Person personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeitet oder
  - (b) ein Unternehmen oder eine Organisation mit weniger als 250 Beschäftigten personenbezogene Daten nur als Nebentätigkeit zusätzlich zu den Haupttätigkeiten verarbeitet.
4. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 250 000 EUR oder im Fall eines Unternehmens bis in Höhe von 0,5 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig
  - (a) keine Vorkehrungen für Anträge betroffener Personen gemäß Artikel 12 Absätze 1 und 2 trifft oder den Betroffenen nicht unverzüglich oder nicht dem verlangten Format entsprechend antwortet;
  - (b) unter Verstoß gegen Artikel 12 Absatz 4 eine Gebühr für die Auskunft oder die Beantwortung von Anträgen betroffener Personen verlangt.
5. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 500 000 EUR oder im Fall eines Unternehmens bis in Höhe von 1 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig
  - (a) der betroffenen Person die Auskünfte gemäß Artikel 11, Artikel 12 Absatz 3 und Artikel 14 nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise erteilt;
  - (b) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt, personenbezogene Daten nicht gemäß Artikel 16 berichtigt oder einen Empfänger nicht gemäß Artikel 13 benachrichtigt;
  - (c) das Recht auf Vergessenwerden oder auf Löschung nicht beachtet, keine Vorkehrungen trifft, um die Einhaltung der Fristen zu gewährleisten, oder nicht alle erforderlichen Schritte unternimmt, um Dritte von einem Antrag der betroffenen Person auf Löschung von Links zu personenbezogenen Daten sowie Kopien oder Replikationen dieser Daten gemäß Artikel 17 zu benachrichtigen;
  - (d) keine Kopie der personenbezogenen Daten in elektronischem Format bereitstellt oder die betroffene Person unter Verstoß gegen Artikel 18 daran hindert, personenbezogene Daten auf eine andere Anwendung zu übertragen;
  - (e) die jeweilige Verantwortung der für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt hat;

- (f) die Dokumentation gemäß Artikel 28, Artikel 31 Absatz 4 und Artikel 44 Absatz 3 nicht oder nicht hinreichend gewährleistet;
  - (g) in Fällen, in denen keine besonderen Kategorien von Daten verarbeitet werden, die Vorschriften im Hinblick auf die freie Meinungsäußerung gemäß Artikel 80, die Datenverarbeitung im Beschäftigungskontext gemäß Artikel 82 oder die Bedingungen für die Verarbeitung zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83 nicht beachtet.
6. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 1 000 000 EUR oder im Fall eines Unternehmens bis in Höhe von 2 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig
- (a) personenbezogene Daten ohne oder ohne ausreichende Rechtsgrundlage verarbeitet oder die Bedingungen für die Einwilligung gemäß den Artikeln 6, 7 und 8 nicht beachtet;
  - (b) unter Verstoß gegen die Artikel 9 und 81 besondere Kategorien von Daten verarbeitet;
  - (c) das Recht auf Widerspruch gemäß Artikel 19 oder eine damit verbundene Bedingung nicht beachtet;
  - (d) die Bedingungen gemäß Artikel 20 in Bezug auf Maßnahmen, die auf Profiling basieren, nicht beachtet;
  - (e) keine internen Datenschutzstrategien festlegt oder keine geeigneten Maßnahmen gemäß den Artikeln 22, 23 und 30 anwendet, um die Beachtung der Datenschutzvorschriften sicherzustellen und nachzuweisen;
  - (f) keinen Vertreter gemäß Artikel 25 benennt;
  - (g) unter Verstoß gegen die mit der Datenverarbeitung im Namen eines für die Verarbeitung Verantwortlichen verbundenen Pflichten gemäß den Artikeln 26 und 27 personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;
  - (h) die Aufsichtsbehörde bei einer Verletzung des Schutzes personenbezogener Daten nicht alarmiert oder sie oder die betroffene Person gemäß den Artikeln 31 und 32 nicht oder nicht rechtzeitig oder nicht vollständig von einer solchen Verletzung benachrichtigt;
  - (i) keine Datenschutz-Folgenabschätzung nach Artikel 33 vornimmt oder personenbezogene Daten entgegen Artikel 34 ohne vorherige Genehmigung oder ohne Zuziehung der Aufsichtsbehörde verarbeitet;
  - (j) keinen Datenschutzbeauftragten nach Artikel 35 benennt oder nicht die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 35, 36 und 37 schafft;
  - (k) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht;

- (l) eine mangels eines Angemessenheitsbeschlusses oder mangels geeigneter Garantien oder einer Ausnahme gemäß den Artikeln 40 bis 44 unzulässige Datenübermittlung in ein Drittland oder an eine internationale Organisation vornimmt oder anordnet;
  - (m) einer Anweisung oder einem vorübergehenden oder endgültigen Verarbeitungsverbot oder einer Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1 nicht Folge leistet;
  - (n) entgegen den Pflichten gemäß Artikel 28 Absatz 3, Artikel 29, Artikel 34 Absatz 6 und Artikel 53 Absatz 2 die Aufsichtsbehörde nicht unterstützt, nicht mit ihr zusammenarbeitet, ihre keine einschlägigen Auskünfte erteilt oder keinen Zugang zu seinen Räumlichkeiten gewährt;
  - (o) die Vorschriften über die Wahrung des Berufsgeheimnisses gemäß Artikel 84 nicht einhält.
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Beträge der in den Absätzen 4, 5 und 6 genannten Geldbußen unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien zu aktualisieren.

## **KAPITEL IX VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN**

### *Artikel 80*

#### ***Verarbeitung personenbezogener Daten und freie Meinungsäußerung***

1. Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen oder Ausnahmen von den allgemeinen Grundsätzen des Kapitels II, von den Rechten der betroffenen Person in Kapitel III, von den Bestimmungen über den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter in Kapitel IV, von der Übermittlung personenbezogener Daten in Drittländer und an internationale Organisationen in Kapitel V, von den Vorschriften über die Aufsichtsbehörden in Kapitel VI sowie von den Vorschriften über Zusammenarbeit und Kohärenz in Kapitel VII vor, um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.
2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlassen hat, und setzt sie unverzüglich von allen weiteren Änderungsgesetzen oder diese Rechtsvorschriften betreffenden Änderungen in Kenntnis.

