28. Juni 2014

Inoffizielle konsolidierte Version

# Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)

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

(2) Die Verarbeitung personenbezogener Daten steht im Dienste des Menschen; die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ungeachtet der Staatsangehörigkeit oder des gewöhnlichen Aufenthaltsorts der natürlichen Personen deren Grundrechte und Grundfreiheiten und insbesondere deren Recht auf Schutz personenbezogener Daten gewahrt bleiben. Die Datenverarbeitung sollte zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen der Menschen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[43] ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

(4) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarktes hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs geführt. Der unionsweite Datenaustausch zwischen wirtschaftlichen und sozialen Akteuren, staatlichen Stellen und Privatpersonen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten zur Zusammenarbeit und zum Austausch personenbezogener Daten, um ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen zu können.

(5) Der rasche technologische Fortschritt und die Globalisierung stellen den Datenschutz vor neue Herausforderungen. Das Ausmaß, in dem Daten ausgetauscht und erhoben werden, ist dramatisch gestiegen. Die Technik macht es möglich, dass Privatwirtschaft und Staat zur Ausübung ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zugreifen können. Zunehmend

werden auch private Informationen ins weltweite Netz gestellt und damit öffentlich zugänglich gemacht. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert, weshalb der Datenverkehr innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtert werden muss, wobei gleichzeitig ein hohes Maß an Datenschutz zu gewährleisten ist.

(6) Diese Entwicklungen erfordern einen soliden, kohärenteren und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, um eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Jede Person sollte die Kontrolle über ihre eigenen Daten besitzen, und private Nutzer, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.

(7) Die Ziele und Grundsätze der Richtlinie 95/46/EG besitzen nach wie vor Gültigkeit, doch hat die Richtlinie eine unterschiedliche Handhabung des Datenschutzes in der Union, Rechtsunsicherheit sowie die weit verbreitete öffentliche Meinung, dass speziell im Internet der Datenschutz nicht immer gewährleistet ist, nicht verhindern können. Unterschiede beim Schutz der Rechte und Grundfreiheiten von Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, kann den freien Verkehr solcher Daten in der gesamten Union behindern. Diese Unterschiede im Schutzniveau können ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.

(8) Um ein hohes Maß an Datenschutz für den Einzelnen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten zu beseitigen, sollte der Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit kohärent und einheitlich angewandt werden.

(9) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine Stärkung und Präzisierung der Rechte der betroffenen Personen sowie eine Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, aber ebenso gleiche Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.

(10) Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union ermächtigt das Europäische Parlament und den Rat, Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten festzulegen.

(11) Damit jeder in der Union das gleiche Maß an Datenschutz genießt und Unterschiede, die den freien Datenverkehr im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die überall in der Union für

Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtsicherheit und Transparenz schafft, den Einzelnen mit denselben durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter vorsieht und eine einheitliche Kontrolle der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten sowie gleiche Sanktionen und eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Um der besonderen Situation von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine Reihe von abweichenden Regelungen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs des Kleinstunternehmens sowie kleiner und mittlerer Unternehmen sollte die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 maßgebend sein.

(12) Der durch diese Verordnung gewährte Schutz betrifft die Verarbeitung personenbezogener Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnorts. Im Falle juristischer Personen und insbesondere von als juristische Person gegründeten Unternehmen, deren Daten, zum Beispiel deren Name, Rechtsform oder Kontaktdaten, verarbeitet werden, sollte eine Berufung auf diese Verordnung nicht möglich sein. Dies sollte auch dann gelten, wenn der Name der juristischen Person die Namen einer oder mehrerer natürlichen Personen enthält.

(13) Der Schutz natürlicher Personen sollte technologieneutral sein und nicht von den verwendeten Verfahren abhängen, da andernfalls das Risiko einer Umgehung der Vorschriften groß wäre. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, die in einem Ablagesystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten vom Anwendungsbereich der Verordnung ausgenommen werden.

(14) Die Verordnung behandelt weder Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Datenverkehrs im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, noch die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union, für die die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates sollte mit dieser Verordnung in Einklang gebracht und im Einklang mit dieser Verordnung angewendet werden.

(15) Die Verordnung sollte nicht für die von einer natürlichen Person vorgenommene Verarbeitung von personenbezogenen Daten rein persönlicher, familiärer oder häuslicher Natur ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit gelten, wie zum Beispiel das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder Privatverkäufe. Die Verordnung sollte jedoch auf die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen, Anwendung finden.

(16) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden dienen, sowie der freie Verkehr solcher Daten sind in einem eigenen EU-Rechtsinstrument geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung von Straftaten oder der Vollstreckung von Strafurteilen verwendet werden, dem spezifischeren EU-Instrument (Richtlinie XX/YYYY) unterliegen.

(17) Die vorliegende Verordnung sollte die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste nicht berühren.

