



Brüssel, den 28. Januar 2016  
(OR. en)

5463/16

---

**Interinstitutionelles Dossier:**  
**2012/0010 (COD)**

---

**DATAPROTECT 4**  
**JAI 46**  
**DAPIX 14**  
**FREMP 6**  
**COMIX 40**  
**CODEC 56**

#### I/A-PUNKT-VERMERK

---

Absender: Vorsitz

Empfänger: Ausschuss der Ständigen Vertreter/Rat

Nr. Vordok.: 15360/15

Betr.: 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, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr [erste Lesung]  
– Politische Einigung

---

#### EINLEITUNG

1. Die Kommission hat am 25. Januar 2012 ein umfassendes Datenschutzpaket vorgeschlagen, das aus Folgendem besteht:

- einem Vorschlag für eine Datenschutz-Grundverordnung, welche die Datenschutzrichtlinie von 1995 (ehemalige erste Säule) ersetzen soll;
- dem vorgenannten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, welche den Datenschutz-Rahmenbeschluss von 2008 (ehemalige dritte Säule) ersetzen soll.

2. Ziel der Datenschutz-Richtlinie ist es, ein einheitliches und hohes Schutzniveau zu gewährleisten und den freien Verkehr personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu erleichtern.
3. Das Europäische Parlament hat seinen Standpunkt in erster Lesung zu der vorgeschlagenen Datenschutz-Richtlinie am 12. März 2014 festgelegt (Dok. 7428/14).
4. Der Rat hat am 8. Oktober 2015 eine allgemeine Ausrichtung (Dok. 12555/15) zu der Richtlinie festgelegt und damit dem Vorsitz ein Verhandlungsmandat zur Aufnahme von Trilogen mit dem Europäischen Parlament erteilt.
5. Nach fünf Trilogen, die von Oktober 2015 an stattfanden, haben der Vorsitz und die Vertreter des Europäischen Parlaments, die von der Kommission unterstützt wurden, Einvernehmen über einen Gesamtkompromisstext erzielt.
6. Der Ausschuss der Ständigen Vertreter hat auf seiner Tagung vom 16. Dezember 2015 den aus dem Trilog vom 15. Dezember 2015 hervorgegangenen Text gebilligt.
7. Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments hat am 17. Dezember 2015 in einer außerordentlichen Sitzung über den im Trilog vereinbarten Text abgestimmt. Am selben Tag ist der Präsident des Ausschusses der Ständigen Vertreter mit einem Schreiben des Vorsitzenden des LIBE-Ausschusses (Dok. 15361/15) darüber unterrichtet worden, dass dieser dem LIBE-Ausschuss und anschließend dem Plenum empfehlen werde, die im Trilog erzielte Einigung, vorbehaltlich der Prüfung durch die Rechts- und Sprachsachverständigen, ohne Abänderungen zu billigen.
8. Der AStV hat den Text auf seiner Tagung vom 18. Dezember 2015 im Hinblick auf eine Einigung bestätigt (Dok. 15360/15).
9. Der Ausschuss der Ständigen Vertreter wird ersucht, dass er dem Rat empfiehlt, eine politische Einigung über den in der Anlage enthaltenen Text der Datenschutz-Richtlinie zu erzielen.

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**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Datenschutzbeauftragten,<sup>1</sup>

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

- (1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union und Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union besagen, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat.

---

<sup>1</sup> ABl. C 192 vom 30.6.2012, S. 7.

- (2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Dies sollte zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen.
- (3) Der rasche technologische Fortschritt und die Globalisierung stellen den Datenschutz vor neue Herausforderungen. Das Ausmaß von Datenerhebung und Datenaustausch hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass für die Ausübung von Tätigkeiten wie die Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgegriffen werden kann.
- (4) Dies setzt voraus, dass der Datenverkehr zwischen den zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, innerhalb der Union und die Datenübermittlung an Drittländer und internationale Organisationen, erleichtert und dabei gleichzeitig ein hohes Schutzniveau für personenbezogene Daten gewährleistet wird. Hierzu bedarf es solider und stärker aufeinander abgestimmter Datenschutzbestimmungen in der Union, die konsequent durchgesetzt werden.
- (5) Die 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>2</sup> gilt für jegliche Verarbeitung personenbezogener Daten in den Mitgliedstaaten sowohl im öffentlichen als auch im privaten Bereich. Ausgenommen ist jedoch die "Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen", beispielsweise im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.

---

<sup>2</sup> ABl. L 281 vom 23.11.1995, S. 31.

- (6) Für den Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit gilt der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit verarbeitet werden<sup>3</sup>. Der Anwendungsbereich dieses Rahmenbeschlusses beschränkt sich auf die Verarbeitung personenbezogener Daten, die zwischen Mitgliedstaaten weitergegeben oder bereitgestellt werden.
- (7) Für den Zweck der wirksamen justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit ist es entscheidend, ein einheitliches und hohes Schutzniveau für die personenbezogenen Daten natürlicher Personen zu gewährleisten und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten zu erleichtern. Im Hinblick darauf sollte dafür gesorgt werden, dass die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, in allen Mitgliedstaaten gleichwertig geschützt werden. Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert nicht nur eine Stärkung der Rechte der betroffenen Personen und eine Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten, sondern auch gleichwertige Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten.
- (8) Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen.
- (9) Auf dieser Grundlage sind in der Verordnung EU ...../XXX des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) allgemeine Bestimmungen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten in der Union niedergelegt.

<sup>3</sup> ABl. L 350 vom 30.12.2008, S. 60.

- (10) In der Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon annahm, erkannte die Regierungskonferenz an, dass es sich aufgrund des spezifischen Charakters dieser Bereiche als erforderlich erweisen könnte, auf Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gestützte Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu erlassen.
- (11) Daher sollte eine gesonderte Richtlinie erlassen werden, die den Besonderheiten dieses Bereichs Rechnung trägt und Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, enthält. Diese zuständigen Behörden können nicht nur staatliche Stellen sein wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden, sondern auch alle anderen Stellen oder Einrichtungen, denen durch nationales Recht die Ausübung hoheitlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als denen dieser Richtlinie verarbeiten, gilt die Verordnung EU/XXX. Daher gilt die Verordnung EU/XXX in Fällen, in denen eine Stelle oder Einrichtung personenbezogene Daten zu anderen Zwecken erhebt und diese personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der sie unterliegt, weiterverarbeitet; zum Beispiel speichern Finanzinstitute zum Zwecke der Untersuchung, Aufdeckung oder Verfolgung bestimmte Daten, die sie verarbeiten, und stellen sie nur den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem nationalen Recht zur Verfügung. Eine Stelle oder Einrichtung, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter nach dieser Richtlinie geltenden Bestimmungen gebunden sein, wobei die Anwendung der Verordnung EU/XXX in Bezug auf Verarbeitungstätigkeiten, die der Auftragsverarbeiter außerhalb des Anwendungsbereichs dieser Richtlinie durchführt, unberührt bleibt.

- (11a) Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet; dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Dies kann ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Diese von den genannten Behörden durchgeführten Tätigkeiten umfassen auch die Aufrechterhaltung von Recht und Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für rechtlich geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist. Die Mitgliedstaaten können die zuständigen Behörden mit anderen Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich der Verordnung EU/XXX fällt, als sie in den Geltungsbereich des Unionsrechts fällt.
- (11aa) Der Begriff der Straftat im Sinne dieser Richtlinie sollte ein eigenständiger Begriff des Unionsrechts in der Auslegung durch den Gerichtshof der Europäischen Union sein.
- (11b) Da diese Richtlinie nicht für die Verarbeitung personenbezogener Daten gelten sollte, die im Rahmen einer nicht unter das Unionsrecht fallenden Tätigkeit erfolgt, sollten die nationale Sicherheit betreffende Tätigkeiten, Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind, und die Verarbeitung personenbezogener Daten, die von den Mitgliedstaaten bei Tätigkeiten vorgenommen wird, die in den Geltungsbereich des Titels V Kapitel 2 des Vertrags über die Europäische Union fallen, nicht als Tätigkeiten betrachtet werden, die in den Anwendungsbereich dieser Richtlinie fallen.

- (12) Um zu gewährleisten, dass jeder in der Union auf der Grundlage unionsweit durchsetzbarer Rechte das gleiche Maß an Schutz genießt und Unterschiede, die den Austausch personenbezogener Daten zwischen den zuständigen Behörden behindern könnten, beseitigt werden, sollte die Richtlinie harmonisierte Vorschriften für den Schutz und den freien Verkehr personenbezogener Daten festlegen, die zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, verarbeitet werden. Die Angleichung der Rechtsvorschriften der Mitgliedstaaten sollte nicht zu einer Lockerung des Datenschutzes in diesen Ländern führen, sondern vielmehr auf ein hohes Schutzniveau in der gesamten Union abstellen. Die Mitgliedstaaten sollten nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.
- (13) Diese Richtlinie berührt nicht den Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten. Gemäß der Verordnung EU/XXX können personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer öffentlichen Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die öffentliche Behörde oder Einrichtung unterliegt, freigegeben werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten in Einklang zu bringen.
- (14) Der durch diese Richtlinie gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten.
- (15) Der Schutz natürlicher Personen sollte technologienutral sein und nicht von den verwendeten Techniken abhängen, da andernfalls ein ernsthaftes Risiko einer Umgehung der Vorschriften bestünde. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung solcher Daten, wenn diese in einer Datei gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten vom Anwendungsbereich der Richtlinie ausgenommen werden.

- (15a) Die Verordnung (EG) Nr. 45/2001<sup>4</sup> gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsinstrumente der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der Verordnung EU/XXX angepasst werden.
- (15b) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, in den nationalen Vorschriften für Strafverfahren Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden festzulegen, insbesondere in Bezug auf personenbezogene Daten in einem Gerichtsbeschluss oder in Dokumenten betreffend Strafverfahren.
- (16) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Um festzustellen, ob eine natürliche Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach genutzt werden, um die Person direkt oder indirekt zu identifizieren. Bei Prüfung der Frage, ob Mittel nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei sowohl die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen, oder Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

---

<sup>4</sup> ABl. L 8 vom 12.1.2001, S. 1.

- (16a) Behörden, an die Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags weitergegeben werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, gelten nicht als Empfänger, wenn sie Daten erhalten, die für die Durchführung – gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten – eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Weitergabe, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateien betreffen oder zur Verknüpfung von Dateien führen. Die Verarbeitung dieser Daten durch die genannten Behörden sollte im Einklang mit den gemäß den Zwecken der Verarbeitung geltenden Datenschutzvorschriften erfolgen.
- (16aa) Als genetische Daten sollten personenbezogene Daten über die ererbten oder erworbenen genetischen Merkmale eines Menschen gelten, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere durch Chromosomen-, DNA- oder RNA-Analyse oder Analyse eines anderen Elements, durch die entsprechende Informationen erlangt werden können, gewonnen werden. Angesichts der Komplexität und Sensibilität genetischer Informationen besteht ein hohes Missbrauchs- und/oder Wiederverwendungsrisiko für unterschiedliche Zwecke durch den für die Verarbeitung Verantwortlichen. Jede Diskriminierung aufgrund genetischer Merkmale sollte grundsätzlich verboten sein.
- (17) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den bisherigen, derzeitigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen; dazu gehören auch Informationen über die Person, die im Zuge der Vormerkung zur Erbringung und der Erbringung von Gesundheitsdienstleistungen an die Person im Sinne der Richtlinie 2011/24/EU erhoben werden, Nummern, Symbole oder Kennzeichen, die einer bestimmten Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder einem In-Vitro-Diagnose-Test stammen.

- (17a) Alle Mitgliedstaaten sind Mitglied der Internationalen Kriminalpolizeilichen Organisation (Interpol). Interpol erhält, speichert und übermittelt für die Erfüllung ihres Auftrags Daten, um die zuständigen Behörden dabei zu unterstützen, internationale Kriminalität zu verhüten und zu bekämpfen. Daher sollte die Zusammenarbeit zwischen der Europäischen Union und Interpol gestärkt werden, indem ein effizienter Austausch personenbezogener Daten gefördert und zugleich die Achtung der Grundrechte und Grundfreiheiten hinsichtlich der automatischen Verarbeitung personenbezogener Daten gewährleistet wird. Wenn personenbezogene Daten aus der Europäischen Union an Interpol und die Staaten, die Mitglieder zu Interpol abgestellt haben, übermittelt werden, sollte diese Richtlinie zur Anwendung kommen, insbesondere die Bestimmungen über grenzüberschreitende Datenübermittlungen. Diese Richtlinie sollte die spezifischen Vorschriften unberührt lassen, die im Gemeinsamen Standpunkt 2005/69/JI des Rates vom 24. Januar 2005 zum Austausch bestimmter Daten mit Interpol<sup>5</sup> und im Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)<sup>6</sup> festgelegt sind.

---

<sup>5</sup> ABl. L 27 vom 29.1.2005, S. 61-62.

<sup>6</sup> ABl. L 205 vom 7.8.2007, S. 63-84.

- (18) Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte, gesetzlich geregelte Zwecke verarbeitet werden. Dies steht an sich der Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden nicht entgegen. Diese Maßnahmen können zwecks Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, getroffen werden, sofern sie im Recht verankert sind und eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen Person gebührend berücksichtigt werden. Der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben ist ein anderes Konzept als das Recht auf ein faires Verfahren im Sinne des Artikels 6 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und des Artikels 47 der Charta der Grundrechte der Europäischen Union. Die betroffenen Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Datenerhebung feststehen. Die Daten sollten für die Zwecke der Datenverarbeitung angemessen und sachlich relevant sein; dies heißt vor allem, dass nicht unverhältnismäßig viele Daten erfasst werden und sie nicht länger aufbewahrt werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Die Mitgliedstaaten sollten geeignete Garantien für den Fall festlegen, dass personenbezogene Daten für die im öffentlichen Interesse liegende archivarische und die wissenschaftliche, statistische oder historische Verwendung für längere Zeiträume gespeichert werden.
- (19) Zur Verhütung, Untersuchung und Verfolgung von Straftaten müssen die zuständigen Behörden personenbezogene Daten, die im Zusammenhang mit der Verhütung, Untersuchung, Aufdeckung oder Verfolgung einer bestimmten Straftat erhoben wurden, auch in einem anderen Kontext verarbeiten können, um sich ein Bild von den kriminellen Handlungen machen und Verbindungen zwischen verschiedenen aufgedeckten Straftaten herstellen zu können.