*Artikel 81*  
**Verarbeitung personenbezogener Gesundheitsdaten**

1. Die Verarbeitung personenbezogener Gesundheitsdaten erfolgt in den Grenzen dieser Verordnung nach Maßgabe von Artikel 9 Absatz 2 Buchstabe h auf der Grundlage des Unionsrechts oder des mitgliedstaatlichen Rechts, das geeignete, besondere Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht; sie muss notwendig sein
  - a) für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten, sofern die Verarbeitung dieser Daten durch dem Berufsgeheimnis unterliegendes ärztliches Personal erfolgt oder durch sonstige Personen, die nach mitgliedstaatlichem Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, einer entsprechenden Geheimhaltungspflicht unterliegen;
  - b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit unter anderem zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards unter anderem für Arzneimittel oder Medizinprodukte oder
  - c) aus anderen Gründen des öffentlichen Interesses in Bereichen wie der sozialen Sicherheit, insbesondere um die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sicherzustellen.
2. Die Verarbeitung personenbezogener Gesundheitsdaten, die zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung unter anderem zur Erstellung von Patientenregistern zur Verbesserung der Diagnose sowie zur Unterscheidung zwischen ähnlichen Krankheitsarten und zur Vorbereitung von Studien zu Therapiezielen erforderlich ist, unterliegt den Bedingungen und Garantien gemäß Artikel 83.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit im Sinne des Absatzes 1 Buchstabe b näher auszuführen und um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.

*Artikel 82*  
**Datenverarbeitung im Beschäftigungskontext**

1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung per Gesetz die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext unter anderem für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, 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 regeln.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.

### *Artikel 83*

#### ***Datenverarbeitung zu historischen oder statistischen Zwecken sowie zum Zwecke der wissenschaftlichen Forschung***

1. In den Grenzen dieser Verordnung dürfen personenbezogene Daten nur dann zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung verarbeitet werden, wenn
  - a) diese Zwecke nicht auf andere Weise durch die Verarbeitung von Daten erfüllt werden können, die eine Bestimmung der betroffenen Person nicht oder nicht mehr ermöglichen;
  - b) Daten, die die Zuordnung von Informationen zu einer bestimmten oder bestimmbar betroffenen Person ermöglichen, von den übrigen Informationen getrennt aufbewahrt werden, sofern diese Zwecke in dieser Weise erfüllt werden können.
2. Einrichtungen, die Arbeiten für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung durchführen, dürfen personenbezogene Daten nur dann veröffentlichen oder auf andere Weise bekannt machen, wenn
  - a) die betroffene Person nach Maßgabe von Artikel 7 ihre Einwilligung erteilt hat,
  - b) die Veröffentlichung personenbezogener Daten für die Darstellung von Forschungsergebnissen oder zur Unterstützung der Forschung notwendig ist, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person diese Interessen nicht überwiegen oder
  - c) die betroffene Person die Daten veröffentlicht hat.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verarbeitung personenbezogener Daten für die Zwecke der Absätze 1 und 2, etwaige erforderliche Beschränkungen der Rechte der betroffenen Person auf Unterrichtung und Auskunft sowie die unter diesen Umständen geltenden Bedingungen und Garantien für die Rechte der betroffenen Person festzulegen.

*Artikel 84*  
**Geheimhaltungspflichten**

1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung die Untersuchungsbefugnisse der Aufsichtsbehörden im Sinne des Artikels 53 Absatz 2 gegenüber den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeitern, die nach einzelstaatlichem Recht oder nach von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen 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 für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.
2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Vorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

*Artikel 85*  
**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 personenbezogener Daten an, 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, richten eine unabhängige Datenschutzaufsicht im Sinne des Kapitels VI ein.

**KAPITEL X**  
**DELEGIERTE RECHTSAKTE UND**  
**DURCHFÜHRUNGSRECHTSAKTE**

*Artikel 86*  
**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 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35

Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 wird der Kommission auf unbestimmte Zeit ab Inkrafttreten dieser Verordnung übertragen.

3. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35 Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Der Beschluss wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Er berührt nicht die Gültigkeit von bereits in Kraft getretenen delegierten Rechtsakten.
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 6 Absatz 5, Artikel 8 Absatz 3, Artikel 9 Absatz 3, Artikel 12 Absatz 5, Artikel 14 Absatz 7, Artikel 15 Absatz 3, Artikel 17 Absatz 9, Artikel 20 Absatz 6, Artikel 22 Absatz 4, Artikel 23 Absatz 3, Artikel 26 Absatz 5, Artikel 28 Absatz 5, Artikel 30 Absatz 3, Artikel 31 Absatz 5, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 34 Absatz 8, Artikel 35 Absatz 11, Artikel 37 Absatz 2, Artikel 39 Absatz 2, Artikel 43 Absatz 3, Artikel 44 Absatz 7, Artikel 79 Absatz 6, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 erlassen worden ist, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb von zwei Monaten nach Übermittlung des Rechtsakts Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

#### *Artikel 87*

#### ***Ausschussverfahren***

1. Die Kommission wird von einem Ausschuss unterstützt. Bei diesem Ausschuss handelt es sich um einen 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 88* ***Aufhebung der Richtlinie 95/46/EG***

1. Die Richtlinie 95/46/EG wird 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 89* ***Verhältnis zur Richtlinie 2002/58/EG und Änderung dieser Richtlinie***

1. Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten 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 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.
2. Artikel 1 Absatz 2 der Richtlinie 2002/58/EG wird gestrichen.

#### *Artikel 90* ***Bewertung***

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht zur Bewertung und Überprüfung dieser Verordnung vor. Der erste Bericht wird spätestens vier Jahre nach Inkrafttreten dieser Verordnung vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Die Kommission legt geeignete Vorschläge zur Änderung dieser Verordnung und zur Anpassung anderer Rechtsinstrumente vor, die sich insbesondere unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen können. Die Berichte werden veröffentlicht.