(18) Diese Verordnung ermöglicht es, dass bei der Anwendung ihrer Vorschriften der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten berücksichtigt wird. Persönliche Daten in Dokumenten, die sich im Besitz einer Behörde oder öffentlichen Einrichtung befinden, können von dieser Behörde oder Einrichtung gemäß unionsrechtlichen oder mitgliedstaatlichen Vorschriften über den Zugang der Öffentlichkeit zu amtlichen Dokumenten offen gelegt werden, die das Recht auf Schutz der personenbezogenen Daten mit dem Recht der Öffentlichkeit auf Zugang zu amtlichen Dokumenten in Einklang bringen und einen fairen Ausgleich der verschiedenen bestehenden Interessen schaffen.

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

(20) Um sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach dieser Verordnung ein Anrecht haben, sollte die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen Produkte und Dienstleistungen gegen Entgelt oder unentgeltlich anzubieten oder diese Personen zu beobachten. Um festzustellen, ob dieser für die Verarbeitung Verantwortliche diesen betroffenen Personen in der Union Waren oder Dienstleistungen anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, in einem oder mehreren Mitgliedstaaten der Union ansässigen betroffenen Personen Dienstleistungen anzubieten.

(21) Ob eine Verarbeitungstätigkeit der Überwachung von Personen gilt, sollte daran festgemacht werden, ob sie – unabhängig von dem Ursprung der Daten und unabhängig davon, ob andere Daten, einschließlich Daten aus öffentlichen Registern und Bekanntmachungen in der Union, die von außerhalb der Union zugänglich sind,

einschließlich mit der Absicht der Verwendung, oder der möglichen nachfolgenden Verwendung über sie erhoben werden – mit Hilfe von Datenverarbeitungstechniken verfolgt werden, durch die einer Person ein Profil zugeordnet wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.

(22) Ist nach internationalem Recht das innerstaatliche Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, sollte die Verordnung auch auf einen nicht in der EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.

(23) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Um festzustellen, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zum unmittelbaren oder mittelbaren Identifizieren oder Herausgreifen der Person genutzt werden. Bei der Prüfung der Frage, ob Mittel nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei sowohl die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Daten gelten, d. h. für Daten, die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen. Die Verordnung betrifft daher nicht die Verarbeitung solcher anonymen Daten, auch wenn sie für statistische und Forschungszwecke verwendet werden.

(24) Diese Verordnung sollte auf eine Verarbeitung angewandt werden, die Kennungen umfasst, die Geräte, Software-Anwendungen und -Tools oder Protokolle liefern, wie etwa IP-Adressen, Cookie-Kennungen und Funkfrequenzkennzeichnungen, es sei denn, diese Kennungen beziehen sich nicht auf eine bestimmte oder bestimmbare natürliche Person.

(25) Die Einwilligung sollte ausdrücklich mittels einer geeigneten Methode erfolgen, die eine ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer eindeutigen bestätigenden Handlung, die auf einer Entscheidung der betroffenen Person basiert, ermöglicht, die sicherstellt, dass der betreffenden Person bewusst ist, dass sie ihre Einwilligung in die Verarbeitung personenbezogener Daten gibt. Eine eindeutige bestätigende Handlung könnte etwa das Anklicken eines Kästchens beim Besuch einer Internetseite oder jede sonstige Erklärung oder Verhaltensweise sein, mit der die betroffene Person in dem jeweiligen Kontext klar und deutlich ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Schweigen, die bloße Nutzung eines Dienstes oder Untätigkeit sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommene Verarbeitungsvorgänge beziehen. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, in dessen Bereitstellung eingewilligt wird, erfolgen.

(26) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten gezählt werden, die sich auf den Gesundheitszustand eines von der Verarbeitung Betroffenen beziehen, außerdem Informationen über die Vormerkung der betreffenden Person zur Erbringung medizinischer Leistungen, Angaben über Zahlungen oder die Berechtigung zum Empfang medizinischer Dienstleistungen, Nummern, Symbole oder Kennzeichen, die einer bestimmten Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, jede Art von Informationen über die betreffende Person, die im Rahmen der Erbringung von medizinischen Dienstleistungen erhoben wurden, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, darunter biologischer Proben, abgeleitet wurden, die Identifizierung einer Person als Erbringer einer Gesundheitsleistung für die betroffene Person sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Beahndlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, gleich, ob sie von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder einem In-Vitro-Diagnose-Test stammen.

(27) Zur Bestimmung der Hauptniederlassung eines für die Verarbeitung Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke, Bedingungen und Mittel der Verarbeitung getroffen werden. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird; das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten begründet an sich noch keine Hauptniederlassung und ist daher kein ausschlaggebender Faktor für das Bestehen einer solchen Niederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem sich seine Hauptverwaltung in der Union befindet.

(28) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund von Eigentümerschaft, finanzieller Beteiligung oder sonstiger Bestimmungen, die die Tätigkeit des Unternehmens regeln, oder der Befugnis, Datenschutzvorschriften einzuführen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann.