- (19a) Um stets eine sichere Verarbeitung zu gewährleisten und Verarbeitungen, die gegen diese Richtlinie verstößen, zu verhindern, sollten personenbezogene Daten so verarbeitet werden, dass ein Maß an Sicherheit und Vertraulichkeit gegeben ist, das unter Berücksichtigung des Stands der verfügbaren Technik und der Kosten für ihre Einführung den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.
- (20) (...)
- (20a) Personenbezogene Daten sollten für festgelegte, eindeutige und rechtmäßige Zwecke innerhalb des Geltungsbereichs dieser Richtlinie erhoben und nicht zu Zwecken verarbeitet werden, die nicht mit den Zwecken der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, zu vereinbaren sind. Werden personenbezogene Daten von demselben oder einem anderen für die Verarbeitung Verantwortlichen für einen anderen der in den Geltungsbereich dieser Richtlinie fallenden Zwecke als den, für den sie erhoben wurden, verarbeitet, so ist diese Verarbeitung unter der Bedingung konform, dass diese Verarbeitung nach den geltenden Rechtsvorschriften zulässig ist und dass sie für diesen anderen Zweck erforderlich und verhältnismäßig ist.
- (21) Der Grundsatz der sachlichen Richtigkeit der Daten sollte unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung angewandt werden. Aussagen, die personenbezogene Daten enthalten, basieren gerade in Gerichtsverfahren auf der subjektiven Wahrnehmung von Personen und sind nicht immer nachprüfbar. Infolgedessen sollte sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.
- (22) (...)

- (23) Bei der Verarbeitung personenbezogener Daten im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geht es naturgemäß um betroffene Personen verschiedener Kategorien. Daher sollte gegebenenfalls und so weit wie möglich klar zwischen den personenbezogenen Daten der einzelnen Kategorien betroffener Personen unterschieden werden wie Verdächtige, verurteilte Straftäter, Opfer und Dritte, beispielsweise Zeugen, Personen, die über einschlägige Informationen verfügen, oder Personen, die mit Verdächtigen oder verurteilten Straftätern in Kontakt oder in Verbindung stehen. Dies sollte nicht der Anwendung des Rechts auf die Unschuldsvermutung, wie es in der Charta der Grundrechte der Europäischen Union und in der Europäischen Menschenrechtskonvention gewährleistet ist, in der Auslegung durch die Rechtsprechung des Gerichtshofs der Europäischen Union bzw. des Europäischen Gerichtshofs für Menschenrechte entgegenstehen.
- (24) Die zuständigen Behörden sollten dafür sorgen, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Um den Schutz der Betroffenen und die Richtigkeit, Vollständigkeit oder den Umfang aktueller personenbezogener Daten sowie die Zuverlässigkeit der übermittelten oder bereitgestellten personenbezogenen Daten zu gewährleisten, sollten die zuständigen Behörden möglichst bei allen Übermittlungen personenbezogener Daten die erforderlichen Informationen beifügen.
- (24a) Wann immer in dieser Richtlinie auf mitgliedstaatliches Recht, eine Rechtsgrundlage oder eine Legislativmaßnahme Bezug genommen wird, muss es sich nicht notwendigerweise um einen von einem Parlament angenommenen Gesetzgebungsakt handeln, wobei Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats unberührt bleiben; die entsprechenden Rechtsvorschriften der Mitgliedstaaten, Rechtsgrundlagen oder Legislativmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte gefordert. In den Rechtsvorschriften der Mitgliedstaaten, die die Verarbeitung personenbezogener Daten innerhalb des Geltungsbereichs dieser Richtlinie regeln, sollten zumindest die Ziele, die zu verarbeitenden personenbezogenen Daten, die Zwecke der Verarbeitung sowie Verfahren zur Wahrung von Integrität und Vertraulichkeit der personenbezogenen Daten und Verfahren für ihre Vernichtung angegeben werden, damit ein ausreichender Schutz gegen die Gefahr des Missbrauchs und der Willkür gewährleistet ist.

(24b) Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, sollte jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung abdecken. Insbesondere sollte diese Richtlinie Anwendung finden, wenn personenbezogene Daten für die Zwecke dieser Richtlinie an einen Empfänger übermittelt werden, der nicht dieser Richtlinie unterliegt. Unter einem solchen Empfänger sollte eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle zu verstehen sein, an die personenbezogene Daten von der zuständigen Behörde rechtmäßig weitergegeben werden. Wurden die Daten ursprünglich von einer zuständigen Behörde für einen der Zwecke dieser Richtlinie erhoben, so sollte die Verordnung EU/XXX für die Verarbeitung dieser Daten für andere Zwecke als diejenigen dieser Richtlinie gelten, wenn eine solche Verarbeitung nach dem Unionsrecht oder nach mitgliedstaatlichem Recht zulässig ist. Insbesondere sollte die Verordnung EU/XXX für die Übermittlung personenbezogener Daten für Zwecke gelten, die außerhalb des Geltungsbereichs dieser Richtlinie liegen. Für die Verarbeitung personenbezogener Daten durch einen Empfänger, der keine zuständige Behörde im Sinne dieser Richtlinie ist oder nicht als solche handelt und an den personenbezogene Daten von einer zuständigen Behörde rechtmäßig weitergegeben werden, sollte die Verordnung EU/XXX gelten. Bei der Umsetzung dieser Richtlinie können die Mitgliedstaaten außerdem die Anwendung der Vorschriften der Verordnung EU/XXX – vorbehaltlich der in der Verordnung EU/XXX genannten Bedingungen – genauer regeln.

- (25) Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde im öffentlichen Interesse auf Grundlage des Unionsrechts oder des Rechts des betreffenden Mitgliedstaats zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, ausführt. Diese Tätigkeiten sollten sich auf die Wahrung lebenswichtiger Interessen der betroffenen Person erstrecken. Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu untersuchen, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern/anweisen, ihren Anordnungen nachzukommen. In diesem Fall sollte die Einwilligung der betroffenen Person (im Sinne der Verordnung EU/XXX) keine rechtliche Handhabe für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden liefern. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, so dass ihre Reaktion nicht als ohne Zwang abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, gesetzlich vorzuschreiben, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung des Aufenthaltsorts der betroffenen Person mittels elektronischer Fußfesseln zur Strafvollstreckung.
- (25a) Die Mitgliedstaaten sollten festlegen, dass immer dann, wenn nach dem Unionsrecht oder nach mitgliedstaatlichem Recht, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung von personenbezogenen Daten unter bestimmten Umständen besondere Bedingungen gelten, etwa zur Verwendung von Bearbeitungscodes, die übermittelnde zuständige Behörde den Empfänger der Daten darauf hinweisen sollte, dass diese Bedingungen gelten und einzuhalten sind. Hierzu kann beispielsweise zählen, dass der Empfänger der Daten diese nicht weiter übermitteln, für andere Zwecke verwenden oder die betroffene Person im Falle der Einschränkung des Rechts auf Unterrichtung nur nach vorheriger Genehmigung der übermittelnden zuständigen Behörde informieren darf. Diese Pflichten gelten auch für Übermittlungen durch die übermittelnde zuständige Behörde an Empfänger in Drittländern oder an internationale Organisationen. Die Mitgliedstaaten sollten festlegen, dass diese Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel IV und V des Vertrags über die Arbeitsweise der Europäischen Union errichtete Einrichtungen und sonstige Stellen nur solche Bedingungen anwendet, die auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

- (26) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und -freiheiten besonders sensibel sind, bedürfen eines besonderen Schutzes, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und -freiheiten auftreten können. Diese Daten sollten auch personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs "rassische Herkunft" in dieser Richtlinie nicht bedeutet, dass die Europäische Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Solche Daten sollten nur dann verarbeitet werden, wenn die Verarbeitung vorbehaltlich angemessener Garantien für die gesetzlich festgelegten Rechte und Freiheiten der betroffenen Person erfolgt und in gesetzlich geregelten Fällen erlaubt ist oder anderenfalls zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist oder aber sich auf Daten bezieht, die die betroffene Person offenkundig öffentlich gemacht hat. Zu den angemessenen Garantien für die Rechte und Freiheiten der betroffenen Person kann beispielsweise zählen, dass diese Daten nur in Verbindung mit anderen Daten über die betroffene Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt oder die Übermittlung dieser Daten verboten wird. Die Verarbeitung solcher Daten sollte ebenfalls gesetzlich erlaubt sein, wenn die betroffene Person ihr in Fällen, in denen die Datenverarbeitung besonders stark in ihre Privatsphäre eingreift, ausdrücklich zugestimmt hat. Die Einwilligung der betroffenen Person allein sollte jedoch noch keine rechtliche Handhabe für die Verarbeitung solch sensibler personenbezogener Daten durch die zuständigen Behörden liefern.
- (27) Die betroffene Person sollte das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die nachteilige rechtliche Wirkung für die betroffene Person entfaltet oder sie in erheblichem Maße beeinträchtigt. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs, das Eingreifen einer Person zu erwirken, insbesondere auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder des Rechts auf Anfechtung der Entscheidung. Ein Profiling, das zur Folge hat, dass natürliche Personen aufgrund von personenbezogenen Daten diskriminiert werden, die ihrem Wesen nach hinsichtlich der Grundrechte und -freiheiten besonders sensibel sind, sollte gemäß den Bestimmungen der Artikel 21 und 52 der Charta der Grundrechte der Europäischen Union untersagt werden.

- (28) Damit die betroffene Person ihre Rechte wahrnehmen kann, sollten die Informationen – auch auf der Website des für die Verarbeitung Verantwortlichen – für sie leicht zugänglich und verständlich, also klar und einfach abgefasst sein. Diese Informationen sollten an die Bedürfnisse von schutzbedürftigen Personen, wie etwa Kindern, angepasst werden.
- (29) Es gilt, die Modalitäten festzulegen, die es einer betroffenen Person ermöglichen, ihre Rechte aufgrund der nach dieser Richtlinie erlassenen Vorschriften wahrzunehmen, was Instrumente zur unentgeltlichen Wahrnehmung des Auskunftsrechts und des Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer personenbezogenen Daten einschließt. Der für die Verarbeitung Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person ohne unangemessene Verzögerung zu beantworten, es sei denn, er wendet Einschränkungen in Bezug auf die Rechte der betroffenen Person gemäß den Vorschriften dieser Richtlinie an. Bei offenkundig unbegründeten oder unverhältnismäßigen Anträgen, zum Beispiel wenn die betroffene Person ungebührlich und wiederholt Informationen verlangt oder wenn die betroffene Person ihr Recht auf Unterrichtung missbraucht, beispielsweise indem sie in ihrem Antrag falsche oder irreführende Angaben macht, kann der für die Verarbeitung Verantwortliche zudem eine angemessene Gebühr erheben oder sich weigern, aufgrund des Antrags tätig zu werden.
- (29a) Fordert der für die Verarbeitung Verantwortliche zusätzliche Informationen an, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, so sollten diese Informationen nur für diesen konkreten Zweck verarbeitet werden und nicht länger gespeichert werden, als es für diesen konkreten Zweck erforderlich ist.
- (30) Der betroffenen Person sollten zumindest folgende Informationen zur Verfügung gestellt werden: die Identität des für die Verarbeitung Verantwortlichen, die Existenz des Verarbeitungsvorgangs, die Zwecke der Verarbeitung, das Beschwerderecht und das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung und auf Einschränkung der Verarbeitung durch den für die Verarbeitung Verantwortlichen. Dies könnte auf der Website der zuständigen Behörde erfolgen. Außerdem sollte die betroffene Person in bestimmten Fällen und zur Ermöglichung der Ausübung ihrer Rechte über die Rechtsgrundlage der Verarbeitung und die Speicherfrist informiert werden, soweit diese zusätzlichen Informationen unter Berücksichtigung der spezifischen Umstände, unter denen die Daten verarbeitet werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.
- (31) (...)

- (32) Eine natürliche Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich von der Rechtmäßigkeit der Verarbeitung überzeugen zu können. Jede betroffene Person sollte daher das Recht haben, zu wissen und zu erfahren, insbesondere zu welchen Zwecken die Daten verarbeitet werden, wie lange sie gespeichert werden und wer deren Empfänger sind, auch wenn es sich um Empfänger in Drittländern handelt. Enthält die entsprechende Mitteilung Informationen über den Ursprung der personenbezogenen Daten, so sollten diese Informationen nicht die Identität natürlicher Personen und insbesondere keine vertraulichen Quellen preisgeben. Damit diesem Recht entsprochen wird, braucht die betroffene Person lediglich im Besitz einer vollständigen Übersicht über diese Daten in verständlicher Form zu sein, d.h. in einer Form, die es ihr ermöglicht, sich dieser Daten bewusst zu werden und nachzuprüfen, ob sie richtig sind und im Einklang mit dieser Richtlinie verarbeitet werden, so dass sie gegebenenfalls die ihr durch diese Richtlinie verliehenen Rechte ausüben kann. Eine solche Übersicht könnte in Form einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, bereitgestellt werden.
- (33) Den Mitgliedstaaten sollte gestattet sein, Rechtsvorschriften zu erlassen, mit denen die Unterrichtung der betroffenen Person zurückgestellt, eingeschränkt oder unterlassen oder die Auskunft über ihre personenbezogenen Daten ganz oder teilweise in dem Umfang und so lange eingeschränkt wird, wie dies in einer demokratischen Gesellschaft unter gebührender Berücksichtigung der Grundrechte und der berechtigten Interessen der betroffenen Person eine notwendige und verhältnismäßige Maßnahme darstellt, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen. Der für die Verarbeitung Verantwortliche sollte im Wege einer konkreten Einzelfallprüfung feststellen, ob das Auskunftsrecht teilweise oder vollständig eingeschränkt werden sollte.
- (34) Eine Verweigerung oder Einschränkung der Auskunft sollte der betroffenen Person grundsätzlich unter Angabe der sachlichen oder rechtlichen Gründe hierfür schriftlich mitgeteilt werden.