*Artikel 91*  
***Inkrafttreten und Anwendung***

1. Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.
2. Ihre Anwendung beginnt [*zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt*].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am

*Im Namen des Europäischen Parlaments*  
*Der Präsident*

*Im Namen des Rates*  
*Der Präsident*

## FINANZBOGEN ZU RECHTSAKTEN

### **1. RAHMEN DES VORSCHLAGS/DER INITIATIVE**

- 1.1. Bezeichnung des Vorschlags/der Initiative
- 1.2. Politikbereiche in der ABM/ABB-Struktur
- 1.3. Art des Vorschlags/der Initiative
- 1.4. Ziele
- 1.5. Begründung des Vorschlags/der Initiative
- 1.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen
- 1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

### **2. VERWALTUNGSMASSNAHMEN**

- 2.1. Monitoring und Berichterstattung
- 2.2. Verwaltungs- und Kontrollsystem
- 2.3. Prävention von Betrug und Unregelmäßigkeiten

### **3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE**

- 3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n):
- 3.2. Geschätzte Auswirkungen auf die Ausgaben
  - 3.2.1. *Übersicht*
  - 3.2.2. *Geschätzte Auswirkungen auf die operativen Mittel*
  - 3.2.3. *Geschätzte Auswirkungen auf die Verwaltungsmittel*
  - 3.2.4. *Vereinbarkeit mit dem mehrjährigen Finanzrahmen*
  - 3.2.5. *Finanzierungsbeitrag Dritter*
- 3.3. Geschätzte Auswirkungen auf die Einnahmen

## FINANZBOGEN ZU RECHTSAKTEN

### **1. RAHMEN DES VORSCHLAGS/DER INITIATIVE**

In diesem Finanzbogen wird der Bedarf an Verwaltungsmitteln für die Datenschutzreform, wie in der dazugehörigen Folgenabschätzung dargelegt, genauer aufgeführt. Das Reformpaket umfasst zwei Vorschläge für Rechtsakte, eine allgemeine Datenschutzverordnung und eine Richtlinie 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. Der Finanzbogen behandelt die Auswirkungen beider Rechtsakte auf den Haushalt.

Je nach Aufgabenverteilung benötigen Kommission und Europäischer Datenschutzbeauftragter (EDSB) Ressourcen.

Die Kommission hat die notwendigen Ressourcen bereits in ihrem Entwurf der Finanziellen Vorausschau 2014-2020 berücksichtigt. Der Datenschutz ist eines der Ziele des Programms „Grundrechte und Unionsbürgerschaft“, durch das auch Maßnahmen zur praktischen Umsetzung des Rechtsrahmens gefördert werden sollen. Die Verwaltungsmittel einschließlich des Personalbedarfs sind im Verwaltungshaushalt der GD JUST eingeplant.

Der EDSB wird den Mittelbedarf in seinen jeweiligen Jahreshaushaltsplänen veranschlagen müssen. Die Mittel sind im Anhang zu diesem Finanzbogen aufgeschlüsselt. Um die notwendigen Mittel für die neuen Aufgaben des Europäischen Datenschutzausschusses, für den der EDSB das Sekretariat übernimmt, bereitstellen zu können, muss Rubrik 5 der Finanziellen Vorausschau 2014-2020 angepasst werden.

#### **1.1. Bezeichnung des Vorschlags/der Initiative**

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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

#### **1.2. Politikbereiche in der ABM/ABB-Struktur<sup>49</sup>**

Justiz – Schutz personenbezogener Daten

---

<sup>49</sup> ABM: Activity Based Management: maßnahmenbezogenes Management – ABB: Activity Based Budgeting: maßnahmenbezogene Budgetierung.

Die Vorschläge wirken sich auf die Haushalte der Kommission und des EDSB aus. Die Einzelheiten zu den Auswirkungen auf den Kommissionshaushalt sind den Tabellen dieses Finanzbogens zu entnehmen. Die operativen Ausgaben werden aus dem Programm „Grundrechte und Unionsbürgerschaft“ finanziert und sind im Finanzbogen zu diesem Programm bereits aufgeführt. Die Verwaltungsausgaben werden aus dem Haushalt der GD Justiz finanziert. Die Posten, die den EDSB betreffen, sind im Anhang aufgeführt.

### 1.3. Art des Vorschlags/der Initiative

- Der Vorschlag/die Initiative betrifft eine **neue Maßnahme**.
- Der Vorschlag/die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**.<sup>50</sup>
- Der Vorschlag/die Initiative betrifft die **Verlängerung einer bestehenden Maßnahme**.
- Der Vorschlag/die Initiative betrifft **eine neu ausgerichtete Maßnahme**.

### 1.4. Ziele

#### 1.4.1. *Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission*

Mit der Reform sollen die ursprünglichen Ziele unter Berücksichtigung neuer Entwicklungen und Herausforderungen vollständig umgesetzt werden, d. h.:

- Stärkung der Wirksamkeit des Grundrechts auf Datenschutz und Übertragung der Kontrolle über die Daten an die Betroffenen, insbesondere vor dem Hintergrund der technologischen Entwicklungen und zunehmenden Globalisierung;
- Vertiefung der Binnenmarktdimension des Datenschutzes durch Abbau der Unterschiede in den Regelungen, Verstärkung der Kohärenz und Vereinfachung des Regelungsumfelds, damit unnötige Kosten vermieden werden und der Verwaltungsaufwand verringert wird.

Darüber hinaus ermöglicht das Inkrafttreten des Vertrags von Lissabon – besonders die Einführung einer neuen Rechtsgrundlage (Artikel 16 AEUV) – die Umsetzung eines neuen Ziels:

- Einführung einer umfassenden Regelung zum Schutz personenbezogener Daten, die für sämtliche Bereiche gleichermaßen gilt.

