RICHTLINIEN

RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren, ([2])

in Erwägung nachstehender Gründe:

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

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Richtlinie soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen.

(3) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass für die Ausübung von Tätigkeiten wie die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung in einem noch nie dagewesenen Umfang personenbezogene Daten verarbeitet werden können.

(4) Der freie Verkehr personenbezogener Daten zwischen den zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen, sollte erleichtert und dabei gleichzeitig ein hohes Schutzniveau für personenbezogene Daten gewährleistet werden. Angesichts dieser Entwicklungen bedarf es des Aufbaus eines soliden und kohärenteren Rechtsrahmens für den Schutz personenbezogener Daten in der Union, die konsequent durchgesetzt werden.

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

([1]) ABl. C 391, 18.12.2012, S. 127.
([2]) Standpunkt des Europäischen Parlamentes vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlamentes vom 14. April 2016.
([3]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

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

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

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

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

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

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

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

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

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

Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist. Die Mitgliedstaaten können die zuständigen Behörden mit anderen Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, als sie in den Anwendungsbereich des Unionsrechts fällt.

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

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

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

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

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

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

(19) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [1] gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften gemäß der Verordnung (EU) 2016/679 angepasst werden.

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

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

(21) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologischen Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

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

(23) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen-, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden. Angesichts der Komplexität und Sensibilität genetischer Informationen besteht ein hohes Missbrauchs- und Wiederverwendungsrisiko für unterschiedliche Zwecke durch den Verantwortlichen. Jede Diskriminierung aufgrund genetischer Merkmale sollte grundsätzlich verboten sein.

(24) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Vormerkung zur Erbringung und der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([1]) erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

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

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

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

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

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

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

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

(28) Um stets eine sichere Verarbeitung zu gewährleisten und Verarbeitungen, die gegen diese Richtlinie verstoßen, zu verhindern, sollten personenbezogene Daten so verarbeitet werden, dass ein Maß an Sicherheit und Vertraulichkeit gegeben ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können, und dass die Verarbeitung den Stand der verfügbaren Technik, die Kosten für ihre Einführung im Verhältnis zu den von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden personenbezogenen Daten berücksichtigt.

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

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

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

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

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

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

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

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

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

(37) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(50) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Richtlinie stehen. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Im Rahmen der von ihm ergriffenen Maßnahmen sollte der Verantwortliche auch spezifische Garantien für die Verarbeitung personenbezogener Daten von schutzbedürftigen natürlichen Personen, wie etwa Kindern, ausarbeiten und implementieren.

(51) Risiken für die Rechte und Freiheiten der natürlichen Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Datenverarbeitung hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten, der unbefugten Umkehr der Pseudonymisierung oder anderen

erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, die Religion oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, wenn genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über die Gesundheit oder Daten über das Sexualleben und sexuelle Orientierung oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert und prognostiziert werden, um ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft.

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

(53) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Richtlinie erfüllt werden. Die Umsetzung dieser Maßnahmen sollte nicht ausschließlich von wirtschaftlichen Erwägungen abhängig gemacht werden. Um die Einhaltung dieser Richtlinie nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun. Hat der Verantwortliche eine Datenschutz-Folgenabschätzung gemäß dieser Richtlinie vorgenommen, sollten die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt werden. Die Maßnahmen könnten u. a. aus einer möglichst frühen Pseudonymisierung bestehen. Gerade durch die Pseudonymisierung für die Zwecke dieser Richtlinie könnte der freie Verkehr personenbezogener Daten im Raum der Freiheit, der Sicherheit und des Rechts erleichtert werden.

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

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

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

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

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

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

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

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

(62) Natürliche Personen, sollten unverzüglich benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, damit sie die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen des Schutzes von Daten zu treffen. In Ausnahmefällen könnte die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen natürlichen Person unterbleiben, wenn ein Aufschub oder eine Einschränkung dieser Benachrichtigung nicht ausreicht, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen.