(29) Die personenbezogenen Daten von Kindern müssen besonderen Schutz genießen, da Kinder sich der Risiken, Folgen, Vorsichtsmaßnahmen und ihrer Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften. Erfolgt die Datenverarbeitung mit Einwilligung der betroffenen Person in Bezug auf das unmittelbare Angebot von Waren oder Dienstleistungen an ein Kind bis zum vollendeten dreizehnten Lebensjahr, sollte die Einwilligung hierzu durch die Eltern oder den rechtlichen Vertreter des Kindes oder mit deren Zustimmung erteilt werden. Sind die Adressaten Kinder, sollte altersgerechte Sprache verwendet werden. Andere Gründe der rechtmäßigen Verarbeitung, etwa Gründe des öffentlichen Interesses, sollten anwendbar bleiben, etwa Verarbeitung im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden.

(30) Jede Verarbeitung personenbezogener Daten sollte gegenüber den betroffenen Personen nach Recht und Gesetz sowie nach Treu und Glauben und in transparenter Form erfolgen. Insbesondere sollten die besonderen Zwecke, zu denen die Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Datenerfassung feststehen. Die erfassten Daten sollten dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Minimum beschränkt sein; dies heißt vor allem, dass nicht unverhältnismäßig viele Daten erfasst werden und die Speicherfrist auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht durch andere Mittel erreicht werden kann. Es sollten alle vertretbaren Schritte unternommen werden, damit unzutreffende oder unvollständige personenbezogene Daten gelöscht oder berichtigt werden. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für deren Löschung oder regelmäßige Überprüfung vorsehen.

(31) Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt. Bei Kindern oder nicht geschäftsfähigen Personen sollte das Unionsrecht oder das Recht der Mitgliedstaaten die Voraussetzungen für die Einwilligung oder die Zustimmung zur Einwilligung dieser Person regeln.

(32) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte die Beweislast, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat, bei dem für die Verarbeitung Verantwortlichen liegen. Vor allem bei Abgabe einer schriftlichen Erklärung in anderem Zusammenhang sollten Vorkehrungen getroffen werden, die sicherstellen, dass die betroffene Person weiß, dass und wozu sie ihre Einwilligung erteilt. Um den Grundsatz der Datenminimierung einzuhalten, sollte die Beweislast nicht so verstanden werden, dass sie die positive Identifizierung der betroffenen Personen erfordert, es sei denn, diese ist notwendig. In Anlehnung an die Regelungen des Zivilrechts (z. B. Richtlinie 93/13/EWG) sollten Datenschutzregelungen so klar und transparent wie möglich sein. Sie sollten keine verborgenen oder nachteiligen Klauseln enthalten. In die Verarbeitung von personenbezogenen Daten Dritter kann nicht eingewilligt werden.

(33) Um sicherzugehen, dass die Einwilligung ohne Zwang erfolgt, sollte klargestellt werden, dass die Einwilligung keine rechtswirksame Grundlage für die Verarbeitung liefert, wenn die betreffende Person keine echte Wahlfreiheit hat und somit nicht in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden. Dies ist insbesondere dann der Fall, wenn es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt, die aufgrund ihrer einschlägigen hoheitlichen Befugnisse eine Verpflichtung auferlegen kann und die Einwilligung deshalb nicht als ohne Zwang abgegeben gelten kann. Die Verwendung von Voreinstellungen, die die betroffene Person verändern muss, um der Verarbeitung zu widersprechen, wie etwa standardmäßig angekreuzte Kästchen, drückt keine freie Einwilligung aus. Die Einwilligung für die Verarbeitung zusätzlicher personenbezogener Daten, die für die Bereitstellung von Dienstleistungen nicht

notwendig sind, sollten für die Verwendung dieser Dienstleistungen nicht verlangt werden. Wird die Einwilligung widerrufen, so kann dies zur Beendigung oder Nichterbringung einer Dienstleistung führen, die von den personenbezogenen Daten abhängig ist. Kann nicht eindeutig festgestellt werden, ob der beabsichtigte Zweck noch besteht, sollte der für die Verarbeitung Verantwortliche in regelmäßigen Abständen die betroffene Person über die Verarbeitung unterrichten und eine erneute Bestätigung ihrer Einwilligung verlangen.

(34) entfällt

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

(36) Erfolgt die Verarbeitung durch den für die Verarbeitung Verantwortlichen aufgrund einer ihm obliegenden gesetzlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt erforderlich, muss hierfür eine Rechtsgrundlage im Unionsrecht oder im nationalen Recht bestehen, die im Falle einer Beschneidung von Rechten und Freiheiten den Anforderungen der Charta der Grundrechte der Europäischen Union genügt. Dies schließt auch Tarifverträge ein, die nach einzelstaatlichem Recht für allgemein verbindlich erklärt werden können. Desgleichen muss im Unionsrecht oder im nationalen Recht geregelt werden, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln soll.

(37) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person zu schützen.