---

<sup>50</sup> Im Sinne von Artikel 49 Absatz 6 Buchstabe a oder b der Haushaltsordnung.

1.4.2. *Einzelziele und ABM/ABB-Tätigkeiten*

Einzelziel Nr. 1

Gewährleistung einer einheitlichen Durchsetzung der Datenschutzvorschriften

Einzelziel Nr. 2

Straffung des derzeitigen Verwaltungssystems zur Förderung einer einheitlicheren Durchsetzung

ABM/ABB-Tätigkeiten

[...]

### 1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppe auswirken dürfte.

Hinsichtlich der für die Datenverarbeitung Verantwortlichen werden sowohl die öffentlichen Stellen als auch der private Sektor von der erheblichen Reduzierung des Verwaltungsaufwands und von harmonisierten und klareren EU-Datenschutzregeln und -verfahren profitieren, die gleiche Wettbewerbsbedingungen und die einheitliche Durchsetzung der Regeln gewährleisten.

Der Einzelne wird mehr Kontrolle über seine personenbezogenen Daten und mehr Vertrauen in die digitale Umgebung haben und wird weiterhin, auch bei der Verarbeitung seiner personenbezogenen Daten im Ausland, geschützt sein. Er wird darüber hinaus von einer verstärkten Rechenschaftspflicht der mit der Verarbeitung personenbezogener Daten Befassten profitieren.

Eine umfassende Datenschutzregelung wird auch die Bereiche Polizei und Justiz erfassen, darunter den Bereich der ehemaligen dritten Säule, über den sie hinausgehen wird.

### 1.4.4. Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

(Siehe Folgenabschätzung, Abschnitt 8)

Die Indikatoren werden regelmäßig überprüft und umfassen folgende Elemente:

- Zeit- und Kostenaufwand der für die Datenverarbeitung Verantwortlichen im Zusammenhang mit der Einhaltung der Vorschriften „in anderen Mitgliedstaaten“
- den Datenschutzbehörden zugewiesene Mittel
- Zahl der Datenschutzbeauftragten in öffentlichen und privaten Organisationen/Unternehmen,
- Durchführung von Datenschutz-Folgenabschätzungen
- Zahl der Beschwerden seitens betroffener Personen und an sie geleisteter Schadenersatz
- Zahl der Sachen, in denen eine strafrechtliche Verfolgung des für die Verarbeitung Verantwortlichen eingeleitet wird
- Geldstrafen, die wegen Datenschutzverletzungen gegen für die Verarbeitung Verantwortliche verhängt werden.

## 1.5. Begründung des Vorschlags/der Initiative

### 1.5.1. Kurz- oder langfristig zu deckender Bedarf

Die bestehenden Unterschiede zwischen den Mitgliedstaaten bei der Umsetzung, Auslegung und Durchsetzung der Richtlinie *behindern das Funktionieren des Binnenmarktes und die*

*Zusammenarbeit zwischen den Behörden bei Maßnahmen der EU.* Diese steht dem übergeordneten Ziel der Richtlinie entgegen, das in der Erleichterung des freien Verkehrs personenbezogener Daten im Binnenmarkt besteht. Die rasante Entwicklung neuer Technologien und die Globalisierung kommen erschwerend hinzu.

Die Rechte des Einzelnen auf Datenschutz sind wegen der rechtlichen Fragmentierung und uneinheitlichen Um- und Durchsetzung in den verschiedenen Mitgliedstaaten unterschiedlich. Darüber hinaus ist sich **der Einzelne oft nicht dessen bewusst, was mit seinen personenbezogenen Daten geschieht, oder er hat keinen Einfluss darauf** und macht daher nicht wirksam von seinen Rechten Gebrauch.

#### 1.5.2. *Mehrwert durch die Intervention der EU*

Die Mitgliedstaaten können der derzeitigen Probleme im Alleingang nicht Herr werden. besonders, wenn es sich um Probleme im Zusammenhang mit der Uneinheitlichkeit der einzelstaatlichen Bestimmungen zur Umsetzung der EU-Datenschutzvorschriften handelt. Vieles spricht daher für eine Datenschutzregelung auf EU-Ebene. Es besteht ein besonderer Bedarf an einer harmonisierten, kohärenten Regelung, die einen reibungslosen Transfer personenbezogener Daten innerhalb der EU ermöglicht und gleichzeitig EU-weit allen Betroffenen einen wirksamen Datenschutz garantiert.

#### 1.5.3. *Aus früheren ähnlichen Maßnahmen gewonnene wesentliche Erkenntnisse*

Die vorliegenden Vorschläge bauen auf den Erfahrungen mit der Richtlinie 95/46/EG und mit den Problemen aufgrund der unterschiedlichen Um- und Durchsetzung der Richtlinie auf, die bisher verhindert haben, dass die Ziele eines hohen Datenschutzes und eines Binnenmarktes für den Datenschutz erreicht werden.

#### 1.5.4. *Kohärenz mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte*

Mit dem Datenschutz-Reformpaket soll eine solide, kohärente und moderne Datenschutzregelung auf EU-Ebene eingeführt werden, die technologieunabhängig ist und in den nächsten Jahrzehnten Bestand haben wird. Sie wird für den Einzelnen Vorteile bringen – indem die Datenschutzrechte des Einzelnen besonders in einer digitalen Umgebung gestärkt werden - und wird das rechtliche Umfeld für Unternehmen und den öffentlichen Sektor vereinfachen, was die Entwicklung der digitalen Wirtschaft im EU-Binnenmarkt und über ihn hinaus entsprechend den Zielen der Strategie Europa 2020 fördern dürfte.

Hauptbestandteile des Datenschutz-Reformpakets sind:

- eine Verordnung zur Ersetzung der Richtlinie 95/46/EG;
- eine Richtlinie 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.



Gemeinsam mit diesen Legislativvorschlägen wird ein Bericht über die Umsetzung des derzeit wichtigsten Datenschutz-Instruments der EU im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, des Rahmenbeschlusses 2008/977/JI, vorgelegt.