- (34a) Jede Einschränkung der Rechte der betroffenen Person muss mit der Charta der Grundrechte der Europäischen Union und mit der Europäische Menschenrechtskonvention in der Auslegung durch die Rechtsprechung des Gerichtshofs der Europäischen Union bzw. des Europäischen Gerichtshofs für Menschenrechte vereinbar sein und insbesondere den Wesensgehalt dieser Rechte und Freiheiten achten.
- (35) (...)
- (36) Eine natürliche Person sollte das Recht auf Berichtigung sie betreffender unzutreffender personenbezogener Daten, insbesondere bei Bezug auf Sachverhalte, sowie das Recht auf Löschung besitzen, wenn bei der Verarbeitung ihrer Daten gegen die Bestimmungen dieser Richtlinie verstoßen wird. Das Recht auf Berichtigung sollte allerdings beispielsweise nicht den Inhalt einer Zeugenaussage berühren. Eine natürliche Person sollte auch das Recht auf Einschränkung der Verarbeitung besitzen, wenn sie die Richtigkeit personenbezogener Daten bestreitet und deren Richtigkeit oder Unrichtigkeit nicht ermittelt werden kann oder wenn die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen. Insbesondere sollten personenbezogene Daten nicht gelöscht, sondern mit einer Einschränkungsmarkierung versehen werden, wenn in einem konkreten Fall berechtigter Grund zu der Annahme besteht, dass eine Löschung die berechtigten Interessen der betroffenen Person beeinträchtigen könnte. In einem solchen Fall sollten Daten mit Einschränkungsmarkierung nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand. Methoden zur Einschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte Daten, beispielsweise zu Archivierungszwecken, auf ein anderes Verarbeitungssystem übertragen oder gesperrt werden. In automatisierten Dateien sollte die Beschränkung der Verarbeitung personenbezogener Daten grundsätzlich durch technische Mittel erfolgen, wobei in dem System unmissverständlich darauf hingewiesen werden sollte, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde. Entsprechende Berichtigungen, Löschungen oder Einschränkungen der Verarbeitung sollten den Empfängern, an die die personenbezogenen Daten weitergegeben wurden, und den zuständigen Behörden, von denen die unzutreffenden Daten stammen, mitgeteilt werden. Der für die Verarbeitung Verantwortliche sollte auch von jeglicher Weiterverbreitung dieser Daten Abstand nehmen.

- (36a) Verweigert ein für die Verarbeitung Verantwortlicher einer betroffenen Person ihr Recht auf Unterrichtung, Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, so sollte die betroffene Person die nationale Aufsichtsbehörde ersuchen können, die Rechtmäßigkeit der Verarbeitung zu überprüfen. Die betroffene Person sollte über dieses Recht unterrichtet werden. Handelt die Aufsichtsbehörde im Namen der betroffenen Person, so sollte sie die betroffene Person mindestens darüber informieren, dass alle erforderlichen Überprüfungen oder Nachprüfungen erfolgt sind. Die Aufsichtsbehörde sollte die betroffene Person zudem über ihr Recht auf Rechtsbehelf in Kenntnis setzen.
- (36aa) Werden personenbezogene Daten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen verarbeitet, so kann die Ausübung des Rechts auf Unterrichtung, Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung nach Maßgabe des einzelstaatlichen Strafprozessrechts erfolgen.
- (37) Die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der für die Verarbeitung Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Richtlinie stehen. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die persönlichen Rechte und Freiheiten berücksichtigen. Im Rahmen der von ihm ergriffenen Maßnahmen sollte der für die Verarbeitung Verantwortliche auch spezifische Garantien für die Verarbeitung personenbezogener Daten von schutzbedürftigen Personen, wie etwa Kindern, ausarbeiten und implementieren.

- (37a) Risiken für die Rechte und Freiheiten der betroffenen Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Datenverarbeitung hervorgehen, die zu einer physischen, materiellen oder moralischen Schädigung führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgheimnis unterliegenden Daten, der unbefugten Umkehr der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, die Religion oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert und prognostiziert werden, um ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft.
- (37b) Eintrittswahrscheinlichkeit und Schwere des Risikos sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen.

- (38) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden persönlichen Rechte und Freiheiten ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Richtlinie erfüllt werden. Die Umsetzung dieser Maßnahmen darf nicht ausschließlich von wirtschaftlichen Erwägungen abhängig gemacht werden. Um die Einhaltung dieser Richtlinie nachweisen zu können, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen Genüge tun. Hat der für die Verarbeitung Verantwortliche eine Datenschutz-Folgenabschätzung gemäß dieser Richtlinie vorgenommen, sollten die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt werden. Die Maßnahmen könnten u.a. aus einer möglichst frühen Pseudonymisierung bestehen. Gerade durch die Pseudonymisierung für die Zwecke dieser Richtlinie könnte der freie Verkehr personenbezogener Daten im Raum der Freiheit, der Sicherheit und des Rechts erleichtert werden.
- (39) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie zur Klärung der Verantwortung und Haftung der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Richtlinie, einschließlich der Fälle, in denen ein für die Verarbeitung Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen für die Verarbeitung Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführt wird.
- (39a) Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf der Grundlage eines Rechtsinstruments einschließlich eines Vertrags erfolgen, der den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter nur auf Weisung des für die Verarbeitung Verantwortlichen handeln sollte. Der Auftragsverarbeiter sollte den Grundsatz des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen berücksichtigen.
- (40) Zum Nachweis der Einhaltung dieser Richtlinie sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis aller Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten, die seiner Zuständigkeit unterliegen, führen. Jeder für die Verarbeitung Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Verlangen dieses Verzeichnisses vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieses Verzeichnisses kontrolliert werden können. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der personenbezogene Daten in nicht automatisierten Verarbeitungssystemen verarbeitet, sollte über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Datenverarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Aufzeichnungen, verfügen.

- (40a) In automatisierten Verarbeitungssystemen werden zumindest über folgende Verarbeitungsvorgänge Protokolle geführt: Erhebung, Veränderung, Abfrage, Weitergabe einschließlich Übermittlungen, Kombination oder Löschung. Die Identität der Person, die personenbezogene Daten abgefragt oder weitergeleitet hat, sollte protokolliert werden; aus dieser Identität sollte sich die Rechtfertigung der Verarbeitungsvorgänge ableiten lassen. Die Protokolle sollten ausschließlich zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Daten sowie für Strafverfahren verwendet werden. Die Eigenüberwachung umfasst auch interne Disziplinarverfahren der zuständigen Behörden.
- (40b) Eine Datenschutz-Folgenabschätzung, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Richtlinie nachgewiesen werden sollen, sollte durch den für die Verarbeitung Verantwortlichen durchgeführt werden, wenn die Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben. Datenschutz-Folgenabschätzungen sollten auf Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen für personenbezogene Daten abstellen, nicht jedoch auf Einzelfälle.
- (41) Um einen wirksamen Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter in bestimmten Fällen vor der Verarbeitung die Aufsichtsbehörde konsultieren.
- (41a) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Richtlinie verstößende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Weitergabe von beziehungsweise unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder moralischen Schaden führen könnte. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter sollten dafür Sorge tragen, dass personenbezogene Daten nicht durch Unbefugte verarbeitet werden.

- (42) Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder moralischen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Umkehr der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile. Deshalb sollte der für die Verarbeitung Verantwortliche, sobald er davon Kenntnis erlangt, dass eine Verletzung des Schutzes personenbezogener Daten erfolgt ist und diese Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hat, die Aufsichtsbehörde ohne unangemessene Verzögerung und, falls möglich, binnen höchstens 72 Stunden, darüber unterrichten. Falls die Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne ungebührliche weitere Verzögerung bereitgestellt werden.
- (43) Natürliche Personen, sollten ohne unangemessene Verzögerung benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten führt, damit sie die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen der Datensicherheit zu treffen. In Ausnahmefällen könnte die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person unterbleiben, wenn eine Zurückstellung oder Einschränkung dieser Benachrichtigung nicht ausreicht, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen.

- (44) Der für die Verarbeitung Verantwortliche sollte eine Person benennen, die ihn dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen, es sei denn, ein Mitgliedstaat beschließt eine Ausnahmeregelung für Gerichte und andere unabhängige Justizbehörden, die in ihrer gerichtlichen Eigenschaft handeln. Bei dieser Person kann es sich um ein Mitglied des vorhandenen Personals des für die Verarbeitung Verantwortlichen handeln, das eine besondere Schulung auf dem Gebiet der Datenschutzvorschriften und -verfahren erhalten hat, um einschlägiges Fachwissen zu erwerben. Der Grad des erforderlichen Fachwissens sollte sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen verarbeiteten personenbezogenen Daten richten. Die betreffende Person kann ihre Aufgabe auf Teilzeit- oder Vollzeitbasis wahrnehmen. Mehrere für die Verarbeitung Verantwortliche können unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe gemeinsam einen Datenschutzbeauftragten bestellen, zum Beispiel im Falle einer gemeinsamen Nutzung von Ressourcen in zentralen Stellen. Die betreffende Person kann auch für verschiedene Positionen innerhalb der Struktur der jeweils für die Verarbeitung Verantwortlichen benannt werden. Sie sollte den für die Verarbeitung Verantwortlichen und die Beschäftigten, die personenbezogene Daten verarbeiten, unterstützen, indem sie diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Diese Datenschutzbeauftragten sollten ihren Auftrag und ihre Aufgaben auf unabhängige Weise gemäß dem nationalen Recht wahrnehmen können.
- (45) Die Mitgliedstaaten sollten dafür sorgen, dass Daten nur dann an ein Drittland oder eine internationale Organisation übermittelt werden, wenn dies für die Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder für die Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, notwendig ist und es sich bei dem für die Verarbeitung Verantwortlichen in dem Drittland oder in der internationalen Organisation um eine zuständige Behörde im Sinne dieser Richtlinie handelt. Eine Übermittlung darf nur durch zuständige Behörden erfolgen, die als für die Verarbeitung Verantwortliche agieren, es sei denn, Auftragsverarbeiter werden ausdrücklich beauftragt, im Namen der für die Verarbeitung Verantwortlichen Übermittlungen vorzunehmen. Derartige Übermittlungen dürfen erfolgen, wenn die Kommission durch Beschluss festgestellt hat, dass das betreffende Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau gewährleistet, oder wenn geeignete Garantien bestehen oder wenn Ausnahmen für Sonderfälle gelten. Das durch diese Richtlinie unionsweit garantierte Schutzniveau für natürliche Personen sollte bei der Übermittlung personenbezogener Daten aus der Union an für die Verarbeitung Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation stammende personenbezogene Daten an für die Verarbeitung Verantwortliche, Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weitergegeben werden.

- (45a) Werden personenbezogene Daten von einem Mitgliedstaat an Drittländer oder internationale Organisationen weitergeleitet, so sollte die Weiterleitung grundsätzlich erst dann erfolgen, wenn der Mitgliedstaat, von dem die Daten stammen, die Weiterleitung genehmigt hat. Im Interesse einer wirksamen Zusammenarbeit bei der Strafverfolgung ist es erforderlich, dass im Falle einer Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlands oder für die wesentlichen Interessen eines Mitgliedstaats, die so unvermittelt eintritt, dass es unmöglich ist, rechtzeitig eine vorherige Genehmigung einzuholen, die zuständige Behörde in der Lage sein sollte, die betreffenden personenbezogenen Daten ohne vorherige Genehmigung an das betreffende Drittland oder die betreffende internationale Organisation zu übermitteln. Die Mitgliedstaaten sollten festlegen, dass Drittländern und/oder internationalen Organisationen etwaige besondere Bedingungen für die Übermittlung mitgeteilt werden. Die Weitergabe personenbezogener Daten sollte der vorherigen Genehmigung durch die zuständige Behörde bedürfen, die die ursprüngliche Übermittlung durchgeführt hat. Bei der Entscheidung über einen Antrag auf Genehmigung einer Weitergabe sollte die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, alle relevanten Faktoren gebührend berücksichtigen, einschließlich der Schwere der Straftat, der mit der Genehmigung verbundenen spezifischen Auflagen und des Zwecks der ursprünglichen Datenübermittlung, der Art und der Bedingungen der Strafvollstreckung sowie des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weitergegeben werden sollen. Die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, kann die Weitergabe auch an besondere Bedingungen knüpfen. Diese besonderen Bedingungen können zum Beispiel in Bearbeitungscodes dargelegt werden.
- (46) Die Kommission darf mit Wirkung für die gesamte Union feststellen, dass bestimmte Drittländer oder ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bieten, und auf diese Weise in Bezug auf die Drittländer und internationale Organisationen, die für fähig gehalten werden, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne besondere Genehmigung an diese Länder übermittelt werden, es sei denn, dass ein anderer Mitgliedstaat, von dem die Daten stammen, die Weiterleitung zu genehmigen hat.

- (47) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlandes oder eines Gebietes oder eines bestimmten Sektors in einem Drittland berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, ein Rechtsschutz existiert und die internationalen Menschenrechtsbestimmungen eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und öffentliche Ordnung sowie das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor in einem Drittland sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmter Verarbeitungsvorgänge und des Geltungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das im Wesentlichen dem innerhalb der Union gewährleisteten Schutzniveau gleichwertig ist, insbesondere in Fällen, in denen Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den europäischen Datenschutzbehörden vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame behördliche und gerichtliche Rechtsbehelfe eingeräumt werden.
- (47a) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des Drittlandes zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Europäischen Datenschutzausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet. Die Kommission sollte ferner alle relevanten Angemessenheitsbeschlüsse berücksichtigen, die sie nach Artikel 41 der Verordnung (EU) XXX angenommen hat.

- (47b) Die Kommission sollte die Wirksamkeit von Feststellungen betreffend das Schutzniveau in einem Drittland oder einem Gebiet oder einem spezifischen Sektor in einem Drittland oder einer internationalen Organisation überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung ihrer Wirksamkeit vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen relevanten Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen.
- (48) Die Kommission sollte gleichfalls feststellen können, dass ein Drittland, ein Gebiet oder ein spezifischer Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen des Artikels 35 oder 36 werden erfüllt. Es sollten Verfahren für Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

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

(49aa) Sind weder ein Angemessenheitsbeschluss noch geeignete Garantien vorhanden, so sollte eine Übermittlung oder eine Kategorie von Übermittlungen nur in Sonderfällen erfolgen können, in denen dies zur Wahrung wesentlicher Interessen der betroffenen oder einer anderen Person notwendig ist oder wenn dies nach dem Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, zum Schutz berechtigter Interessen der betroffenen Person notwendig ist oder wenn dies zur Abwehr einer unmittelbaren, ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlands notwendig ist oder in einem Einzelfall zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, notwendig ist oder in einem Einzelfall zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen notwendig ist. Diese Ausnahmen sollten restriktiv ausgelegt werden, wiederkehrende, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen in großem Umfang ausschließen und daher auf unbedingt notwendige Daten beschränkt sein. Derartige Übermittlungen sollten dokumentiert werden, und die entsprechende Dokumentation sollte der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden, damit diese die Rechtmäßigkeit der Übermittlung überprüfen kann.