(38) Die berechtigten Interessen eines für die Verarbeitung Verantwortlichen oder, im Fall der Weitergabe, die berechtigten Interessen eines Dritten, dem die Daten weitergegeben wurden, können eine Rechtsgrundlage für die Verarbeitung darstellen, sofern die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllt werden und die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Diese Interessen sind besonders sorgfältig abzuwägen, wenn es sich bei der betroffenen Person um ein Kind handelt, da Kinder besonders schutzwürdig sind. Sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sollte von der Verarbeitung, die auf pseudonymisierte Daten beschränkt ist, vermutet werden, dass die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllt werden. Die betroffene Person sollte das Recht haben, der Verarbeitung zu widersprechen, ohne dass ihr dadurch Kosten entstehen. Aus Transparenzgründen sollte der für die Verarbeitung Verantwortliche verpflichtet werden, seine berechtigten Interessen gegenüber der betroffenen Person ausdrücklich darzulegen und diese außerdem zu dokumentieren und die betroffene Person über ihr Widerspruchsrecht zu belehren. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine

betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss könnten die Interessen und Grundrechte der betroffenen Person das Interesse des für die Verarbeitung Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Gesetz die Rechtsgrundlage für die Verarbeitung von Daten durch Behörden zu schaffen, greift dieser Rechtfertigungsgrund nicht bei Verarbeitungen durch Behörden, die diese in Erfüllung ihrer Aufgaben vornehmen.

(39) Die Verarbeitung von Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und –diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d. h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, Störungen oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den unberechtigten Zugang zu elektronischen Kommunikationsnetzen, die Verbreitung schädlicher Programmcodes, die Abwehr von Angriffen in Form der gezielten Überlastung von Servern („Denial of access“-Angriffe) sowie Schädigungen von Computer- und elektronischen Kommunikationssystemen zu verhindern. Dieser Grundsatz gilt auch für die Verarbeitung personenbezogener Daten zur Beschränkung missbräuchlichen Zugangs zu und die Verwendung von öffentlich zugänglichen Netzwerken oder Informationssystemen, wie das Führen schwarzer Listen von elektronischen Kennungen.

(39a) Sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sollte die Vermutung gelten, dass die Verhütung oder Begrenzung von Schäden beim für die Datenverarbeitung Verantwortlichen für die berechtigten Interessen des für die Datenverarbeitung Verantwortlichen oder, im Fall der Weitergabe, für die berechtigten Interessen des Dritten, an den die Daten weitergegeben wurden, durchgeführt wird und die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllt werden. Dieser Grundsatz gilt auch für die Durchsetzung von Rechtsansprüchen gegen eine betroffene Person, wie die Einziehung von Forderungen oder zivilrechtliche Schadensersatzansprüche und Rechtsbehelfe.

(39b) Sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sollte die Vermutung gelten, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktvermarktung für eigene oder ähnliche Waren und Dienstleistungen oder zum Zwecke der Direktvermarktung auf dem Postweg für die berechtigten Interessen des für die Datenverarbeitung Verantwortlichen oder, im Fall der Weitergabe, für die berechtigten Interessen des Dritten, an den die Daten weitergegeben wurden, durchgeführt wird und die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllt werden, wenn gut sichtbare Informationen über das Widerspruchsrecht und die

Quelle der personenbezogenen Daten angegeben werden. Die Verarbeitung von Angaben über Geschäftskontakte sollten im Allgemeinen so betrachtet werden, dass sie für die berechtigten Interessen des für die Datenverarbeitung Verantwortlichen oder, im Fall der Weitergabe, für die berechtigten Interessen des Dritten, an den die Daten weitergegeben wurden, durchgeführt wird und die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllt werden. Dies sollte auch für die Verarbeitung personenbezogener Daten gelten, die die betroffene Person offenkundig veröffentlicht hat.

(40) entfällt

(41) entfällt

(42) Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien sollten auch dann erlaubt sein, wenn es dafür eine gesetzliche Grundlage gibt, und – vorbehaltlich bestimmter Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte – wenn dies durch ein öffentliches Interesse gerechtfertigt ist, speziell wenn es um gesundheitliche Belange geht, wie die Gewährleistung der öffentlichen Gesundheit oder der sozialen Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, vor allem wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sichergestellt werden soll, oder wenn die Verarbeitung historischen oder statistischen Zwecken oder wissenschaftlichen Forschungszwecken oder Archivdiensten dient.

(43) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im internationalen Recht verankerte Ziele von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.

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

(45) Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen. Macht die betroffene Person von ihrem Auskunftsrecht Gebrauch, sollte der für die Verarbeitung Verantwortliche das Recht haben, bei der betroffenen Person weitere Informationen einzuholen, die ihn in die Lage versetzen, die von der betreffenden Person gesuchten personenbezogenen Daten zu lokalisieren. Ist es der betroffenen Person möglich, diese Informationen bereitzustellen, sollte der für die Verarbeitung Verantwortliche nicht die Möglichkeit haben, sich auf einen Mangel an Informationen zu berufen, um ein Ersuchen um Zugang abzulehnen.

(46) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information leicht zugänglich sowie in

einfacher und verständlicher Sprache abgefasst ist. Dies gilt ganz besonders für bestimmte Situationen wie etwa Werbung im Internet, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck seine Daten erfasst werden. Wenn sich die Verarbeitung speziell an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer kindgerechten Sprache erfolgen.