## 1.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen

Vorschlag/Initiative mit **befristeter Geltungsdauer**

1.  Geltungsdauer: [TT/MM]JJJJ bis [TT/MM]JJJJ

2.  Finanzielle Auswirkungen: JJJJ bis JJJJ

Vorschlag/Initiative mit **unbefristeter Geltungsdauer**

1. Umsetzung mit einer Anlaufphase von 2014 bis 2016,

2. Vollbetrieb wird angeschlossen.

## 1.7. Vorgeschlagene Methoden der Mittelverwaltung<sup>51</sup>

**Direkte zentrale Verwaltung** durch die Kommission

**Indirekte zentrale Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

3.  Exekutivagenturen

4.  von den Europäischen Gemeinschaften geschaffene Einrichtungen<sup>52</sup>

5.  nationale öffentliche Einrichtungen bzw. privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden

3.  Personen, die mit der Durchführung bestimmter Maßnahmen im Rahmen des Titels V des Vertrags über die Europäische Union betraut und in dem maßgeblichen Basisrechtsakt nach Artikel 49 der Haushaltsordnung bezeichnet sind

Mit den Mitgliedstaaten **geteilte Verwaltung**

**Dezentrale Verwaltung** mit Drittstaaten

**Gemeinsame Verwaltung** mit internationalen Organisationen (*bitte auflisten*)

*Falls mehrere Methoden der Mittelverwaltung zum Einsatz kommen, ist dies unter „Bemerkungen“ näher zu erläutern.*

Bemerkungen

//

<sup>51</sup> Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

<sup>52</sup> Einrichtungen im Sinne des Artikels 185 der Haushaltsordnung.

## 2. VERWALTUNGSMASSNAHMEN

### 2.1. Monitoring und Berichterstattung

*Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.*

Die erste Evaluierung wird vier Jahre nach Inkrafttreten der Rechtsakte vorgenommen. Die Rechtsakte enthalten eine Überprüfungs Klausel, die es der Kommission ermöglicht, die Umsetzung zu bewerten. Die Kommission wird dem Europäischen Parlament und dem Rat über die Ergebnisse der Evaluierung berichten. Die Evaluierung, die alle vier Jahre wiederholt wird, wird nach der einschlägigen Methode der Kommission vorgenommen. Dazu werden u. a. gezielte Studien zur Umsetzung der Rechtsakte, Befragungen der nationalen Datenschutzbehörden mit Hilfe von Fragebögen, Sachverständigendiskussionen, Workshops und Eurobarometer-Umfragen durchgeführt.

### 2.2. Verwaltungs- und Kontrollsystem

#### 2.2.1. Ermittelte Risiken

Zur Reform der Datenschutzregelung in der EU wurde eine Folgenabschätzung vorgenommen, die den Vorschlägen der Verordnung und der Richtlinie beigelegt sind.

Durch den neuen Rechtsakt wird ein Kohärenzverfahren eingeführt, das eine einheitliche und kohärente Anwendung der Vorschriften durch die unabhängigen Aufsichtsbehörden in den Mitgliedstaaten gewährleistet. Für die Anwendung des Verfahrens wird der Europäische Datenschutzausschuss zuständig sein, der sich aus den Leitern der nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten (EDSB) zusammensetzt. Der Datenschutzausschuss wird die bisherige Artikel-29-Datenschutzgruppe ersetzen. Der EDSB wird für den Datenschutzausschuss das Sekretariat übernehmen.

In Fällen, in denen die Behörden der Mitgliedstaaten unterschiedlich entscheiden könnten, wird der Europäische Datenschutzausschuss konsultiert, der eine Stellungnahme dazu abgibt. Führt das Verfahren zu keinem Ergebnis oder weigert sich eine Aufsichtsbehörde, der Stellungnahme Folge zu leisten, kann die Kommission eine Stellungnahme abgeben, um die ordnungsgemäße und kohärente Anwendung der Verordnung sicherzustellen, oder erforderlichenfalls einen Beschluss fassen, wenn ernsthafte Zweifel daran bestehen, dass die geplante Maßnahme die ordnungsgemäße Anwendung der Verordnung sicherstellt, oder wenn die Maßnahme zu einer unkohärenten Anwendung führen würde.

Zur Durchführung des Kohärenzverfahrens müssen dem EDSB (12 VZE and sowie entsprechende Verwaltungsmittel und operative Mittel beispielsweise für IT-Systeme und den IT-Betrieb) für seine Sekretariatsaufgaben und der Kommission (5 VZE und entsprechende Verwaltungsmittel und operative Mittel) für die Bearbeitung konkreter Kohärenzsachen zusätzliche Mittel zur Verfügung gestellt werden.

2.2.2. *Vorgesehene Kontrollen*

Die Verwaltung der zusätzlichen Mittel wird nach den üblichen Verfahren des EDSB und der Kommission kontrolliert.

**2.3. Prävention von Betrug und Unregelmäßigkeiten**

*Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.*

Die zusätzlichen Mittel werden den üblichen Betrugsbekämpfungsmaßnahmen des EDSB und der Kommission unterzogen.

### 3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

#### 3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n):

##### 1. Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Bezeichnung.....]	GM/NGM <sup>(53)</sup>	von EFTA <sup>54</sup> -Ländern	von Bewerberländern <sup>55</sup>	von Drittländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushaltsordnung

<sup>53</sup> GM=Getrennte Mittel / NGM=Nicht getrennte Mittel.

<sup>54</sup> EFTA: Europäische Freihandelsassoziation.

<sup>55</sup> Bewerberländer und gegebenenfalls potenzielle Bewerberländer des Westbalkans.