(49b) Die zuständigen Behörden der Mitgliedstaaten wenden die geltenden bilateralen oder multilateralen internationalen Übereinkünfte, die mit Drittländern auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geschlossen wurden, für den Austausch zweckdienlicher Informationen an, um ihnen zu ermöglichen, die ihnen rechtlich zugewiesenen Aufgaben wahrzunehmen. Grundsätzlich erfolgt dies über die zuständigen Behörden des betreffenden Drittlands oder zumindest in Zusammenarbeit mit diesen zuständigen Behörden, mitunter auch dann, wenn keine bilaterale oder multilaterale internationale Übereinkunft existiert. In speziellen Einzelfällen kann es jedoch vorkommen, dass die regulären Verfahren, die eine Kontaktaufnahme mit der zuständigen Behörde in dem betreffenden Drittland vorschreiben, wirkungslos oder ungeeignet wären, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden könnte oder weil die zuständige Behörde in dem betreffenden Drittland die Rechtsstaatlichkeit oder die internationalen Menschenrechtsbestimmungen nicht achtet, so dass die zuständigen Behörden der Mitgliedstaaten beschließen könnten, die personenbezogenen Daten direkt an in Drittländern niedergelassene Empfänger zu übermitteln. Dies kann der Fall sein, wenn es dringend geboten ist, personenbezogene Daten zu übermitteln, um das Leben einer Person zu schützen, die Gefahr läuft, Opfer einer Straftat zu werden, oder um die unmittelbar bevorstehende Begehung einer Straftat, einschließlich einer terroristischen Straftat, zu verhindern. Auch wenn diese Übermittlung zwischen zuständigen Behörden und in Drittländern niedergelassenen Empfängern nur in speziellen Einzelfällen erfolgen sollte, sollte diese Richtlinie die Voraussetzungen für die Regelung solcher Fälle vorsehen. Diese Bestimmungen sollten nicht als Ausnahmen von geltenden bilateralen oder multilateralen internationalen Übereinkünften auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit betrachtet werden. Diese Vorschriften sollten zusätzlich zu den sonstigen Vorschriften der Richtlinie gelten, insbesondere den Vorschriften über die Rechtmäßigkeit der Verarbeitung und von Kapitel V.

(50) Wenn personenbezogene Daten in ein anderes Land übermittelt werden, kann dies dazu führen, dass die betroffene Person weniger Möglichkeiten hat, ihre Datenschutzrechte wahrzunehmen und sich gegen eine unrechtmäßige Nutzung oder Weitergabe ihrer Daten zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse und durch nicht übereinstimmende Rechtsordnungen behindert werden. Die Zusammenarbeit zwischen den Datenschutzbehörden muss daher gefördert werden, um ihnen den Informationsaustausch mit Aufsichtsbehörden in anderen Ländern zu erleichtern.

- (51) Die Einrichtung von Aufsichtsbehörden in den Mitgliedstaaten, die ihre Aufgaben völlig unabhängig erfüllen, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Aufsichtsbehörden sollten die Anwendung der nach dieser Richtlinie erlassenen Vorschriften überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.
- (52) Die Mitgliedstaaten können einer bereits gemäß der Verordnung EU/XXX errichteten Aufsichtsbehörde die Verantwortung für die Aufgaben übertragen, die von den nach dieser Richtlinie einzurichtenden nationalen Aufsichtsbehörden auszuführen sind.
- (53) Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde einrichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht. Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über eigene, öffentliche, jährliche Haushaltspläne verfügen, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.
- (53a) Die Aufsichtsbehörden sollten unabhängigen Kontroll- oder Überwachungsmechanismen hinsichtlich ihrer Ausgaben unterliegen, sofern diese Finanzkontrolle ihre Unabhängigkeit nicht berührt.
- (54) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten gesetzlich von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des betreffenden Mitgliedstaats auf Vorschlag der Regierung oder eines Regierungsmitglieds oder des Parlaments oder dessen Kammer oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder integer handeln, von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarenden entgeltliche oder unentgeltliche Tätigkeit ausüben. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollte ihr Personal von der Aufsichtsbehörde selbst ausgewählt werden; dabei kann eine unabhängige, nach mitgliedstaatlichem Recht betraute Stelle eingeschaltet werden.

- (55) Obgleich diese Richtlinie auch für die Tätigkeit der nationalen Gerichte und anderer Justizbehörden gilt, sollte sich die Zuständigkeit der Aufsichtsbehörden nicht auf die von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Datenverarbeitungen erstrecken, damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben gewahrt bleibt. Diese Ausnahme sollte allerdings begrenzt werden auf justizielle Tätigkeiten in Gerichtssachen und sich nicht auf andere Tätigkeiten beziehen, mit denen Richter nach nationalem Recht betraut werden können. Die Mitgliedstaaten können außerdem vorsehen, dass sich die Zuständigkeit der Aufsichtsbehörde nicht auf die Überwachung der Verarbeitung personenbezogener Daten erstreckt, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit, beispielsweise Staatsanwaltschaften, erfolgt. Die Einhaltung der Vorschriften dieser Richtlinie durch die Gerichte und andere unabhängige Justizbehörden sollte in jedem Fall stets der unabhängigen Überwachung gemäß Artikel 8 Absatz 3 der Charta der Grundrechte der Europäischen Union unterliegen.
- (56) Jede Aufsichtsbehörde sollte Beschwerden von betroffenen Personen bearbeiten und die Angelegenheit untersuchen. Die Untersuchung aufgrund einer Beschwerde sollte vorbehaltlich einer gerichtlichen Nachprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb einer angemessenen Frist über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde vonnöten sein, so sollte die betroffene Person eine Zwischenunterrichtung erhalten.

- (57) Um die wirksame, zuverlässige und einheitliche Überwachung der Einhaltung und Durchsetzung dieser Richtlinie in der gesamten Union gemäß dem Vertrag in der Auslegung durch den Gerichtshof der Europäischen Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse, die notwendige Instrumente zur Erfüllung ihrer Aufgaben darstellen. Ihre Befugnisse dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschließlich der Untersuchung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren. Unbeschadet der Befugnisse der Strafverfolgungsbehörden nach nationalem Recht sollten die Aufsichtsbehörden außerdem die Befugnis haben, Verstöße gegen diese Richtlinie den Justizbehörden zur Kenntnis zu bringen und/oder Gerichtsverfahren anzustrengen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach Unionsrecht und einzelstaatlichem Recht unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Richtlinie geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im nationalen Recht ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Der Erlass eines rechtsverbindlichen Beschlusses sollte in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, einer gerichtlichen Prüfung unterliegen.
- (58) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und einander Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung der nach dieser Richtlinie erlassenen Vorschriften gewährleistet ist.
- (59) Der auf der Grundlage der Verordnung EU/XXX eingerichtete Europäische Datenschutzausschuss sollte zur einheitlichen Anwendung dieser Richtlinie in der Union beitragen, was Beratung der Kommission und Förderung der Zusammenarbeit der Aufsichtsbehörden in der Union einschließt.

- (60) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde eine Beschwerde einzureichen und gemäß Artikel 47 der Grundrechtecharta der Europäischen Union einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten aufgrund von nach dieser Richtlinie erlassenen Vorschriften verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die zuständige Aufsichtsbehörde sollte die betroffene Person innerhalb einer angemessenen Frist über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde vonnöten sein, so sollte die betroffene Person eine Zwischenunterrichtung erhalten. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.
- (61) Jede natürliche oder juristische Person sollte das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Dieses Recht umfasst jedoch nicht andere – rechtlich nicht bindende – Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem nationalen Verfahrensrecht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit relevanten Sach- und Rechtsfragen zu prüfen, einschließt.

- (62) Betroffene Personen, die sich in ihren Rechten gemäß dieser Richtlinie verletzt sehen, sollten das Recht haben, Einrichtungen, die sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Schutzes ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, zu beauftragen, in ihrem Namen eine Beschwerde bei einer Aufsichtsbehörde einzureichen und einen gerichtlichen Rechtsbehelf einzulegen. Das Recht betroffener Personen auf Vertretung sollte das nationale Verfahrensrecht unberührt lassen, nach dem eine obligatorische Vertretung betroffener Personen durch einen Rechtsanwalt im Sinne der Richtlinie 77/249/EWG vor nationalen Gerichten erforderlich sein kann.
- (63) (...)
- (64) Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften steht, sollten von dem für die Verarbeitung Verantwortlichen oder einer anderen nach nationalem Recht zuständigen Behörde ersetzt werden. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs der Europäischen Union weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Richtlinie in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Wird auf eine Verarbeitung Bezug genommen, die unrechtmäßig ist oder nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften steht, so gilt dies auch für Verarbeitungen, die nicht im Einklang mit den aufgrund dieser Richtlinie erlassenen Durchführungsrechtsakten stehen. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.
- (65) Gegen jede natürliche oder juristische – privatem oder öffentlichem Recht unterliegende – Person, die gegen diese Richtlinie verstößt, sollten Sanktionen verhängt werden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sind, und alle Maßnahmen zur Anwendung der Sanktionen treffen.
- (66) (...)

- (67) Um einheitliche Bedingungen für die Anwendung dieser Richtlinie sicherzustellen, sollten der Kommission Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder einem spezifischen Sektor dieses Drittlands oder in einer internationalen Organisation, das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss. 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, ausgeübt werden<sup>7</sup>.
- (68) Durchführungsrechtsakte über die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder einem spezifischen Sektor dieses Drittlands oder in einer internationalen Organisation, das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.
- (69) Die Kommission sollte in hinreichend begründeten Fällen äußerster Dringlichkeit, die ein Drittland oder ein Gebiet oder einen spezifischen Sektor in diesem Drittland oder eine internationale Organisation betreffen, die kein angemessenes Schutzniveau mehr gewährleisten, sofort geltende Durchführungsrechtsakte erlassen.

---

<sup>7</sup> ABl. L 55 vom 28.2.2011, S. 13.

- (70) Da die Ziele dieser Richtlinie, nämlich die Grundrechte und Grundfreiheiten betroffener Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten und den ungehinderten Austausch personenbezogener Daten im Verkehr zwischen den zuständigen Behörden innerhalb der Union zu gewährleisten, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus. Die Mitgliedstaaten können höhere Standards als die in dieser Richtlinie festgelegten vorsehen.
- (71) Der Rahmenbeschluss 2008/977/JI sollte durch diese Richtlinie aufgehoben werden.
- (72) Besondere Bestimmungen, die in vor Erlass dieser Richtlinie im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander sowie den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen im Anwendungsbereich dieser Richtlinie regeln, sollten unberührt bleiben, beispielsweise die besonderen Bestimmungen betreffend den Schutz personenbezogener Daten gemäß dem Beschluss 2008/615/JI des Rates<sup>8</sup> oder Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. 2000 C 197/1)<sup>9</sup>. Da Artikel 8 der Grundrechtecharta und Artikel 16 AEUV vorschreiben, dass das Grundrecht auf Schutz personenbezogener Daten in der Union einheitlich angewendet werden sollte, sollte die Kommission das Verhältnis zwischen dieser Richtlinie und den vor ihrem Erlass angenommenen Rechtsakten, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander oder den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen regeln, daraufhin prüfen, inwieweit die besonderen Bestimmungen dieser Rechtsakte an diese Richtlinie angepasst werden müssen. Die Kommission sollte gegebenenfalls Vorschläge zur Gewährleistung einheitlicher Rechtsvorschriften in Bezug auf die Verarbeitung personenbezogener Daten unterbreiten.

<sup>8</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).

<sup>9</sup> Rechtsakt des Rates vom 29. Mai 2000 über die Erstellung – gemäß Artikel 34 des Vertrags über die Europäische Union – des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. C 197 vom 12.7.2000, S. 1).

- (73) Zur Gewährleistung eines umfassenden und kohärenten Schutzes personenbezogener Daten in der Union sollten internationale Übereinkünfte, die von den Mitgliedstaaten vor Inkrafttreten dieser Richtlinie geschlossen wurden und die im Einklang mit dem maßgeblichen vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht stehen, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden.
- (73a) Die Mitgliedstaaten sollten gehalten sein, diese Richtlinie innerhalb von höchstens zwei Jahren nach ihrem Inkrafttreten umzusetzen. Verarbeitungen, die zum Zeitpunkt des Inkrafttretens dieser Richtlinie bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Richtlinie mit ihr in Einklang gebracht werden. Stehen die Verarbeitungen jedoch im Einklang mit dem vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht, so sollten die Anforderungen der vorliegenden Richtlinie betreffend die vorherige Konsultation der Aufsichtsbehörde nicht für Verarbeitungsvorgänge gelten, die bereits vor dem Inkrafttreten der vorliegenden Richtlinie eingeleitet wurden, da diese Anforderungen naturgemäß vor der Verarbeitung erfüllt sein müssen. Nehmen Mitgliedstaaten die längere Umsetzungsfrist, die sieben Jahre nach dem Inkrafttreten dieser Richtlinie endet, in Anspruch, um den Protokollierungspflichten für vor dem Inkrafttreten dieser Richtlinie eingerichtete automatisierte Verarbeitungssysteme nachzukommen, so sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Datenverarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Aufzeichnungen, verfügen.
- (74) Diese Richtlinie lässt die Vorschriften zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie nach Maßgabe der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 unberührt.<sup>10</sup>

<sup>10</sup> ABl. L 335 vom 17.12.2011, S. 1.

- (75) Nach Artikel 6a des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Bestimmungen dieser Richtlinie über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union fallen, für das Vereinigte Königreich und Irland nicht bindend, wenn das Vereinigte Königreich und Irland nicht durch Unionsvorschriften gebunden sind, die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 des Vertrags über die Arbeitsweise der Europäischen Union festgelegten Vorschriften eingehalten werden müssen.
- (76) Nach den Artikeln 2 und 2a des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position Dänemarks ist Dänemark durch die Bestimmungen dieser Richtlinie, die sich auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten beziehen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 des Vertrags über die Arbeitsweise der Europäischen Union fallen, weder gebunden noch zu ihrer Anwendung verpflichtet. Da diese Richtlinie den Schengen-Besitzstand gemäß dem Dritten Teil Titel V des Vertrags über die Arbeitsweise der Europäischen Union ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten nach Erlass dieser Richtlinie, ob es sie in innerstaatliches Recht umsetzt.
- (77) Für Island und Norwegen stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assozierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.<sup>11</sup>

---

<sup>11</sup> ABl. L 176 vom 10.7.1999, S. 36.