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

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

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

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

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

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

(68) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des Drittlandes zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen

Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss (im Folgenden „Ausschuss") konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet. Die Kommission sollte ferner alle maßgeblichen Angemessenheitsbeschlüsse berücksichtigen, die sie nach Artikel 45 der Verordnung (EU) 2016/679 angenommen hat.

(69) Die Kommission sollte die Wirksamkeit von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem spezifischen Sektor in einem Drittland oder einer internationalen Organisation überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung ihrer Wirkungsweise vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen.

(70) Die Kommission sollte auch feststellen können, dass ein Drittland, ein Gebiet oder ein spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Richtlinie in Bezug auf Datenübermittlung vorbehaltlich geeigneter Garantien und Ausnahmen für bestimmte Fälle werden erfüllt. Es sollten Verfahren für Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

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

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

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

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

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

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

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

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

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

(79) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Recht der Mitgliedstaaten geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des betreffenden Mitgliedstaats auf Vorschlag der Regierung oder eines Regierungsmitglieds oder des Parlaments oder dessen Kammer oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder integer handeln, von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollte ihr Personal von der Aufsichtsbehörde selbst ausgewählt werden; dabei kann eine unabhängige, nach dem Recht des Mitgliedstaats betraute Stelle eingeschaltet werden.

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

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

(82) Um die wirksame, zuverlässige und einheitliche Überwachung der Einhaltung und Durchsetzung dieser Richtlinie in der gesamten Union gemäß dem AEUV in der Auslegung durch den Gerichtshof sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse, die notwendige Instrumente zur Erfüllung ihrer Aufgaben darstellen. Ihre Befugnisse dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschließlich der Ermittlung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren. Unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten sollten die Aufsichtsbehörden außerdem die Befugnis haben, Verstöße gegen diese Richtlinie den Justizbehörden zur Kenntnis zu bringen oder Gerichtsverfahren anzustrengen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Richtlinie geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf die betroffene Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für sie zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Recht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Der Erlass eines rechtsverbindlichen Beschlusses sollte in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, einer gerichtlichen Überprüfung unterliegen.

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

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

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

(86) Jede natürliche oder juristische Person sollte das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Dieses Recht umfasst jedoch nicht andere — rechtlich nicht bindende — Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Recht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit maßgeblichen Sach- und Rechtsfragen zu prüfen, einschließt.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(99) Nach Artikel 6a des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Bestimmungen dieser Richtlinie über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, für das Vereinigte Königreich und Irland nicht bindend, wenn das Vereinigte Königreich und Irland nicht durch die Vorschriften gebunden sind, die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften eingehalten werden müssen.

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

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

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

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

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

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

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

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

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

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

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

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

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(2) Gemäß dieser Richtlinie haben die Mitgliedstaaten

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

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

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

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

Artikel 2

Anwendungsbereich

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

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

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

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

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

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

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

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

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

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

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

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

7. „zuständige Behörde“

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

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

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

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

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

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

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

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

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

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

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

KAPITEL II

Grundsätze

Artikel 4

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor dass personenbezogene Daten

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

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

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

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

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

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

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

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

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

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

Artikel 5

Fristen für die Speicherung und Überprüfung

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

Artikel 6

Unterscheidung verschiedener Kategorien betroffener Personen

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

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

b) verurteilte Straftäter,

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

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

Artikel 7

Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der personenbezogenen Daten

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

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

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

Artikel 8

Rechtmäßigkeit der Verarbeitung

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

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

Artikel 9

Besondere Verarbeitungsbedingungen

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

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

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

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

Artikel 10

Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

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

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

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

Artikel 11

Automatisierte Entscheidungsfindung im Einzelfall

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

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

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

KAPITEL III

Rechte der betroffenen Person

Artikel 12

Mitteilungen und Modalitäten für die Ausübung der Rechte der betroffenen Person

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

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

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

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

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

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

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

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

Artikel 13

Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen

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

a) den Namen und die Kontaktdaten des Verantwortlichen,

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,

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

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

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

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

a) die Rechtsgrundlage der Verarbeitung,

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

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

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

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

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

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

c) zum Schutz der öffentlichen Sicherheit,

d) zum Schutz der nationalen Sicherheit,

e) zum Schutz der Rechte und Freiheiten anderer.