### 3.2. Geschätzte Auswirkungen auf die Ausgaben

#### 3.2.1. Übersicht

in Mio. EUR (3 Dezimalstellen)

<b>Rubrik des mehrjährigen Finanzrahmens</b>	Nummer	
--	--------	--

			Jahr N <sup>56</sup> = 2014	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			INSGESAMT
• Operative Mittel										
Nummer der Haushaltslinie	Verpflichtungen	(1)								
	Zahlungen	(2)								
Nummer der Haushaltslinie	Verpflichtungen	(1a)								
	Zahlungen	(2a)								
Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben <sup>57</sup>										
Nummer der Haushaltslinie		(3)								
<b>Mittel INSGESAMT für GD</b>	Verpflichtungen	=1+1a +3								
	Zahlungen	=2+2a +3								

<sup>56</sup> Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

<sup>57</sup> Ausgaben für technische und administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

• Operative Mittel INSGESAMT	Verpflichtungen	(4)								
	Zahlungen	(5)								
• Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)								
<b>Mittel INSGESAMT unter RUBRIK 3</b> des mehrjährigen Finanzrahmens	Verpflichtungen	=4+ 6								
	Zahlungen	=5+ 6								

**Wenn der Vorschlag/die Initiative mehrere Rubriken betrifft:**

• Operative Mittel INSGESAMT	Verpflichtungen	(4)								
	Zahlungen	(5)								
• Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)								
<b>Mittel INSGESAMT unter RUBRIKEN 1 bis 4</b> des mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4+ 6								
	Zahlungen	=5+ 6								

<b>Rubrik des mehrjährigen Finanzrahmens</b>	<b>5</b>	„Verwaltungsausgaben“
--	----------	-----------------------

in Mio. EUR (3 Dezimalstellen)

	Jahr N= 2014	Jahr 2015	Jahr 2016	Jahr 2017	Jahr 2018	Jahr 2019	Jahr 2020	INSGESAMT
GD: JUST								
• Personalausgaben	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>20,454</u>

• Sonstige Verwaltungsausgaben		<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>3,885</u>
<b>GD JUST INSGESAMT</b>		<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>

<b>Mittel INSGESAMT unter RUBRIK 5</b> des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>
--	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

in Mio. EUR (3 Dezimalstellen)

		Jahr N <sup>58</sup>	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			INSGESAMT
<b>Mittel INSGESAMT unter RUBRIKEN 1 bis 5</b> des mehrjährigen Finanzrahmens	Verpflichtungen	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>
	Zahlungen	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>

<sup>58</sup> Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.



3.2.2. *Geschätzte Auswirkungen auf die operativen Mittel*

6.  Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

Ein hoher Schutz personenbezogener Daten ist auch eines der Ziele des Programms „Grundrechte und Unionsbürgerschaft“.

7.  Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse			Jahr N=2014		Jahr N+1		Jahr N+2		Jahr N+3		Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen						INSGESAMT	
	ERGEBNISSE																	
	↓	Art der Ergebnisse <sup>59</sup>	Durchschnitts-Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl insgesamt
EINZELZIEL Nr. 1																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2																		
- Ergebnis Sachen <sup>61</sup>																		
Zwischensumme für Einzelziel Nr. 2																		

<sup>59</sup> Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z.B.: Austausch von Studenten, gebaute Straßenkilometer...).

<sup>60</sup> Stellungnahmen, Beschlüsse, Verfahrenssitzungen des Datenschutzausschusses.

<sup>61</sup> Im Rahmen des Kohärenzverfahrens behandelte Sachen.

<b>GESAMTKOSTEN</b>																	
---------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

### 3.2.3. Geschätzte Auswirkungen auf die Verwaltungsmittel

#### 3.2.3.1. Übersicht

8.  Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.
9.  Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr N <sup>62</sup> 2014	Jahr 2015	Jahr 2016	Jahr 2017	Jahr 2018	Jahr 2019	Jahr 2020	INSGE- SAMT
--	---------------------------------	--------------	-----------	-----------	-----------	-----------	-----------	----------------

<b>RUBRIK 5 des mehrjährigen Finanzrahmens</b>								
Personalausgaben	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>2,922</u>	<u>20,454</u>
Sonstige Verwaltungs- ausgaben	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>0,555</u>	<u>3,885</u>
<b>Zwischensumme RUBRIK 5 des mehrjährigen Finanzrahmens</b>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>

<b>Außerhalb der RUBRIK 5<sup>63</sup> des mehrjährigen Finanzrahmens</b>								
Personalausgaben								
Sonstige Verwaltungs- ausgaben								
<b>Zwischensumme der Mittel außerhalb der RUBRIK 5 des mehrjährigen Finanzrahmens</b>								

<sup>62</sup> Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

<sup>63</sup> Ausgaben für technische und administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

INSGESAMT	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>3,477</u>	<u>24,339</u>
-----------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

### 3.2.3.2. Geschätzter Personalbedarf

10.  Für den Vorschlag/die Initiative wird kein Personal benötigt.
11.  Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

*Schätzung (in Vollzeitäquivalenten oder mit höchstens einer Dezimalstelle)*

	Jahr 2014	Jahr 2015	Jahr 2016	Jahr 2017	Jahr 2018	Jahr 2019	Jahr 2020
<b>• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)</b>							
XX 01 01 01 (am Sitz und in den Vertretungen der Kommission)	22	22	22	22	22	22	22
XX 01 01 02 (in den Delegationen)							
<b>• Externes Personal (in Vollzeitäquivalenten = FTE)<sup>64</sup></b>							
XX 01 02 01 (AC, INT, ANS der Globaldotation)	2	2	2	2	2	2	2
XX 01 02 02 (AC, AL, JED, INT und ANS in den Delegationen)							
XX 01 04 <i>jj</i> <sup>65</sup>	- am Sitz <sup>66</sup>						
	- in den Delegationen						
XX 01 05 02 (AC, INT, ANS der indirekten Forschung)							
10 01 05 02 (AC, INT, ANS der direkten Forschung)							
Sonstige Haushaltslinien (bitte angeben)							
<b>INSGESAMT</b>	<b>24</b>	<b>24</b>	<b>24</b>	<b>24</b>	<b>24</b>	<b>24</b>	<b>24</b>

**XX** steht für den jeweiligen Haushaltstitel bzw. Politikbereich

Durch die Reform erhält die Kommission neue, zusätzliche Aufgaben im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten. Diese stehen in erster Linie mit dem neuen Kohärenzverfahren, mit dem die kohärente Anwendung der harmonisierten Datenschutzregelung, mit der Angemessenheitsprüfung für Drittländer, für die die Kommission alleine zuständig sein wird, sowie mit der Ausarbeitung von Umsetzungsmaßnahmen und delegierten Rechtsakten in Zusammenhang. Daneben wird die Kommission auch weiterhin ihre bisherigen Aufgaben wahrnehmen müssen (darunter Strategieentwicklung, Monitoring der Umsetzung, Information, Beschwerden).