- (78) Für die Schweiz stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.<sup>12</sup>
- (79) Für Liechtenstein stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.<sup>13</sup>
- (80) Diese Richtlinie steht im Einklang mit den 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, dem Recht auf Schutz personenbezogener Daten sowie dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren. Die Einschränkungen dieser Rechte stehen im Einklang mit Artikel 52 Absatz 1 der Charta, da sie erforderlich sind, um den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und der Freiheiten anderer zu entsprechen.
- (81) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission vom 28. September 2011 zu erläuternden Dokumenten<sup>14</sup> haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen einzelstaatlicher Umsetzungsinstrumente erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

<sup>12</sup> ABl. L 53 vom 27.2.2008, S. 52.

<sup>13</sup> ABl. L 160 vom 18.6.2011, S. 21.

<sup>14</sup> ABl. C 369 vom 17.12.2011, S. 14.

- (82) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, die Bestimmungen über die Ausübung der Rechte der betroffenen Personen auf Unterrichtung, Auskunft, Berichtigung, Löschung und Beschränkung ihrer im Rahmen eines Strafverfahrens verarbeiteten personenbezogenen Daten sowie mögliche Beschränkungen dieser Rechte in ihr einzelstaatliches Strafprozessrecht umzusetzen.

# **KAPITEL I**

## **ALLGEMEINE BESTIMMUNGEN**

### *Artikel 1*

#### ***Gegenstand und Ziele***

1. Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt.
- 1a. Diese Richtlinie hindert die Mitgliedstaaten nicht daran, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.
2. Gemäß dieser Richtlinie haben die Mitgliedstaaten
  - a) die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und
  - b) sicherzustellen, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union – sofern er nach dem Unionsrecht oder dem nationalen Recht erforderlich ist – nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten wird.

### *Artikel 2*

#### ***Anwendungsbereich***

1. Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken.
2. Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

3. Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten
  - a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt,
  - b) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union.

### *Artikel 3*

#### ***Begriffsbestimmungen***

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

- (1) "personenbezogene Daten" alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person ("betroffene Person") beziehen; als bestimmbare wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen bestimmt werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
- (2) (...)
- (3) "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- (4) "Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
- (4a) "Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die die Nichtzuordnung zu einer bestimmten oder bestimmbaren Person gewährleisten;

- (5) "Datei" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder aufgeschlüsselt nach funktionalen oder geografischen Gesichtspunkten geführt wird;
- (6) "für die Verarbeitung Verantwortlicher" die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten durch einzelstaatliches oder Unionsrecht vorgegeben, so können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach Unionsrecht oder einzelstaatlichem Recht bestimmt werden;
- (7) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- (8) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags nach dem nationalen Recht möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den gemäß den Zwecken der Verarbeitung geltenden Datenschutzvorschriften;
- (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" personenbezogene Daten jedweder Art zu den ererbten oder erworbenen genetischen Merkmalen eines Menschen, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden;
- (11) "biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die die eindeutige Identifizierung dieses Menschen ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

- (12) "Gesundheitsdaten" Daten, die sich auf die körperliche oder geistige Gesundheit einer Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
- (12a) "Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- (13) (...)
- (14) "zuständige Behörde"
- a) eine staatliche Stelle, die für die Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, zuständig ist, oder
  - b) eine andere Stelle oder Einrichtung, der durch nationales Recht die Ausübung hoheitlicher Befugnisse zur Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, übertragen wurde;
- (15) "Aufsichtsbehörde" eine von einem Mitgliedstaat gemäß Artikel 39 eingerichtete unabhängige staatliche Stelle;
- (16) "internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

## **KAPITEL II**

### **GRUNDSÄTZE**

#### *Artikel 4*

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

1. Die Mitgliedstaaten legen fest, dass personenbezogene Daten
  - a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
  - b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
  - c) dem Verarbeitungszweck entsprechen, sachlich relevant und in Bezug auf die Zwecke, für die sie verarbeitet werden, verhältnismäßig sind,
  - d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden,
  - e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,
  - f) (...)
  - fb) so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen.
2. Eine Verarbeitung durch denselben oder einen anderen für die Verarbeitung Verantwortlichen für andere der in Artikel 1 Absatz 1 genannten Zwecke als den, für den die Daten erhoben werden, ist erlaubt, sofern
  - a) der für die Verarbeitung Verantwortliche nach Unions- oder einzelstaatlichem Recht befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und

- b) die Verarbeitung für diesen anderen Zweck nach einzelstaatlichem oder Unionsrecht erforderlich und verhältnismäßig ist.
3. Die Verarbeitung durch denselben oder einen anderen für die Verarbeitung Verantwortlichen kann die im öffentlichen Interesse liegende archivarische oder die wissenschaftliche, statistische oder historische Verwendung für die in Artikel 1 Absatz 1 genannten Zwecke umfassen, sofern angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorhanden sind.
4. Der für die Verarbeitung Verantwortliche ist für die Einhaltung der Absätze 1, 2 und 3 verantwortlich und muss dies nachweisen können.

*Artikel 4b*

***Fristen für die Speicherung und Überprüfung***

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

*Artikel 5*

***Unterscheidung verschiedener Kategorien von betroffenen Personen***

1. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien von betroffenen Personen klar unterscheidet, darunter:
- a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,
  - b) verurteilte Straftäter,
  - c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

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

#### *Artikel 6*

#### ***Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der Daten***

1. Die Mitgliedstaaten tragen dafür Sorge, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird.
2. Die Mitgliedstaaten legen fest, dass die zuständigen Behörden alle angemessenen Maßnahmen ergreifen müssen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Zu diesem Zweck überprüft jede zuständige Behörde, soweit durchführbar, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit die erforderlichen Informationen beigefügt, die es der empfangenden zuständigen Behörde gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.
3. Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 15 eine Berichtigung, Löschung oder Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen.

*Artikel 7*

***Rechtmäßigkeit der Verarbeitung***

1. Die Mitgliedstaaten legen fest, dass die Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unions- oder einzelstaatlichen Rechts erfolgt.
  - a) (...)
  - b) (...)
  - c) (...)
  - d) (...)

- 1a. Im Recht der Mitgliedstaaten, das die Verarbeitung personenbezogener Daten innerhalb des Geltungsbereichs dieser Richtlinie regelt, werden mindestens die Ziele, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben.

*Artikel 7a*

***Besondere Verarbeitungsbedingungen***

1. Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unions- oder dem einzelstaatlichen Recht zulässig. In diesen Fällen gilt für diese Verarbeitung die Verordnung EU/XXX, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt.
- 1a. Sind nach dem einzelstaatlichen Recht zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den in Artikel 1 Absatz 1 genannten Zwecken decken, so gilt die Verordnung EU/XXX für die Verarbeitung zu diesen Zwecken – wozu auch die im öffentlichen Interesse liegende archivarische und die wissenschaftliche, statistische oder historische Verwendung zählt –, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt.

- 1b. Die Mitgliedstaaten legen fest, dass immer dann, wenn nach dem Unions- oder dem einzelstaatlichen Recht, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung von personenbezogenen Daten besondere Bedingungen gelten, die übermittelnde zuständige Behörde den Empfänger der Daten darauf hinweisen muss, dass diese Bedingungen gelten und einzuhalten sind.
2. Die Mitgliedstaaten legen fest, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel IV und V des Vertrags über die Arbeitsweise der Europäischen Union errichtete Einrichtungen und sonstige Stellen nur solche Bedingungen nach Absatz 1b anwendet, die auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

### *Artikel 8*

#### ***Verarbeitung besonderer Datenkategorien***

1. Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer Person und Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich angemessener Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und wenn sie
  - a) nach dem Unionsrecht oder dem einzelstaatlichen Recht zulässig ist oder
  - b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen Person dient oder
  - c) sich auf Daten bezieht, die die betroffene Person offenkundig öffentlich gemacht hat.
2. (...)

*Artikel 9*

***Automatisierte Generierung von Einzelentscheidungen***

1. Die Mitgliedstaaten legen fest, dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung – einschließlich Profiling –, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, verboten ist, es sei denn, sie ist nach dem Unions- oder dem einzelstaatlichen Recht, dem der für die Verarbeitung Verantwortliche unterliegt und das angemessene Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des für die Verarbeitung Verantwortlichen, erlaubt.
2. Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 8 beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.
- 2b. Profiling, das zur Folge hat, dass natürliche Personen aufgrund von besonderen Datenkategorien nach Artikel 8 diskriminiert werden, ist nach Unionsrecht verboten.

## **KAPITEL III**

### **RECHTE DER BETROFFENEN PERSON**

#### *Artikel 10*

##### ***Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person***

1. (...)
2. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche alle angemessenen Maßnahmen trifft, um der betroffenen Person alle Informationen gemäß Artikel 10a sowie alle Mitteilungen gemäß den Artikeln 9, 12 bis 17 und 29, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Übermittlung der Informationen erfolgt in einer beliebigen geeigneten Form, wozu auch die elektronische Übermittlung zählt. Grundsätzlich übermittelt der für die Verarbeitung Verantwortliche die Informationen in derselben Form, in der er den Antrag erhalten hat.
3. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche die Ausübung der den betroffenen Personen gemäß den Artikeln 9 und 12 bis 17 zustehenden Rechte erleichtert.
4. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche die betroffene Person ohne unangemessene Verzögerung schriftlich von den Maßnahmen in Kenntnis setzt, die im Zusammenhang mit ihrem Antrag getroffen wurden.
5. Die Mitgliedstaaten tragen dafür Sorge, dass die Informationen gemäß Artikel 10a und alle Mitteilungen und Maßnahmen gemäß den Artikeln 9, 12 bis 17 und 29 unentgeltlich zur Verfügung gestellt werden. Bei offenkundig unbegründeten oder – insbesondere im Fall ihrer Häufung – unverhältnismäßigen Anträgen einer betroffenen Person kann der für die Verarbeitung Verantwortliche ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder er kann sich weigern, aufgrund des Antrags tätig zu werden. In diesen Fällen hat er den Nachweis für den offenkundig unbegründeten oder unverhältnismäßigen Charakter des Antrags zu erbringen.
- 5a. Hat der für die Verarbeitung Verantwortliche begründete Zweifel an der Identität der Person, die den Antrag gemäß den Artikeln 12 und 15 stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

*Artikel 10a*

***Unterrichtung der betroffenen Person***

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche der betroffenen Person mindestens die folgenden Informationen zur Verfügung stellt:
  - a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen; zusätzlich werden, falls vorhanden, auch die Kontaktdaten des Datenschutzbeauftragten angegeben,
  - b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden,
  - c) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontakt-  
daten,
  - d) das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten und auf Einschränkung der Verarbeitung dieser Daten durch den für die Verarbeitung Verantwortlichen.
2. Die Mitgliedstaaten schreiben gesetzlich vor, dass der für die Verarbeitung Verantwortliche der betroffenen Person in besonderen Fällen die folgenden Informationen gibt, die die in Absatz 1 genannten Informationen ergänzen, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:
  - a) die Rechtsgrundlage der Verarbeitung,
  - b) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
  - c) gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,
  - d) erforderlichenfalls jede weitere Information, insbesondere wenn die Daten ohne Wissen der betroffenen Person erhoben werden.

3. Die Mitgliedstaaten dürfen Rechtsvorschriften erlassen, nach denen die Unterrichtung der betroffenen Person gemäß Absatz 2 zu folgenden Zwecken in dem Umfang und so lange zurückgestellt, eingeschränkt oder unterlassen werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen Person Rechnung getragen wird:
  - a) Gewährleistung, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden,
  - b) Gewährleistung, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,
  - c) Schutz der öffentlichen Sicherheit,
  - d) Schutz der nationalen Sicherheit,
  - e) Schutz der Rechte und Freiheiten anderer.
4. Die Mitgliedstaaten können Rechtsvorschriften zur Festlegung der Datenverarbeitungskategorien erlassen, für die die Ausnahmeregelung nach Absatz 3 vollständig oder teilweise zur Anwendung kommt.

*Artikel 11*

(...)

*Artikel 12*  
***Auskunftsrecht der betroffenen Person***

1. Vorbehaltlich des Artikels 13 tragen die Mitgliedstaaten dafür Sorge, dass die betroffene Person das Recht hat, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Zugang zu diesen Daten und zu folgenden Informationen zu erhalten:
  - a) die Verarbeitungszwecke sowie die Rechtsgrundlage für die Verarbeitung,
  - b) die Kategorien personenbezogener Daten, die verarbeitet werden,
  - c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind, speziell bei Empfängern in Drittländern oder bei internationalen Organisationen,
  - d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
  - e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten und auf Einschränkung der Verarbeitung dieser Daten durch den für die Verarbeitung Verantwortlichen,
  - f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontakt-  
daten,
  - g) Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.
2. (...)

## Artikel 13

### ***Einschränkung des Auskunftsrechts***

1. Die Mitgliedstaaten können Rechtsvorschriften erlassen, die zu nachstehenden Zwecken das Recht der betroffenen Person auf Auskunft teilweise oder vollständig einschränken, soweit und für die geplante Dauer diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen Person Rechnung getragen wird:
  - a) Gewährleistung, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden,
  - b) Gewährleistung, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,
  - c) Schutz der öffentlichen Sicherheit,
  - d) Schutz der nationalen Sicherheit,
  - e) Schutz der Rechte und Freiheiten anderer.
2. Die Mitgliedstaaten können Rechtsvorschriften zur Festlegung der Datenverarbeitungskategorien erlassen, für die die Ausnahmeregelung nach Absatz 1 vollständig oder teilweise zur Anwendung kommt.
3. Für die in den Absätzen 1 und 2 genannten Fälle legen die Mitgliedstaaten fest, dass der für die Verarbeitung Verantwortliche die betroffene Person ohne unangemessene Verzögerung schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür unterrichtet. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in Absatz 1 genannten Zwecke zuwiderliefe. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche die betroffene Person über die Möglichkeiten unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.
4. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche die sachlichen oder rechtlichen Gründe für die Entscheidung dokumentiert. Diese Angaben sind der Aufsichtsbehörde zur Verfügung zu stellen.

*Artikel 14*

(...)