(47) Es gilt, die Modalitäten festzulegen, die es einer betroffenen Person ermöglichen, die ihr nach dieser Verordnung zustehenden Rechte und etwa das Recht auf kostenfreie Auskunft oder das Recht auf Berichtigung oder Löschung der Daten wahrzunehmen oder von ihrem Widerspruchsrecht Gebrauch zu machen. Der für die Verarbeitung Verantwortliche sollte verpflichtet werden, innerhalb einer angemessenen Frist auf das Ansuchen der betroffenen Person zu antworten und eine etwaige Ablehnung des Ansuchens zu begründen

(48) Die Grundsätze von Treu und Glauben und Transparenz bei der Verarbeitung setzen voraus, dass die betroffene Person insbesondere über die Existenz des Verarbeitungsvorgangs und seine Zwecke, die voraussichtliche Speicherdauer für den jeweiligen Zweck, ob Daten an Dritte oder in Drittstaaten übermittelt werden sollen, die betreffenden Widerspruchsmöglichkeiten und das Recht auf Auskunft sowie das Recht auf Berichtigung und Löschung der Daten und das Beschwerderecht informiert werden sollte. Werden die Daten bei der betroffenen Person erhoben, sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Diese Information sollte den betroffenen Personen nach der Bereitstellung vereinfachter Informationen in Form standardisierter Icons präsentiert werden, was auch bedeuten kann, dass sie leicht zugänglich ist. Das sollte auch bedeuten, dass personenbezogene Daten in einer Weise verarbeitet werden, die es den betroffenen Personen erlaubt, ihre Rechte wirksam wahrzunehmen.

(49) Die Unterrichtung einer betroffenen Person, dass sie betreffende personenbezogene Daten verarbeitet werden, sollte zum Zeitpunkt der Erhebung erfolgen oder für den Fall, dass die Daten nicht bei ihr erhoben werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die Daten rechtmäßig an einen anderen Empfänger weitergegeben werden dürfen, sollte die betroffene Person bei der erstmaligen Weitergabe der Daten an diesen Empfänger darüber aufgeklärt werden.

(50) Diese Pflicht erübrigt sich jedoch, wenn die betroffene Person bereits informiert ist oder wenn die Speicherung oder Weitergabe ausdrücklich gesetzlich geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist.

(51) Jede Person sollte ein Auskunftsrecht hinsichtlich der Daten, die bei ihr erhoben worden sind, besitzen und dieses Recht problemlos wahrnehmen können, um sich von der Rechtmäßigkeit ihrer Verarbeitung überzeugen zu können. Jede betroffene Person sollte einen Anspruch darauf haben zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie voraussichtlich gespeichert werden, wer die Empfänger der Daten sind, nach welcher allgemeinen Logik die Daten verarbeitet werden und welche Folgen eine solche Verarbeitung haben kann.

Dabei sollten die Grundrechte und Grundfreiheiten anderer Personen, etwa das Geschäftsgeheimnis oder das geistige Eigentum. etwa im Zusammenhang mit Urheberrechten an Software, nicht angetastet werden. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

(52) Der für die Verarbeitung Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Falle von Online-Kennungen. Ein für die Verarbeitung Verantwortlicher sollte personenbezogene Daten nicht nur deshalb speichern, um auf mögliche Ansuchen reagieren zu können.

(53) Jede Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein Recht auf Löschung, wenn die Speicherung ihrer Daten unter Verstoß gegen die Verordnung erfolgt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht weiter verarbeitet werden, wenn sich die Zwecke, für die die Daten erhoben wurden, erübrigt haben, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen unter Verstoß gegen die Verordnung erfolgt ist. Die weitere Speicherung der Daten sollte jedoch zulässig sein, wenn dies für historische oder statistische Zwecke, zum Zwecke der wissenschaftlichen Forschung, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zur Ausübung des Rechts auf freie Meinungsäußerung erforderlich ist, wenn es hierfür eine gesetzliche Grundlage gibt oder wenn eine beschränkte Verarbeitung der Daten anstatt ihrer Löschung gerechtfertigt ist. Auch sollte das Recht auf Löschung nicht gelten, wenn die Speicherung personenbezogener Daten notwendig ist, um einen Vertrag mit der betroffenen Person zu erfüllen, oder wenn die Speicherung dieser Daten gesetzlich vorgeschrieben ist.

(54) Um dem „Recht auf Löschung“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung so weit gehen, dass ein für die Verarbeitung Verantwortlicher, der die personenbezogenen Daten ohne rechtlichen Grund öffentlich gemacht hat, die Pflicht hat, alle notwendigen Schritte zu unternehmen, um die Daten, auch bei Dritten, zu löschen, wobei das Recht der betroffenen Person unberührt bleibt, Schadensersatz zu verlangen.