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

Artikel 14

Auskunftsrecht der betroffenen Person

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

a) die Zwecke der Verarbeitung und deren Rechtsgrundlage,

b) die Kategorien personenbezogener Daten, die verarbeitet werden,

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

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

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

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

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

Artikel 15

Einschränkung des Auskunftsrechts

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

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

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

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

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

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

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

Artikel 16

Recht auf Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung

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

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

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

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

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

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

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

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

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

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

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

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

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

Artikel 17

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

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

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

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

Artikel 18

Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren

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

KAPITEL IV

Verantwortlicher und Auftragsverarbeiter

Abschnitt 1

Allgemeine Pflichten

Artikel 19

Pflichten des Verantwortlichen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

Artikel 20

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Artikel 21

Gemeinsam Verantwortliche

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

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

Artikel 22

Auftragsverarbeiter

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

(2) Die Mitgliedstaaten sehen vor, dass der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt. Im Fall einer allgemeinen schriftlichen Genehmigung unterrichtet der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Mitgliedstaaten sehen vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und der den Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) nur auf Weisung des Verantwortlichen handelt,

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

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

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

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

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

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

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

Artikel 23

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

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

Artikel 24

Verzeichnis von Verarbeitungstätigkeiten

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

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

b) die Zwecke der Verarbeitung,

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

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

e) gegebenenfalls die Verwendung von Profiling,

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

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

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

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

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

a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Datenschutzbeauftragten,

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

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn vom Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation,

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

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

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

Artikel 25

Protokollierung

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

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

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

Artikel 26

Zusammenarbeit mit der Aufsichtsbehörde

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

Artikel 27

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so sehen die Mitgliedstaaten vor, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.

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

Artikel 28

Vorherige Konsultation der Aufsichtsbehörde

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

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

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

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

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

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

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

Abschnitt 2

Sicherheit personenbezogener Daten

Artikel 29

Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 10.

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

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

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

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

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

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

f) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

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

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

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

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

Artikel 30

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

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

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

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

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

b) Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

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

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

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

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

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

Artikel 31

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

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

(2) Die in Absatz 1 dieses Artikels genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 30 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

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

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

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

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

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

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

Abschnitt 3

Datenschutzbeauftragter

Artikel 32

Benennung eines Datenschutzbeauftragten

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

(2) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 34 genannten Aufgaben.

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

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

Artikel 33

Stellung des Datenschutzbeauftragten

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

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

Artikel 34

Aufgaben des Datenschutzbeauftragten

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

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

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

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

d) Zusammenarbeit mit der Aufsichtsbehörde,

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

KAPITEL V

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Artikel 35

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

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

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

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

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

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

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

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

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

Artikel 36

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

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

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

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

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

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 dieses Artikels bietet. In dem Durchführungsrechtsakt wird ein Mechanismus für die regelmäßige Überprüfung vorgesehen, die mindestens alle vier Jahre erfolgt und bei der allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b dieses Artikels genannte Aufsichtsbehörde oder die dort genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 erlassenen Beschlüsse beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen gemäß dem in Artikel 58 Absatz 3 genannten Verfahren erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 58 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

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

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

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

Artikel 37

Datenübermittlung vorbehaltlich geeigneter Garantien

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

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

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

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

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

Artikel 38

Ausnahmen für bestimmte Fälle

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

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

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

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

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

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

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

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

Artikel 39

Übermittlung personenbezogener Daten an in Drittländern niedergelassene Empfänger

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

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

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

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

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

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

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

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

(4) Übermittlungen gemäß Absatz 1 werden dokumentiert.

Artikel 40

Internationale Zusammenarbeit zum Schutz personenbezogener Daten

In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Mitgliedstaaten geeignete Maßnahmen zur

a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,

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

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

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

KAPITEL VI

Unabhänge Aufsichtsbehörden

Abschnitt 1

Unabhängigkeit

Artikel 41

Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Richtlinie zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde").