*Artikel 15*

***Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung***

1. Die Mitgliedstaaten sehen vor, dass die betroffene Person das Recht hat, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende unzutreffende personenbezogene Daten ohne unangemessene Verzögerung berichtigt werden. Im Hinblick auf den Zweck der jeweiligen Verarbeitung sorgen die Mitgliedstaaten dafür, dass die betroffene Person das Recht hat, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.
- 1a. Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche verpflichtet ist, personenbezogene Daten ohne unangemessene Verzögerung zu löschen, und dass die betroffene Person das Recht hat, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten ohne unangemessene Verzögerung zu verlangen, wenn die Verarbeitung nicht im Einklang mit den nach den Artikeln 4, 7 und 8 erlassenen Vorschriften steht oder wenn die Daten zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, der der für die Verarbeitung Verantwortliche unterliegt.
- 1b. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung beschränken, wenn
  - a) die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht ermittelt werden kann, oder
  - b) die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen.
- 1c. Unterliegt die Verarbeitung personenbezogener Daten einer Beschränkung gemäß Absatz 1b Buchstabe a, unterrichtet der für die Verarbeitung Verantwortliche die betroffene Person, bevor er die Beschränkung aufhebt.

2. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche die betroffene Person schriftlich über eine Verweigerung der Berichtigung, Löschung oder Einschränkung der Verarbeitung und über die Gründe für die Verweigerung unterrichtet. Die Mitgliedstaaten können Rechtsvorschriften erlassen, die zu nachstehenden Zwecken die Pflicht, diese Informationen zur Verfügung zu stellen, teilweise oder vollständig einschränken, soweit diese Einschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen Person Rechnung getragen wird:
- a) Gewährleistung, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden,
  - b) Gewährleistung, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,
  - c) Schutz der öffentlichen Sicherheit,
  - d) Schutz der nationalen Sicherheit,
  - e) Schutz der Rechte und Freiheiten anderer.

Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche die betroffene Person über die Möglichkeiten unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.

- 2b. Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die Berichtigung von unzutreffenden personenbezogenen Daten der zuständigen Behörde, von der die falschen Daten stammen, mitteilt.
3. Die Mitgliedstaaten tragen dafür Sorge, dass in den Fällen nach den Absätzen 1, 1a, 1b und 1c der für die Verarbeitung Verantwortliche die Empfänger in Kenntnis setzt und dass die Empfänger die ihrer Verantwortung unterliegenden personenbezogenen Daten berichtigten, löschen oder deren Verarbeitung einschränken.

*Artikel 15a*

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

1. In den in Artikel 10a Absatz 3, Artikel 13 Absatz 3 und Artikel 15 Absatz 2 genannten Fällen erlassen die Mitgliedstaaten Maßnahmen, in denen vorgesehen ist, dass die Rechte der betroffenen Person auch über die zuständige Aufsichtsbehörde ausgeübt werden können.
  - 1a. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, ihr Recht auf Befassung der Aufsichtsbehörde gemäß Absatz 1 auszuüben.
2. Wird das in Absatz 1 genannte Recht ausgeübt, unterrichtet die Aufsichtsbehörde die betroffene Person zumindest darüber, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Aufsichtsbehörde erfolgt sind. Die Aufsichtsbehörde hat zudem die betroffene Person über ihr Recht auf einen Rechtsbehelf zu unterrichten.

*Artikel 16*

(...)

*Artikel 17*

***Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren***

Die Mitgliedstaaten können vorsehen, dass die Ausübung der Rechte nach den Artikeln 10a, 12 und 15 im Einklang mit dem einzelstaatlichen Recht erfolgt, wenn es um personenbezogene Daten in einem Gerichtsbeschluss oder einer Aufzeichnung oder einer Verfahrensakte geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden.

**KAPITEL IV**  
**FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER**  
**ABSCHNITT 1**  
**ALLGEMEINE PFLICHTEN**

*Artikel 18*

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

1. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass personenbezogene Daten in Übereinstimmung mit dieser Richtlinie verarbeitet werden. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
  - 1a. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den für die Verarbeitung Verantwortlichen umfassen.
2. (...)
3. (...)

*Artikel 19*

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

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche unter Berücksichtigung des Stands der Technik und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die persönlichen Rechte und Freiheiten sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch am Ende der Verarbeitung selbst der Verarbeitungstätigkeit und ihren Zielen angemessene technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, mit denen die wirksame Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung erreicht werden sollen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.
2. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden; dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne Eingriff einer natürlichen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

## *Artikel 20*

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

1. Die Mitgliedstaaten legen fest, dass in dem Fall, dass zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung personenbezogener Daten festlegen, sie gemeinsam für die Verarbeitung Verantwortliche sind. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche ihnen gemäß dieser Richtlinie obliegenden Aufgaben erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß Artikel 10a nachkommt, sofern und soweit die jeweiligen Aufgaben der für die Verarbeitung Verantwortlichen nicht durch Unions- oder einzelstaatliches Recht, dem die für die Verarbeitung Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung wird eine einzige Anlaufstelle für die betroffenen Personen angegeben. Die Mitgliedstaaten können angeben, welcher der gemeinsam für die Verarbeitung Verantwortlichen als einzige Anlaufstelle für die betroffenen Personen handeln kann, wenn es um die Ausübung ihrer Rechte geht.
  - 1a. Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 können die Mitgliedstaaten festlegen, dass die betroffene Person ihre Rechte im Rahmen der nach dieser Richtlinie erlassenen Vorschriften bei und gegenüber jedem einzelnen der für die Verarbeitung Verantwortlichen geltend machen kann.

## *Artikel 21*

### ***Auftragsverarbeiter***

1. Die Mitgliedstaaten tragen dafür Sorge, dass in dem Fall, dass eine Verarbeitung im Auftrag eines für die Verarbeitung Verantwortlichen erfolgt, dieser nur mit Auftragsverarbeitern arbeitet, die hinreichende Garantien dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Richtlinie erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
  - 1a. Die Mitgliedstaaten tragen dafür Sorge, dass der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des für die Verarbeitung Verantwortlichen in Anspruch nimmt. Im letzteren Fall unterrichtet der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der für die Verarbeitung Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

2. Die Mitgliedstaaten tragen dafür Sorge, dass die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unions- oder dem einzelstaatlichen Recht erfolgt, der bzw. das den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien von betroffenen Personen und die Pflichten und Rechte des für die Verarbeitung Verantwortlichen festgelegt sind und insbesondere vorgesehen ist, dass der Auftragsverarbeiter
  - a) nur auf Weisung des für die Verarbeitung Verantwortlichen handelt,
  - b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
  - c) den für die Verarbeitung Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,
  - d) alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen zurückgibt bzw. löscht – nach Wahl des für die Verarbeitung Verantwortlichen –, sofern nicht nach dem Unions- oder dem einzelstaatlichen Recht eine Verpflichtung zur Speicherung der Daten besteht,
  - e) dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt,
  - f) die in den Absätzen 1a und 2 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält.
- 2a. Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 2 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
3. Ein Auftragsverarbeiter, der unter Verstoß gegen diese Richtlinie die Zwecke und Mittel der Datenverarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als für die Verarbeitung Verantwortlicher.

## *Artikel 22*

### ***Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters***

Die Mitgliedstaaten tragen dafür Sorge, dass der Auftragsverarbeiter und jede dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unions- oder dem einzelstaatlichen Recht zur Verarbeitung verpflichtet sind.

## *Artikel 23*

### ***Verzeichnis von Verarbeitungstätigkeiten***

1. Die Mitgliedstaaten legen fest, dass jeder für die Verarbeitung Verantwortliche ein Verzeichnis aller Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten, die seiner Zuständigkeit unterliegen, führt. Dieses Verzeichnis enthält folgende Angaben:
  - a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen, etwaiger gemeinsam mit ihm Verantwortlicher und eines etwaigen Datenschutzbeauftragten,
  - b) die Verarbeitungszwecke,
  - c) die Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, einschließlich Empfängern in Drittländern,
  - ca) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien personenbezogener Daten,
  - cb) gegebenenfalls die Verwendung von Profiling,
  - d) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation,
  - da) Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die Daten bestimmt sind,
  - e) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
  - f) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 27 Absatz 1.

2. (...)
- 2a. Die Mitgliedstaaten legen fest, dass jeder Auftragsverarbeiter eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten führt, die Folgendes enthält:
- a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes für die Verarbeitung Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Datenschutzbeauftragten,
  - b) die Kategorien der Verarbeitungen, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden,
  - c) gegebenenfalls Angaben über etwaige Datenübermittlungen in Drittländer oder an internationale Organisationen einschließlich deren Namen, wenn diese ausdrücklich vom für die Verarbeitung Verantwortlichen in Auftrag gegeben wurden,
  - d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 27 Absatz 1.
- 2b. Die in den Absätzen 1 und 2a genannten Aufzeichnungen sind schriftlich zu führen; dies schließt elektronische Formate ein.
3. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter stellen der Aufsichtsbehörde die Aufzeichnung auf Anforderung zur Verfügung.

#### *Artikel 24*

#### ***Protokollierung***

1. Die Mitgliedstaaten tragen dafür Sorge, dass in Systemen automatisierter Verarbeitung zumindest über die folgenden Verarbeitungsvorgänge protokolliert werden: Erhebung, Veränderung, Abfrage, Weitergabe einschließlich Übertragung, Kombination oder Löschung. Die Protokolle über Abfragen und Weiterleitungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder weitergeleitet hat, und die Identität des Empfängers solcher Daten festzustellen.

2. Die Protokolle werden ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Daten sowie für Strafverfahren verwendet.
- 2a. Der für die Verarbeitung Verantwortliche sowie der Auftragsverarbeiter stellen die Protokolle der Aufsichtsbehörde auf Anforderung zur Verfügung.

*Artikel 25*

***Zusammenarbeit mit der Aufsichtsbehörde***

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter auf Verlangen mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.
2. (...)

*Artikel 25a*

***Datenschutz-Folgenabschätzung***

1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge, so legen die Mitgliedstaaten fest, dass der für die Verarbeitung Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.
2. Die Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Bestimmungen dieser Richtlinie eingehalten werden.

## Artikel 26

### ***Vorherige Konsultation der Aufsichtsbehörde***

1. Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateien die Aufsichtsbehörde konsultiert, wenn
  - a) aus einer Datenschutz-Folgenabschätzung gemäß Artikel 25a hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder
  - b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.
- 1a. Die Mitgliedstaaten tragen dafür Sorge, dass bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzesvorschriften oder von auf solchen Gesetzesvorschriften basierenden Regelungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, die Aufsichtsbehörde konsultiert wird.
2. Die Mitgliedstaaten legen fest, dass die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellen kann, die der Pflicht zur vorherigen Konsultation nach Absatz 1 unterliegen.
- 2a. Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche der Aufsichtsbehörde die Datenschutz-Folgenabschätzung gemäß Artikel 25a vorlegt und ihr auf Aufforderung alle sonstigen Informationen übermittelt, die sie benötigt, um die Ordnungsgemäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Sicherheitsgarantien bewerten zu können.
3. Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, wenn sie der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften stünde, insbesondere weil der für die Verarbeitung Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, dem für die Verarbeitung der Daten Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter spätestens sechs Wochen nach dem Antrag auf Konsultation schriftlich entsprechende Empfehlungen unterbreitet und ihre in Artikel 46 genannten Befugnisse ausüben kann. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um einen weiteren Monat verlängert werden. Kommt es zu einer Fristverlängerung, wird der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter innerhalb eines Monats nach Eingang des Antrags – auch über die Gründe für die Verzögerung – unterrichtet.

## **ABSCHNITT 2**

### **DATENSICHERHEIT**

#### *Artikel 27*

##### *Sicherheit der Verarbeitung*

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien von Daten im Sinne von Artikel 8.
2. Die Mitgliedstaaten legen im Hinblick auf die automatisierte Datenverarbeitung fest, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen ergreift, die Folgendes bezwecken:
  - a) Verwehrung des Zugangs zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, für Unbefugte (Zugangskontrolle),
  - b) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle),
  - c) Verhinderung der unbefugten Eingabe von Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
  - d) Verhinderung der Nutzung automatisierter Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
  - e) Gewährleistung, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
  - f) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übermittlungskontrolle),

- g) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
- h) Verhinderung, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
- i) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),
- j) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Dateneintegrität).

3. (...)

*Artikel 28*

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

- 1. Die Mitgliedstaaten legen fest, dass im Falle einer Verletzung des Schutzes personenbezogener Daten der für die Verarbeitung Verantwortliche diese der Aufsichtsbehörde ohne unangemessene Verzögerung und nach Möglichkeit binnen 72 Stunden nach Feststellung der Verletzung meldet, es sei denn, die Verletzung des Schutzes personenbezogener Daten dürfte voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führen. Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen.
- 2. Nach Feststellung einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter diese dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung.
- 3. Die Meldung gemäß Absatz 1 muss mindestens folgende Informationen enthalten:
  - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze,

- b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen,
  - c) (...)
  - d) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
  - e) eine Beschreibung der von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen negativen Auswirkungen.
- 3a. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, stellt der für die Verarbeitung Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.
4. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche etwaige Verletzungen des Schutzes personenbezogener Daten nach Absatz 1 unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentiert. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.
- 4a. Die Mitgliedstaaten tragen dafür Sorge, dass, soweit von der Schutzverletzung personenbezogene Daten betroffen sind, die von dem oder an den für die Verarbeitung Verantwortlichen eines anderen Mitgliedstaats übermittelt wurden, die in Absatz 3 genannten Informationen dem für die Verarbeitung Verantwortlichen jenes Mitgliedstaats ohne unangemessene Verzögerung übermittelt werden.
5. (...)
6. (...)

### *Artikel 29*

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

1. Die Mitgliedstaaten tragen dafür Sorge, dass, wenn die Verletzung des Schutzes personenbezogener voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, der für die Verarbeitung Verantwortliche die betroffene Person ohne unangemessene Verzögerung von der Verletzung benachrichtigt.

2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 28 Absatz 3 Buchstaben b, d und e genannten Informationen und Empfehlungen.
3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn
  - a) der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die betreffenden Daten für alle Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht werden, etwa durch Verschlüsselung, oder
  - b) der für die Verarbeitung Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht, oder
  - c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesen Fällen hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.
- 3a. Wenn der für die Verarbeitung Verantwortliche die Verletzung des Schutzes personenbezogener Daten nicht bereits der betroffenen Person mitgeteilt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, nach der die Verletzung zu einem hohen Risiko führen kann, von dem für die Verarbeitung Verantwortlichen verlangen, dies nachzuholen oder sie kann mit einem Beschluss feststellen, dass alle in Absatz 3 genannten Voraussetzungen erfüllt sind.
4. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 kann unter zu den in Artikel 10a Absatz 3 genannten Voraussetzungen und aus den dort genannten Gründen zurückgestellt, eingeschränkt oder unterlassen werden.