(54a) Vom Betroffenen bestrittene Daten, deren Richtigkeit oder Unrichtigkeit sich nicht feststellen lässt, sollten bis zur Klärung der Angelegenheit gesperrt werden.

(55) Damit die betroffenen Personen eine bessere Kontrolle über ihre eigenen Daten haben und ihr Auskunftsrecht besser ausüben können, sollten sie im Falle einer elektronischen Verarbeitung ihrer personenbezogenen Daten in einem strukturierten gängigen Format ebenfalls Anspruch auf Erhalt einer Kopie der sie betreffenden Daten in einem gängigen elektronischen Format haben. Die betroffene Person sollte auch befugt sein, die von ihr zur Verfügung gestellten Daten von einer automatisierten Anwendung, etwa einem sozialen Netzwerk, auf eine andere Anwendung zu übertragen. Die für Datenverarbeitung Verantwortlichen sollten dazu angehalten werden sollte nahegelegt werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dies sollte dann möglich sein, wenn die

betroffene Person die Daten dem automatisierten Verarbeitungssystem mit ihrer ausdrücklichen Einwilligung oder im Zuge der Erfüllung eines Vertrags zur Verfügung gestellt hat. Anbieter von Diensten der Informationsgesellschaft sollten die Übertragung dieser Daten für die Bereitstellung ihrer Dienste nicht verbindlich vorschreiben.

(56) In Fällen, in denen die personenbezogenen Daten zum Schutz der lebenswichtigen Interessen der betroffenen Person oder im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder aufgrund der berechtigten Interessen des für die Verarbeitung Verantwortlichen rechtmäßig verarbeitet werden dürfen, sollte jede betroffene Person trotzdem das Recht haben, unentgeltlich und auf einfache und effektive Weise Widerspruch gegen die Verarbeitung der sie betreffenden Daten einzulegen. Die Beweislast sollte bei dem für die Verarbeitung Verantwortlichen liegen, der darlegen muss, dass seine berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.

(57) Hat die betroffene Person das Recht, der Verarbeitung zu widersprechen, sollte der für die Verarbeitung Verantwortliche dies der betroffenen Person ausdrücklich und in verständlicher Art und Form unter Verwendung einer klaren und einfachen Sprache zur Verfügung stellen und diese klar von anderen Informationen trennen.

(58) Unbeschadet der Rechtmäßigkeit der Datenverarbeitung sollte jede natürliche Person das Recht haben, dem Profiling zu widersprechen. Profiling, das Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat, sollte nur erlaubt sein, wenn sie ausdrücklich per Gesetz genehmigt wurde, bei Abschluss oder in Erfüllung eines Vertrags durchgeführt wird oder wenn die betroffene Person ihre Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden werden, einschließlich der spezifischen Unterrichtung der betroffenen Person und dem Anspruch auf persönliche Prüfung sowie dem Ausschluss von Kindern von einer solchen Maßnahme. Diese Maßnahmen sollten nicht dazu führen, dass Menschen aufgrund ihrer Rasse, ethnischer Herkunft, politischen Überzeugung, Religion oder Weltanschauung, Mitgliedschaft in einer Gewerkschaft, sexueller Orientierung oder Geschlechtsidentität diskriminiert werden.

(58a) Stützt sich das Profiling ausschließlich auf die Verarbeitung pseudonymisierter Daten, sollte die Vermutung gelten, dass es keine erheblichen Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat. Erlaubt das Profiling, sei es auf Grundlage einer einzigen Quelle pseudonymisierter Daten oder einer Sammlung pseudonymisierter Daten aus verschiedenen Quellen, dem für die Verarbeitung Verantwortlichen pseudonymisierte Daten einer spezifischen betroffenen Person zuzuordnen, sollten die verarbeiteten Daten nicht länger als pseudonymisiert betrachtet werden.

(59) Im Unionsrecht oder im Recht der Mitgliedstaaten können Beschränkungen bestimmter Grundsätze sowie des Rechts auf Unterrichtung, Berichtigung, Löschung oder des Rechts auf Zugang oder Herausgabe von Daten und des Widerspruchrechts, von Profiling, und von Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person sowie von bestimmten damit zusammenhängenden Pflichten der für die Verarbeitung

Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben bei Naturkatastrophen oder vom Menschen verursachten Katastrophen sowie die Verhütung, Aufdeckung und strafrechtliche Verfolgung von Straftaten und von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen gehört, und um sonstige spezifische und klar definierte öffentliche Interessen der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen zu schützen. Diese Beschränkungen müssen mit der Charta der Grundrechte der Europäischen Union und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

(60) Die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen für jedwede durch diesen oder in dessen Auftrag erfolgende Verarbeitung personenbezogener Daten sollte umfassend geregelt werden, insbesondere im Hinblick auf Dokumentation, Datensicherheit, Folgenabschätzungen, Datenschutzbeauftragte und Kontrolle durch Datenschutzbehörden. Insbesondere sollte der für die Verarbeitung Verantwortliche dafür Sorge tragen, dass jeder Verarbeitungsvorgang im Einklang mit dieser Verordnung steht, und er sollte dazu auch in der Lage sein. Dies sollte von unabhängigen internen oder externen Prüfern überprüft werden.