Der Personalbedarf wird durch bereits der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel für Personal, die der für die Verwaltung der Maßnahme

<sup>64</sup> AC= Vertragsbediensteter, INT= Leiharbeitskraft ("Interimaire"), JED= Junger Sachverständiger in Delegationen, AL= örtlich Bediensteter, ANS= Abgeordneter Nationaler Sachverständiger.

<sup>65</sup> Teilobergrenze für aus den operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

<sup>66</sup> Insbesondere für Strukturfonds, Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und Europäischer Fischereifonds (EFF).

zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

<p>Beamte und Zeitbedienstete</p>	<p>Sachbearbeiter (Case handlers) für das Datenschutz-Kohärenzverfahren, mit dem eine einheitliche Anwendung der Datenschutzregelung der EU sichergestellt werden soll. Zu ihren Aufgaben gehören die Untersuchung von Sachen, die von einer Behörde eines Mitgliedstaats zur Entscheidung vorgelegt wurde, sowie entsprechende Nachforschungen, Verhandlungen mit den Mitgliedstaaten und Ausarbeitung eines Beschlusses der Kommission. Ausgehend von den bisherigen Erfahrungen sind jährlich etwa fünf bis zehn Sachen zu erwarten, in denen das Kohärenzverfahren eingeleitet werden muss.</p> <p>Entscheidungen in Angemessenheitsfragen erfordern die Zusammenarbeit mit dem Land, das den Antrag gestellt hat, möglicherweise die Betreuung von Sachverständigengutachten über die Bedingungen im Land, die Bewertung der Bedingungen, Ausarbeitung von Beschlüssen der Kommission und Vorbereitung des Verfahrens, einschließlich des Ausschusses zur Unterstützung der Kommission und sonstiger Expertengremien. Ausgehend von den bisherigen Erfahrungen sind jährlich bis zu 4 Anträge auf Angemessenheitsprüfung zu erwarten.</p> <p>Zur Annahme von Umsetzungsmaßnahmen müssen vorbereitende Tätigkeiten durchgeführt, beispielsweise Berichte und Untersuchungen verfasst und Konsultationen vorgenommen sowie Rechtsakte ausgearbeitet und Verhandlungen in den zuständigen Ausschüssen und Gremien geführt werden. Auch müssen allgemein die Kontakte zu den interessierten Kreisen gepflegt werden. Für diejenigen Bereiche, zu denen genauere Anweisungen nötig sind, dürften jährlich insgesamt bis zu drei Umsetzungsmaßnahmen anfallen, wobei jedes Verfahren je nach Intensität der Konsultationen bis zu 24 Monate beanspruchen könnte.</p>
<p>Externes Personal</p>	<p>Administrative Unterstützung und Sekretariat</p>

#### 3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

12.  Der Vorschlag/die Initiative ist mit dem *nächsten* mehrjährigen Finanzrahmen vereinbar.
13.  Der Vorschlag/die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Der nachstehenden Tabelle ist zusätzlich zu den bereits veranschlagten Maßnahmen der jährliche Mittelbedarf des Europäischen Datenschutzbeauftragten für seine neuen Aufgaben (Sekretariat des Europäischen Datenschutzausschusses) sowie die damit verbundenen Verfahren und Instrumente in der nächsten Finanziellen Vorausschau zu entnehmen.

Jahr	2014	2015	2016	2017	2018	2019	2020	Total
Personal usw.	1,555	1,555	1,543	1,543	1,543	1,543	1,543	10,823
Operationen	0,850	1,500	1,900	1,900	1,500	1,200	1,400	10,250
<b>Insgesam</b>	<b>2,405</b>	<b>3,055</b>	<b>3,443</b>	<b>3,443</b>	<b>3,043</b>	<b>2,743</b>	<b>2,943</b>	<b>21,073</b>

14.  Der Vorschlag/die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens.<sup>67</sup>

### 3.2.5. Finanzierungsbeteiligung Dritter

15.  Der Vorschlag/die Initiative sieht keine Kofinanzierung durch Dritte vor.
16.  Der Vorschlag/die Initiative sieht folgende Kofinanzierung vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			Insgesamt
Geldgeber kofinanzierende Organisation /								
Kofinanzierung INSGESAMT								

### 3.3. Geschätzte Auswirkungen auf die Einnahmen

17.  Der Vorschlag/die Initiative wirkt sich nicht auf die Einnahmen aus.
18.  Der Vorschlag/die Initiative wirkt sich auf die Einnahmen aus, und zwar
- auf die Eigenmittel
  - auf die sonstigen Einnahmen

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative <sup>68</sup>					
		Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen	

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die einschlägigen Ausgabenlinien an.  
Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

<sup>67</sup> Siehe Nummern 19 und 24 der Interinstitutionellen Vereinbarung.

<sup>68</sup> Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d.h. abzüglich 25 % für Erhebungskosten, anzugeben.

Anhang zum Finanzbogen für den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

### Zugrunde liegende Methodik und Annahmen

Die Kosten der neuen Aufgaben des Europäischen Datenschutzbeauftragten (EDSB) im Zusammenhang mit den beiden Vorschlägen wurden auf der Grundlage der Personalausgaben der Kommission für ähnliche Ausgaben geschätzt.

Der EDSB übernimmt das Sekretariat des Europäischen Datenschutzausschusses, der die Artikel-29-Datenschutzgruppe ersetzt. Gemessen am bisherigen Arbeitsaufwand der Kommission für diese Aufgabe dürften drei zusätzliche VZE sowie entsprechende Verwaltungsmittel und operativen Mittel nötig sein. Die zusätzlichen Aufgaben müssen ab Inkrafttreten der Verordnung wahrgenommen werden.