## **ABSCHNITT 3**

### **DATENSCHUTZBEAUFTRAGTER**

#### *Artikel 30*

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

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche einen Datenschutzbeauftragten benennt. Mitgliedstaaten können Gerichte und andere unabhängige Justizbehörden, die in ihrer gerichtlichen Eigenschaft handeln, von dieser Pflicht befreien.
2. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 32 genannten Aufgaben.
3. Ein Datenschutzbeauftragter kann für mehrere zuständige Behörden gemeinsam ernannt werden, wobei deren Organisationsstruktur und Größe Rechnung getragen wird.
- 3a. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und diese Daten der Aufsichtsbehörde mitteilt.

#### *Artikel 31*

##### ***Stellung des Datenschutzbeauftragten***

1. Die Mitgliedstaaten legen fest, dass der für die Verarbeitung Verantwortliche sicherstellt, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in die Behandlung aller mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
2. Der für die Verarbeitung Verantwortliche unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 32, indem er die hierfür erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

*Artikel 32*

***Aufgaben des Datenschutzbeauftragten***

Die Mitgliedstaaten tragen dafür Sorge, dass der für die Verarbeitung Verantwortliche den Datenschutzbeauftragten mit mindestens folgenden Aufgaben betraut:

- a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen und der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten nach dieser Richtlinie sowie anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten,
- b) Überwachung der Einhaltung dieser Richtlinie, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten sowie der Strategien des für die Verarbeitung Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,
- c) (...)
- d) (...)
- e) (...)
- f) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 25a,
- g) Zusammenarbeit mit der Aufsichtsbehörde,
- h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 26, und gegebenenfalls Beratung zu allen sonstigen Fragen.

# KAPITEL V

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN AN DRITTLÄNDER

### ODER INTERNATIONALE ORGANISATIONEN

#### Artikel 33

##### *Allgemeine Grundsätze für die Übermittlung personenbezogener Daten*

1. Die Mitgliedstaaten sehen vor, dass jedwede von einer zuständigen Behörde vorgenommene Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, einschließlich der Weitergabe an ein anderes Drittland oder eine andere internationale Organisation, nur unter Einhaltung der nach Maßgabe anderer Bestimmungen dieser Richtlinie erlassenen nationalen Bestimmungen, zulässig ist, wenn die in diesem Kapitel festgelegten Bedingungen eingehalten werden, nämlich
  - a) die Übermittlung für die in Artikel 1 Absatz 1 genannten Zwecke erforderlich ist und
  - b) (...);
  - c) die Daten an einen für die Verarbeitung Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde ist, übermittelt werden und
  - d) in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor in Einklang mit seinem nationalen Recht genehmigt hat und
  - e) die Kommission gemäß Artikel 34 festgestellt hat, dass das betreffende Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet oder, wenn kein Angemessenheitsbeschluss gemäß Artikel 34 vorliegt, geeignete Garantien im Sinne des Artikels 35 erbracht werden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß Artikel 34 vorliegt und keine geeigneten Garantien im Sinne des Artikels 35 vorhanden sind, Ausnahmen für Sonderfälle gemäß Artikel 36 anwendbar sind,

- ea) im Fall der Weitergabe an ein anderes Drittland oder eine andere internationale Organisation genehmigt die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, oder eine andere zuständige Behörde des gleichen Mitgliedstaats die Weitergabe nach gebührender Berücksichtigung sämtlicher relevanter Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Datenübermittlung und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weitergegeben werden.
2. Die Mitgliedstaaten sehen vor, dass Übermittlungen ohne vorherige Genehmigung durch einen anderen Mitgliedstaat gemäß Buchstabe d nur dann zulässig sind, wenn die Übermittlung der personenbezogenen Daten erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlands oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die Behörde, die für die Erteilung der vorherigen Genehmigung zuständig ist, wird unverzüglich unterrichtet.
- 3a. Sämtliche Bestimmungen dieses Kapitels werden angewendet, um sicherzustellen, dass das durch diese Richtlinie garantierte Schutzniveau für natürliche Personen nicht untergraben wird.

#### *Artikel 34*

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

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn die Kommission festgestellt hat, dass das betreffende Drittland bzw. ein Gebiet oder ein oder mehrere spezifische Sektoren dieses Drittlands oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.
2. Bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigt die Kommission insbesondere

- a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und der Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, juristische Präzedenzfälle sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame administrative und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,
  - b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und
  - c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Rechtsinstrumenten sowie aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.
3. Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 bietet. In dem Durchführungsrechtsakt wird ein Mechanismus für die regelmäßige Überprüfung vorgesehen, die mindestens alle vier Jahre erfolgt und bei allen relevanten Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde oder die dort genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 57 Absatz 2 genannten Prüfverfahren erlassen.

4. (...)
- 4a. Die Kommission überwacht kontinuierlich die Entwicklungen in Drittländern und internationalen Organisationen, die die Wirksamkeit der nach Absatz 3 erlassenen Beschlüsse beeinträchtigen könnten.
5. Die Kommission wird durch Beschluss feststellen, dass ein Drittland bzw. ein Gebiet oder ein spezifischer Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 mehr bietet, wenn dies aus verfügbaren Informationen insbesondere nach der Überprüfung gemäß Absatz 3 hervorgeht, und erforderlichenfalls den in Absatz 3 genannten Beschluss ohne rückwirkende Kraft widerrufen, ändern oder aussetzen. Die Durchführungsrechtsakte werden gemäß dem in Artikel 57 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen gemäß dem in Artikel 57 Absatz 3 genannten Verfahren erlassen.
- 5a. Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem Beschluss nach Absatz 5 geführt hat.
6. Die Mitgliedstaaten sehen vor, dass Übermittlungen personenbezogener Daten an das betreffende Drittland bzw. an das Gebiet oder den spezifischen Sektor dieses Drittlands oder an die betreffende internationale Organisation gemäß den Artikeln 35 bis 36 durch einen Beschluss nach Absatz 5 nicht berührt werden.
7. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer bzw. Gebiete und spezifischen Sektoren eines Drittlands und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese ein beziehungsweise kein angemessenes Schutzniveau für personenbezogene Daten bieten.
8. (...)

## *Artikel 35*

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

1. Liegt kein Beschluss nach Artikel 34 vor, so sehen die Mitgliedstaaten vor, dass eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen darf, wenn
  - a) in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
  - b) der für die Verarbeitung Verantwortliche alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.
- 1a. Der für die Verarbeitung Verantwortliche unterrichtet die Aufsichtsbehörde über die Übermittlungen gemäß Absatz 1 Buchstabe b.
2. Übermittlungen gemäß Absatz 1 Buchstabe b müssen dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übertragung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt werden.

## *Artikel 36*

### ***Ausnahmen für Sonderfälle***

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 34 vorliegt noch geeignete Garantien nach Artikel 35 bestehen, sehen die Mitgliedstaaten vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig ist, wenn
  - a) die Übermittlung zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist oder
  - b) die Übermittlung nach dem Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, zur Wahrung berechtigter Interessen der betroffenen Person notwendig ist oder

- c) die Übermittlung zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlands notwendig ist oder
  - d) die Übermittlung im Einzelfall für die in Artikel 1 Absatz 1 genannten Zwecke erforderlich ist oder
  - e) die Übermittlung im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Artikel 1 Absatz 1 genannten Zwecken erforderlich ist.
2. Personenbezogene Daten dürfen nicht übermittelt werden, wenn die übermittelnde zuständige Behörde feststellt, dass Grundrechte und -freiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung im Sinne des Absatzes 1 Buchstaben d und e überwiegen.
  3. Übermittlungen gemäß Absatz 1 müssen dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übertragung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt werden.

*Artikel 36aa*

***Übermittlung personenbezogener Daten an in Drittländern niedergelassene Empfänger***

1. Abweichend von Artikel 33 Absatz 1 Buchstabe c und unbeschadet der in Absatz 2 genannten internationalen Übereinkünfte können die Union oder die Mitgliedstaaten vorsehen, dass die in Artikel 3 Absatz 14 Buchstabe a genannten zuständigen Behörden im speziellen Einzelfall nur dann personenbezogene Daten direkt an in Drittstaaten niedergelassene Empfänger übermitteln dürfen, wenn die übrigen Bestimmungen dieser Richtlinie eingehalten werden und folgende Voraussetzungen gegeben sind:
  - a) Die Übermittlung ist für die Ausübung einer Aufgabe der übermittelnden zuständigen Behörde gemäß dem Unions- oder dem einzelstaatlichen Recht für die in Artikel 1 Absatz 1 genannten Zwecke unbedingt erforderlich und
  - b) die übermittelnde zuständige Behörde stellt fest, dass im konkreten Fall keine Grundrechte und -freiheiten der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen, und

- c) die übermittelnde zuständige Behörde hält die Übermittlung an eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland für wirkungslos oder ungeeignet, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
  - d) die zuständige Behörde in dem Drittland wird ohne unangemessene Verzögerung unterrichtet, es sei denn, dies ist wirkungslos oder ungeeignet, und
  - e) die übermittelnde zuständige Behörde teilt dem Empfänger den festgelegten Zweck oder die festgelegten Zwecke mit, für die die personenbezogenen Daten nur dann durch diesen verarbeitet werden, wenn eine derartige Verarbeitung erforderlich ist.
2. Eine internationale Übereinkunft im Sinne des Absatzes 1 ist jede in Kraft befindliche bilaterale oder multilaterale internationale Übereinkunft zwischen Mitgliedstaaten und Drittländern im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.
- 2a. Die übermittelnde zuständige Behörde unterrichtet die Aufsichtsbehörde über die Übermittlungen gemäß diesem Artikel.
- 2b. Übermittlungen gemäß Absatz 1 müssen dokumentiert werden.

*Artikel 37*

(...)

*Artikel 38*

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

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Mitgliedstaaten geeignete Maßnahmen zur
  - a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,
  - b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch 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 zum Schutz personenbezogener Daten dienen,
  - d) Förderung des Austausches und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten einschließlich Zuständigkeitskonflikten mit Drittländern.
2. (...)

# **KAPITEL VI**

## **UNABHÄNGIGKEIT DER AUFSICHTSBEHÖRDEN**

### **ABSCHNITT 1**

#### **UNABHÄNGIGKEIT**

##### *Artikel 39*

###### ***Aufsichtsbehörde***

1. Jeder Mitgliedstaat trägt dafür Sorge, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Richtlinie zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten geschützt werden und der freie **Verkehr** personenbezogener Daten in der Union erleichtert wird.
  - 1a. Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Richtlinie in der gesamten Union. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden mit der Kommission sowie der Aufsichtsbehörden untereinander gemäß Kapitel VII.
2. Die Mitgliedstaaten können vorsehen, dass die gemäß der Verordnung (EU) XXX in den Mitgliedstaaten errichtete Aufsichtsbehörde die in dieser Richtlinie genannte Aufsichtsbehörde sein kann und die Verantwortung für die Aufgaben der nach Absatz 1 zu errichtenden Aufsichtsbehörde übernimmt.
3. Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Europäischen Datenschutzausschuss vertreten.

##### *Artikel 40*

###### ***Unabhängigkeit***

1. Die Mitgliedstaaten stellen sicher, dass jede Aufsichtsbehörde bei der Erfüllung der Aufgaben und der Ausübung der Befugnisse, die ihr gemäß dieser Richtlinie übertragen werden, völlig unabhängig handelt.

2. Die Mitgliedstaaten tragen dafür Sorge, dass das Mitglied oder die Mitglieder jeder Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Richtlinie weder direkter noch indirekter Beeinflussung von außen unterliegen und weder um Weisung ersuchen noch Weisungen entgegennehmen.
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. (...)
5. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.
6. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde über eigenes Personal verfügt, das von ihr ausgewählt wird und ausschließlich der Leitung des Mitglieds oder der Mitglieder der Aufsichtsbehörde untersteht.
7. Die Mitgliedstaaten stellen sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass jede Aufsichtsbehörde über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

*Artikel 41*

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

1. Die Mitgliedstaaten tragen dafür Sorge, dass jedes Mitglied einer Aufsichtsbehörde vom Parlament oder von der Regierung oder vom Staatsoberhaupt des betreffenden Mitgliedstaats oder von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird, im Wege eines transparenten Verfahrens ernannt wird.
2. Das Mitglied oder die Mitglieder müssen über die für die Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.
3. Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder seiner Enthebung aus dem Amt gemäß dem Recht des betroffenen Mitgliedstaats.
4. Ein Mitglied kann seines Amtes nur enthoben werden, wenn er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Erfüllung seiner Aufgaben nicht mehr erfüllt.
5. (...)

*Artikel 42*

***Errichtung der Aufsichtsbehörde***

1. Jeder Mitgliedstaat regelt durch Gesetz
  - a) die Errichtung jeder Aufsichtsbehörde,
  - b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde,
  - c) die Vorschriften und Verfahren für die Ernennung der Mitglieder jeder Aufsichtsbehörde,

- d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde, die mindestens vier Jahre beträgt; dies gilt nicht für die erste Amtszeit nach Inkrafttreten dieser Richtlinie, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist,
  - e) die Frage, ob und – wenn ja – wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können,
  - f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Leistungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.
  - g) (...)
- 1a Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Erfüllung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während ihrer Amtszeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstöße gegen diese Richtlinie.

*Artikel 43*

(...)

## **ABSCHNITT 2**

### **ZUSTÄNDIGKEIT, AUFGABEN UND BEFUGNISSE**

#### *Artikel 44*

##### ***Zuständigkeit***

1. Die Mitgliedstaaten sehen vor, dass jede Aufsichtsbehörde dafür zuständig ist, im Hoheitsgebiet ihres eigenen Mitgliedstaats die Aufgaben zu erfüllen und die Befugnisse auszuüben, die ihr gemäß dieser Richtlinie übertragen werden.
2. Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde nicht für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. Die Mitgliedstaaten können vorsehen, dass die Aufsichtsbehörde nicht für die Überwachung der von anderen unabhängigen Gerichtsbehörden im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen zuständig ist.