(61) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten der betroffenen Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen sowohl bei der Konzipierung der Verarbeitungsvorgänge als auch zum Zeitpunkt der Verarbeitung getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Anforderungen sicherzustellen und nachzuweisen, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und geeignete Maßnahmen ergreifen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Der Grundsatz des Datenschutzes durch Technik verlangt, dass der Datenschutz während des gesamten Lebenszyklus der Technologie eingebaut sein muss, von der frühesten Entwicklungsphase über ihre endgültige Einführung und Verwendung bis zur endgültigen Außerbetriebnahme. Das sollte auch die Verantwortlichkeit für die Waren und Dienstleistungen, die von dem für die Verarbeitung Verantwortlichen oder von dem Auftragsverarbeiter verwendet werden, einschließen. Der Grundsatz der datenschutzfreundlichen Voreinstellungen verlangt auf Diensten und Waren installierte Einstellungen zum Schutz der Privatsphäre, die standardmäßig mit den allgemeinen Grundsätzen des Datenschutzes vereinbar sein sollten, wie etwa mit dem Grundsatz der Datenminimierung und dem Grundsatz der Zweckbeschränkung.

(62) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie zur Klärung der Verantwortung und der Haftung der für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, insbesondere für Fälle, in denen ein für die Verarbeitung Verantwortlicher die Verarbeitungszwecke, -bedingungen und -mittel gemeinsam mit anderen für die Verarbeitung

Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführt wird.

(63) Verarbeitet ein für die Verarbeitung Verantwortlicher ohne Niederlassung in der Union personenbezogene Daten von betroffenen Personen in der Union, sollte der für die Verarbeitung Verantwortliche einen Vertreter benennen, es sei denn, der für die Verarbeitung Verantwortliche ist in einem Drittland niedergelassen, das einen angemessenen Schutz bietet, oder es handelt sich um die Verarbeitung in Bezug auf weniger als 5 000 betroffene Personen innerhalb eines Zeitraumes von zwölf aufeinanderfolgenden Monaten, die nicht in Bezug auf besondere Kategorien personenbezogener Daten durchgeführt wird, oder um eine Behörde oder um eine öffentliche Einrichtung oder der betreffende für die Verarbeitung Verantwortliche bietet den betroffenen Personen nicht nur gelegentlich Waren oder Dienstleistungen an. Der Vertreter sollte im Namen des für die Verarbeitung Verantwortlichen tätig werden und den Aufsichtsbehörden als Ansprechpartner dienen.

(64) Zur Klärung der Frage, ob ein für die Verarbeitung Verantwortlicher betroffenen Personen in der Union nur gelegentlich Waren und Dienstleistungen anbietet, sollte jeweils geprüft werden, ob aus dem allgemeinen Tätigkeitsprofil des für die Verarbeitung Verantwortlichen ersichtlich ist, dass das Anbieten der betreffenden Waren und Dienstleistungen lediglich eine zusätzlich zu seinen Haupttätigkeiten hinzukommende Tätigkeit darstellt.

(65) Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die zur Erfüllung der in dieser Verordnung festgelegten Anforderungen notwendige Dokumentation vorhalten. Jeder für die Verarbeitung Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Verlangen die entsprechende Dokumentation vorzulegen, damit diese für die Bewertung der Einhaltung dieser Verordnung herangezogen werden können. Es sollte aber ebenso wichtig sein, bewährten Verfahren und der Einhaltung der Vorschriften Beachtung zu schenken und nicht nur der Zusammenstellung der Dokumentation.

(66) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu deren Eindämmung ergreifen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der dabei anfallenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Festlegung technischer Standards und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sollten die technologische Neutralität, die Interoperabilität sowie Innovationen sowie gegebenenfalls die Zusammenarbeit mit Drittländern gefördert werden.

(67) Eine Verletzung des Schutzes personenbezogener Daten kann erhebliche wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs für die betroffene Person nach sich ziehen, wenn nicht rechtzeitig und angemessen reagiert wird. Deshalb sollte der für die Verarbeitung Verantwortliche die Aufsichtsbehörde ohne unangemessene Verzögerung – von der angenommen

werden sollte, dass sie nicht länger als 72 Stunden dauern sollte– davon in Kenntnis setzen. Gegebenenfalls sollten in der Benachrichtigung die Gründe für die Verzögerung angegeben werden. Natürliche Personen, für die eine derartige Verletzung des Schutzes ihrer personenbezogenen Daten nachteilige Auswirkungen haben könnte, sollten ohne unangemessene Verzögerung benachrichtigt werden, damit sie die erforderlichen Sicherheitsvorkehrungen treffen können. Die Auswirkungen einer solchen Verletzung sollten als nachteilig für den Schutz der personenbezogenen Daten oder der Privatsphäre einer natürlichen Person angesehen werden, wenn sie zum Beispiel einen Identitätsdiebstahl oder -betrug, eine physische Schädigung, eine erhebliche Demütigung oder Rufschädigung zur Folge haben. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung beinhalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden (z.B. Strafverfolgungsbehörden) erteilten Weisungen erfolgen. Damit eine betroffene Person das Risiko eines unmittelbaren Schadens für sich klein halten kann, bedarf es beispielsweise ihrer sofortigen Benachrichtigung, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen der Datensicherheit zu ergreifen.