(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Richtlinie in der gesamten Union. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII.

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

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

Artikel 42

Unabhängigkeit

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

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

(3) Die Mitglieder der Aufsichtsbehörden der Mitgliedstaaten sehen von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihre eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

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

Artikel 43

Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar

— vom Parlament;

— von der Regierung;

— vom Staatsoberhaupt oder

— von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.

(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.

(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Erfüllung seiner Aufgaben nicht mehr erfüllt.

Artikel 44

Errichtung der Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor

a) die Errichtung jeder Aufsichtsbehörde,

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

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

d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren, außer für die erste Amtszeit nach dem 6. Mai 2016, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist,

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

f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während ihrer Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstöße gegen diese Richtlinie.

Abschnitt 2

Zuständigkeit, Aufgaben und Befugnisse

Artikel 45

Zuständigkeit

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

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

Artikel 46

Aufgaben

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

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

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

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

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

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

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

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

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

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

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

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

l) Beiträge zur Tätigkeit des Ausschusses leistet.

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

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

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

Artikel 47

Befugnisse

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

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

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

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

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

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

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

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

Artikel 48

Meldung von Verstößen

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

Artikel 49

Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der verhängten Sanktionen enthalten kann. Die Berichte werden dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Sie werden der Öffentlichkeit, der Kommission und dem Ausschuss zugänglich gemacht.

KAPITEL VII

Zusammenarbeit

Artikel 50

Gegenseitige Amtshilfe

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

(2) Jeder Mitgliedstaaten sieht vor, dass jede Aufsichtsbehörde alle geeigneten Maßnahmen ergreift, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu kann insbesondere auch die Übermittlung maßgeblicher Informationen über die Durchführung einer Untersuchung gehören.

(3) Amtshilfeersuchen enthalten alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.

(4) Die ersuchte Aufsichtsbehörde lehnt das Ersuchen nur ab, wenn

a) sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder

b) ein Eingehen auf das Ersuchen gegen diese Richtlinie oder gegen das Unionsrecht verstoßen würde oder gegen das Recht des Mitgliedstaats, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt.

(5) Die ersuchte Aufsichtsbehörde informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen. Die ersuchte Aufsichtsbehörde erläutert gemäß Absatz 4 die Gründe für die Ablehnung des Ersuchens.

(6) Die ersuchten Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.

(7) Ersuchte Aufsichtsbehörden verlangen für Maßnahmen, die sie aufgrund eines Amtshilfeersuchens getroffen haben, keine Gebühren. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.

(8) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 51

Aufgaben des Ausschusses

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) Der Ausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 58 Absatz 1 genannten Ausschuss weiter und veröffentlicht sie.

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

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Artikel 52

Recht auf Beschwerde bei einer Aufsichtsbehörde

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

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

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

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

Artikel 53

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

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

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

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

Artikel 54

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

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

Artikel 55

Vertretung von betroffenen Personen

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

Artikel 56

Recht auf Schadenersatz

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

Artikel 57

Sanktionen

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

KAPITEL IX

Durchführungsrechtsakte

Artikel 58

Ausschussverfahren

(1) Die Kommission wird von dem mit Artikel 93 der Verordnung (EU) 2016/679 eingesetzten Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

(3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

KAPITEL X

Schlussbestimmungen

Artikel 59

Aufhebung des Rahmenbeschlusses 2008/977/JI

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

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

Artikel 60

Bestehende Unionsrechtsakte

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

Artikel 61

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

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

Artikel 62

Berichte der Kommission

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

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

(3) Für die in den Absätzen 1 und 2 genannten Zwecke kann die Kommission Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern.

(4) Bei den in den Absätzen 1 und 2 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates sowie der anderen einschlägigen Stellen und Quellen.

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

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

Artikel 63

Umsetzung

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

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

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

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

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

Artikel 64

Inkrafttreten

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

Artikel 65

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 27. April 2016.

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