#### *Artikel 45*

##### ***Aufgaben***

1. Die Mitgliedstaaten tragen dafür Sorge, dass jede Aufsichtsbehörde in ihrem Hoheitsgebiet
  - a) die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt;
  - aa) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten sensibilisiert und sie darüber aufklärt;
  - ab) im Einklang mit dem einzelstaatlichen Recht das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten berät;
  - ac) die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter über die ihnen aus dieser Richtlinie entstehenden Pflichten aufklärt;

- ad) auf Antrag jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Richtlinie zur Verfügung stellt und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeitet;
  - b) sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 53 befasst, den Gegenstand der Beschwerde in angemessenem Umfang untersucht und den Beschwerdeführer innerhalb einer angemessenen Frist über den Stand und das Ergebnis der Untersuchung unterrichtet, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
  - c) die Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 15a überprüft und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß Artikel 15a Absatz 2 unterrichtet oder ihr die Gründe mitteilt, aus denen die Überprüfung nicht vorgenommen wurde;
  - d) mit anderen Aufsichtsbehörden zusammenarbeitet, auch durch Informationsaustausch, und ihnen Amtshilfe leistet, um die einheitliche Anwendung und Durchsetzung dieser Richtlinie zu gewährleisten;
  - e) Untersuchungen über die Anwendung dieser Richtlinie durchführt, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;
  - f) relevante Entwicklungen verfolgt, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie;
  - g) (...)
  - h) Beratung in Bezug auf die in Artikel 26 genannten Verarbeitungsvorgänge leistet;
  - i) Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses leistet.
2. (...)
3. (...)

4. Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe b genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.
5. Die Leistungen jeder Aufsichtsbehörde sind für die betroffene Person und für den Datenschutzbeauftragten unentgeltlich.
6. Bei offenkundig unbegründeten oder – besonders wegen ihrer Häufung – unverhältnismäßigen Anträgen kann die Aufsichtsbehörde ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offensichtlich unbegründeten oder unverhältnismäßigen Charakter des Antrags.

*Artikel 46*

***Befugnisse***

1. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt, mindestens aber über die Befugnis, von dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter Zugriff auf alle personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten.
  - a) (...)
  - b) (...)
  - c) (...)
  - 1.a) Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die folgenden verfügt, die es ihr gestatten,
    - a) einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die nach dieser Richtlinie erlassenen Vorschriften verstößen;

- b) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung, Einschränkung oder Löschung von Daten gemäß Artikel 15;
  - c) eine vorübergehende oder endgültige Einschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.
- 1.b) Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde über wirksame Beratungsbefugnisse verfügt, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach Artikel 26 den für die Verarbeitung Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem einzelstaatlichen Recht an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.
2. Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse gemäß diesem Artikel erfolgt vorbehaltlich angemessener Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta der Grundrechte der Europäischen Union.
3. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen nach dieser Richtlinie erlassene Vorschriften den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um den nach dieser Richtlinie erlassenen Vorschriften Geltung zu verschaffen.

#### *Artikel 46a*

#### ***Meldung von Verstößen***

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

*Artikel 47*

***Tätigkeitsbericht***

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der verhängten Sanktionen enthalten kann. Der Bericht wird dem nationalen Parlament, der Regierung und anderen nach dem einzelstaatlichen Recht bestimmten Behörden übermittelt. Er wird der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

## **KAPITEL VII**

### **ZUSAMMENARBEIT**

#### *Artikel 48*

##### ***Gegenseitige Amtshilfe***

1. Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörden einander zweckdienliche Informationen übermitteln und Amtshilfe gewähren, um diese Richtlinie einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.
2. Die Mitgliedstaaten tragen dafür Sorge, dass jede Aufsichtsbehörde alle geeigneten Maßnahmen ergreift, um dem Ersuchen einer anderen Aufsichtsbehörde ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu kann insbesondere auch die Übermittlung zweckdienlicher Informationen über die Durchführung einer Untersuchung gehören.
  - 2a. Das Amtshilfeersuchen enthält alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.
  - 2b. Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn
    - a) sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder
    - b) ein Eingehen auf das Ersuchen gegen die Bestimmungen dieser Richtlinie oder gegen das Unionsrecht oder das mitgliedstaatliche Recht, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt, verstößen würde.
3. 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. Bei einer Ablehnung gemäß Absatz 2b erläutert sie ihre Gründe für die Ablehnung des Ersuchens.

- 3a. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.
- 3b. Maßnahmen, die aufgrund eines Amtshilfeersuchens getroffen werden, sind unentgeltlich. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.
- 3c. 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 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 57 Absatz 2 genannten Prüfverfahren erlassen.

#### *Artikel 49*

#### ***Aufgaben des Europäischen Datenschutzausschusses***

1. Der mit der Verordnung (EU) ..../XXX eingesetzte Europäische Datenschutzausschuss nimmt in Bezug auf Verarbeitungsvorgänge im Anwendungsbereich dieser Richtlinie folgende Aufgaben wahr:
  - a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, auch zu etwaigen Vorschlägen zur Änderung dieser Richtlinie;
  - b) von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission vorgenommene Prüfung von Fragen, die die Anwendung dieser Richtlinie betreffen, und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Richtlinie;
  - ba) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 46 Absätze 1 und 1b;

- bb) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b für die Feststellung von Verletzungen des Datenschutzes und die Festlegung der ungebührlichen Verzögerung im Sinne des Artikels 28 Absätze 1 und 2 und für die konkreten Umstände, unter denen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben;
  - bc) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b in Bezug auf die Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen im Sinne des Artikels 29 Absatz 1 zur Folge hat;
  - c) Überprüfung der praktischen Anwendung der unter den Buchstaben b und ba genannten Leitlinien, Empfehlungen und bewährten Verfahren;
  - d) Abgabe einer Stellungnahme gegenüber der Kommission zur Beurteilung der Angemessenheit des in einem Drittland oder einer internationalen Organisation gebotenen Schutzniveaus sowie zur Beurteilung der Frage, ob das Drittland, das Gebiet, die internationale Organisation oder der spezifische Sektor kein angemessenes Schutzniveau mehr bietet. Zu diesem Zweck versorgt die Kommission den Europäischen Datenschutzausschuss mit allen erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlandes, mit dem Gebiet oder Verarbeitungssektor dieses Drittlands oder mit der internationalen Organisation.
  - e) Förderung der Zusammenarbeit und eines wirksamen bilateralen und multilateralen Austauschs von Informationen und Verfahren zwischen den Aufsichtsbehörden;
  - f) Förderung von Schulungsprogrammen und Erleichterung des Personalaustauschs zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder internationalen Organisationen;
  - g) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzzvorschriften und -praxis 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 angeben.

3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 57 Absatz 1 genannten Ausschuss weiter und veröffentlicht sie.
4. Die Kommission setzt den Europäischen Datenschutzausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die von ihm herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren ergriffen hat.

## **KAPITEL VIII**

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

#### *Artikel 50*

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

1. Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs das Recht hat, bei einer einzigen Aufsichtsbehörde eine Beschwerde einzureichen, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften steht.
  - 1a. Die Mitgliedstaaten sehen vor, dass eine Beschwerde, die nicht bei der gemäß Artikel 44 Absatz 1 zuständigen Aufsichtsbehörde eingereicht wird, von der Aufsichtsbehörde, bei der die Beschwerde eingelegt wird, ohne ungebührliche Verzögerung an die zuständige Aufsichtsbehörde übermittelt wird. Die betroffene Person wird über die Übermittlung unterrichtet.
  - 1b. Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, auf Ersuchen der betroffenen Person weitere Unterstützung leistet.
2. (...)
- 2a. Die betroffene Person wird von der zuständigen Aufsichtsbehörde über den Stand und das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 51 unterrichtet.
3. (...)

#### *Artikel 51*

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

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

2. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach Artikel 44 Absatz 1 zuständige Aufsichtsbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 50 erhobenen Beschwerde in Kenntnis gesetzt hat.
3. Die Mitgliedstaaten sehen vor, dass für Verfahren gegen eine Aufsichtsbehörde die Gerichte des Mitgliedstaats zuständig sind, in dem die Aufsichtsbehörde ihren Sitz hat.

### *Artikel 52*

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

Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines verfügbaren administrativen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 50 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn sie der Ansicht ist, dass die Rechte, die ihr aufgrund von nach dieser Richtlinie erlassenen Vorschriften zustehen, infolge einer nicht mit diesen Vorschriften im Einklang stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

### *Artikel 53*

#### ***Vertretung von betroffenen Personen***

1. Die Mitgliedstaaten sehen im Einklang mit dem nationalen Verfahrensrecht vor, dass die betroffene Person das Recht hat, eine Einrichtung, eine Organisation oder eine Vereinigung, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist und keinen Erwerbszweck verfolgt, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die auf dem Gebiet des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und in ihrem Namen die in den Artikeln 50, 51 und 52 genannten Rechte wahrzunehmen.
2. (...)
3. (...)

*Artikel 54*

***Recht auf Schadenersatz***

1. Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen Handlung, die mit den nach Maßgabe dieser Richtlinie erlassenen innerstaatlichen Vorschriften nicht zu vereinbaren ist, ein materieller oder immaterieller Schaden entstanden ist, Recht auf Schadenersatz seitens des für die Verarbeitung Verantwortlichen oder jeder sonst nach innerstaatlichem Recht zuständigen Stelle hat.
2. (...)
3. (...)

*Artikel 55*

***Sanktionen***

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

## **KAPITEL IX**

### **DURCHFÜHRUNGSRECHTSAKTE**

#### *Artikel 56*

( ... )

#### *Artikel 57*

##### ***Ausschussverfahren***

1. Die Kommission wird von dem mit Artikel 87 der Verordnung (EU) XXX eingesetzten Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.
2. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.
3. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

## **KAPITEL X**

### **SCHLUSSBESTIMMUNGEN**

#### *Artikel 58*

##### ***Aufhebung***

1. Der Rahmenbeschluss 2008/977/JI des Rates wird mit Wirkung von dem in Artikel 62 Absatz 1 genannten Zeitpunkt aufgehoben.
2. Verweise auf den in Absatz 1 genannten aufgehobenen Rahmenbeschluss gelten als Verweise auf diese Richtlinie.

#### *Artikel 59*

##### ***Verhältnis zu bestehenden Rechtsakten der Union für die justizielle Zusammenarbeit in Strafsachen und für die polizeiliche Zusammenarbeit***

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

#### *Artikel 60*

##### ***Verhältnis zu bestehenden internationalen Übereinkünften im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit***

Internationale Übereinkünfte, die die Weitergabe personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, von den Mitgliedstaaten vor dem Inkrafttreten dieser Richtlinie geschlossen wurden und im Einklang mit dem vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht stehen, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

*Artikel 61*

**Bewertung**

1. Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht über die Bewertung und Überprüfung dieser Richtlinie vor.
  - 1a. Im Rahmen dieser Bewertungen und Überprüfungen prüft die Kommission insbesondere die Anwendung und Wirkung der Bestimmungen des Kapitels V über die Weitergabe personenbezogener Daten an Drittländer oder internationale Organisationen und vor allem die Beschlüsse nach Artikel 34 Absätze 3 und Artikel 36aa.
  - 1b. Für die in den Absätzen 1 und 1a genannten Zwecke kann die Kommission Informationen von den Mitgliedstaaten und den Aufsichtsbehörden einholen.
  - 1c. Bei den in den Absätzen 1 und 1a genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates sowie der anderen einschlägigen Stellen und Quellen.
  - 1d. Der erste Bericht wird spätestens vier Jahre nach Ablauf der Umsetzungsfrist für diese Richtlinie vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Der Bericht wird veröffentlicht.
  - 1e. Die Kommission legt geeignete Vorschläge zur Änderung dieser Richtlinie und zur Anpassung anderer Rechtsinstrumente vor, die sich insbesondere unter Berücksichtigung der Entwicklung der Informationstechnologie und der Fortschritte in der Informationsgesellschaft als notwendig erweisen können.
2. Die Kommission überprüft innerhalb von drei Jahren nach Inkrafttreten dieser Richtlinie andere Rechtsakte der Europäischen Union über die Verarbeitung personenbezogener Daten durch die zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke, einschließlich der auf der Grundlage von Artikel 59 erlassenen Rechtsakte, um festzustellen, inwieweit eine Anpassung an diese Richtlinie erforderlich ist, und um gegebenenfalls die erforderlichen Vorschläge zur Änderung dieser Rechtsakte zu unterbreiten, damit ein einheitliches Vorgehen beim Schutz personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie gewährleistet ist.
3. (...)

*Artikel 62*

***Umsetzung***

1. Die Mitgliedstaaten erlassen und veröffentlichen spätestens [Datum/zwei Jahre nach Inkrafttreten] die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit. Sie wenden diese Vorschriften ab xx.xx.201x [Datum/zwei Jahre nach Inkrafttreten] an.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

- 1a. Abweichend von Absatz 1 können die Mitgliedstaaten vorsehen, dass in Ausnahmefällen, in denen dies mit einem unverhältnismäßigen Aufwand verbunden ist, die vor dem Inkrafttreten dieser Richtlinie eingerichteten automatisierten Verarbeitungssysteme innerhalb von sieben Jahren nach dem Inkrafttreten dieser Richtlinie mit Artikel 24 Absatz 1 in Einklang gebracht werden müssen.
- 1b. In Ausnahmefällen kann ein Mitgliedstaat ein vor dem Inkrafttreten dieser Richtlinie eingerichtetes automatisiertes Verarbeitungssystem innerhalb einer bestimmten Frist nach Ablauf der in Absatz 1a genannten Frist mit Artikel 24 Absatz 1 in Einklang bringen, wenn hierdurch sonst schwerwiegende Schwierigkeiten für den Betrieb dieses automatisierten Verarbeitungssystems entstehen würden. Er begründet gegenüber der Kommission, weshalb diese schwerwiegenden Schwierigkeiten entstehen würden und weshalb er das automatisierte Verarbeitungssystem innerhalb der bestimmten Frist mit Artikel 24 Absatz 1 in Einklang bringen wird. Diese Frist darf die in Absatz 1a genannte Frist um höchstens drei Jahre überschreiten.
2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

*Artikel 63*

***Inkrafttreten***

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

*Artikel 64*

***Adressaten***

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu ... am ...

*Im Namen des Europäischen Parlaments*

*Der Präsident*

*Im Namen des Rates*

*Der Präsident*