Darüber hinaus fallen dem EDSB Aufgaben im Zusammenhang mit dem Kohärenzverfahren (Personalbedarf 5 VZE) und mit der Entwicklung und dem Betrieb von IT-Programmen für nationale Datenschutzbehörden (Personalbedarf 2 VZE) zu.

Weitere Einzelheiten zur Berechnung der in den nächsten sieben Jahren zusätzlich erforderlichen Mittel sind der nachstehenden Tabelle zu entnehmen. Die zweite Tabelle enthält den operativen Mittelbedarf. Dieser wird in Teil IX (EDSB) des EU-Haushaltsplans erscheinen.

Kostenart	Berechnung	Betrag (in tausend EUR)							
		2014	2015	2016	2017	2018	2019	2020	Insgesamt
<i>Gehälter und Zulagen</i>									
- Vorsitz des EDSB		0,300	0,300	0,300	0,300	0,300	0,300	0,300	2,100
- Beamte und Zeitbedienstete	=7*0,127	0,889	0,889	0,889	0,889	0,889	0,889	0,889	6,223
- abgeordnete nationale Sachverständige	=1*0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,511
- Vertragsbedienstete	=2*0,064	0,128	0,128	0,128	0,128	0,128	0,128	0,128	0,896
<i>Ausgaben für Einstellungsverfahren</i>	=10*0,005	0,025	0,025	0,013	0,013	0,013	0,013	0,013	0,113
<i>Dienstreisekosten</i>		0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,630
<i>Sonstige Ausgaben, Fortbildung</i>	=10*0,005	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,350
<b>Verwaltungsausgaben insgesamt</b>		<b>1,555</b>	<b>1,555</b>	<b>1,543</b>	<b>1,543</b>	<b>1,543</b>	<b>1,543</b>	<b>1,543</b>	<b>10,823</b>



Beschreibung der auszuführenden Aufgaben:

<p>Beamte und Zeitbedienstete</p>	<p>Für das Sekretariat des Datenschutzausschusses zuständige Sachbearbeiter (Desk officers). Neben der logistischen Unterstützung, darunter in Haushalts- und Vertragsangelegenheiten, gehören zu deren Aufgaben die Vorbereitung der Tagesordnungen und die Einladung von Sachverständigen, Hintergrundarbeiten zu Tagesordnungspunkten des Rates, die Verwaltung der Unterlagen für die Tätigkeit des Rates, einschließlich der Kontrolle der Datenschutz-, Vertraulichkeitsschutz- und Zugangsanforderungen. Unter Einbeziehung aller Untergruppen und Expertengruppen dürften jährlich bis zu 50 Sitzungen abgehalten und Beschlussverfahren durchgeführt werden müssen.</p> <p>Sachbearbeiter (Case handlers) für das Datenschutz-Kohärenzverfahren, mit dem eine einheitliche Anwendung der Datenschutzregelung der EU sichergestellt werden soll. Zu ihren Aufgaben gehören die Untersuchung von Sachen, die von einer Behörde eines Mitgliedstaats zur Entscheidung vorgelegt wurde, sowie entsprechende Nachforschungen, Verhandlungen mit den Mitgliedstaaten und Ausarbeitung eines Beschlusses der Kommission. Ausgehend von bisherigen Erfahrungen sind jährlich etwa 5 bis 10 Sachen zu erwarten, in denen das Kohärenzverfahren eingeleitet werden muss.</p> <p>Das IT-Instrument wird die Zusammenarbeit zwischen den nationalen Datenschutzbehörden und den für die Verarbeitung Verantwortlichen, die den öffentlichen Behörden Informationen übermitteln müssen, erleichtern. Die zuständigen Bediensteten werden die Qualitätskontrolle, das Projektmanagement und die Haushaltskontrolle für die IT-Operationen im Zusammenhang mit der Anforderungstechnik, der Einführung und dem Betrieb der Systeme übernehmen.</p>
<p>Externes Personal</p>	<p>Administrative Unterstützung und Sekretariat</p>

Ausgaben des EDSB für die einzelnen Aufgaben

Ziele und Ergebnisse			Jahr N=2014	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen										INSGESAMT			
	ERGEBNISSE																			
↓	Art der Ergebnisse <sup>69</sup>	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl insgesamt	Gesamtkosten
EINZELZIEL Nr. 1 <sup>70</sup>			Sekretariat des Datenschutzausschusses																	
- Ergebnis	Sachen <sup>71</sup>	0,010	30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
Zwischensumme für Einzelziel Nr. 1			30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
EINZELZIEL Nr. 2			Kohärenzverfahren																	
- Ergebnis	Dossiers <sup>72</sup>	0,050	5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	8	0,400	59	2,950
Zwischensumme für Einzelziel Nr. 2			5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	8	0,400	59	2,950
EINZELZIEL Nr. 3			Gemeinsames IT-Programm für Datenschutzbehörden (EDSB)																	
- Ergebnis	Sachen <sup>73</sup>	0,100	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500			41	4,100
Zwischensumme für Einzelziel Nr. 3			3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500			41	4,100
<b>GESAMTKOSTEN</b>			38	0,850	56	1,500	69	1,900	69	1,900	64	1,500	61	1,200	63	1,400			420	10,250

<sup>69</sup> Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z.B.: Austausch von Studenten, gebaute Straßenkilometer...).

<sup>70</sup> Wie in Ziffer 1.4.2. („Einzelziele...“) beschrieben.

<sup>71</sup> Im Rahmen des Kohärenzverfahrens behandelte Fälle.

<sup>72</sup> Stellungnahmen, Beschlüsse, Verfahrenssitzungen des Datenschutzausschusses.

<sup>73</sup> Der Gesamtbetrag für jedes Jahr sind Schätzwerte für die Entwicklung und den Betrieb der IT-Instrumente.