(68) Um bestimmen zu können, ob eine gegebene Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde und der betroffenen Person ohne unangemessene Verzögerung gemeldet wurde, sollte jeweils überprüft werden, ob der für die Verarbeitung Verantwortliche ausreichende technische Vorkehrungen und organisatorische Maßnahmen getroffen hat, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können, noch bevor persönliche oder wirtschaftliche Interessen Schaden nehmen können, wobei die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren negative Folgen für die betroffene Person zu berücksichtigen sind.

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

(70) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat doch keineswegs in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslose allgemeine Meldepflicht sollte daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit jenen Verarbeitungsvorgängen befassen, die aufgrund ihres Wesens,

ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können. In derartigen Fällen sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen.

(71) Dies sollte insbesondere für neu geschaffene umfangreiche Dateien gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, und die eine große Zahl von Personen betreffen könnten.

(71a) Folgenabschätzungen sind der wesentliche Kern jedes nachhaltigen Datenschutzrahmens und stellen sicher, dass sich Unternehmen von Anfang an aller möglichen Konsequenzen ihrer Datenverarbeitungsvorgänge bewusst sind. Werden Folgenabschätzungen mit Sorgfalt durchgeführt, kann die Wahrscheinlichkeit einer Verletzung des Datenschutzes oder eines Eingriffs in die Privatsphäre ganz wesentlich beschränkt werden. Bei den Datenschutz-Folgenabschätzungen sollte somit das gesamte Lebenszyklusmanagement personenbezogener Daten von der Erhebung über die Verarbeitung bis zur Löschung berücksichtigt werden und im Einzelnen die beabsichtigten Verarbeitungsvorgänge, die Risiken für die Rechte und Freiheiten von betroffenen Personen, die beabsichtigten Maßnahmen zur Eindämmung der Risiken, die Schutzmechanismen und Sicherheitsmaßnahmen sowie die Mechanismen beschrieben werden, durch die die Einhaltung der Verordnung sichergestellt wird.

(71b) Die für die Verarbeitung Verantwortlichen sollten sich auf den Schutz personenbezogener Daten während des gesamten Datenlebenszyklus von der Erhebung über die Verarbeitung bis zur Löschung konzentrieren, indem sie von Anfang an in einen nachhaltigen Datenmanagementrahmen investieren und darauf folgend umfassende Einhaltungsmechanismen einrichten.

(72) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten sinnvoll sein, eine Datenschutz-Folgenabschätzung nicht auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen – beispielsweise wenn Behörden oder öffentliche Einrichtungen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere für die Verarbeitung Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.

(73) entfällt

(74) In Fällen, in denen die Datenschutz-Folgenabschätzung ergibt, dass bestimmte Verarbeitungsvorgänge große konkrete Risiken für die Rechte und Freiheiten von betroffenen Personen bergen, zum Beispiel das Risiko, infolge des Rückgriffs auf neue Technologien von dem Recht auf Datenschutz nicht Gebrauch machen zu können, sollte der Datenschutzbeauftragte oder die Aufsichtsbehörde vor Beginn dieser Vorgänge zu der Frage, ob die geplante risikobehaftete Verarbeitung gegen die Bestimmungen dieser Verordnung verstößt, zu Rate gezogen werden müssen

und Abhilfevorschläge unterbreiten dürfen. Eine Konsultation der Aufsichtsbehörde sollte auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer darauf basierenden Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

(74a) Folgenabschätzungen können nur hilfreich sein, wenn die für die Verarbeitung Verantwortlichen sicherstellen, dass sie die Versprechen einhalten, die ursprünglich in ihnen gegeben wurden. Deshalb sollten die für die Verarbeitung Verantwortlichen regelmäßig Überprüfungen der Einhaltung der Datenschutzvorschriften vornehmen, durch die nachgewiesen wird, dass die eingerichteten Datenverarbeitungsmechanismen die Zusagen einhalten, die in den Datenschutz-Folgenabschätzungen gegeben wurden. Außerdem sollte nachgewiesen werden, dass der für die Datenverarbeitung Verantwortliche in der Lage ist, der autonomen Wahl betroffener Personen zu entsprechen. Darüber hinaus sollte er in dem Fall, dass die Überprüfung Unstimmigkeiten bei der Einhaltung ergibt, diesen Umstand hervorheben und Empfehlungen abgeben, wie eine vollständige Einhaltung erreicht werden kann.

(75) In Fällen, in denen die Verarbeitung im öffentlichen Sektor erfolgt oder sich im privaten Sektor auf mehr als 5 000 betroffene Personen innerhalb von zwölf Monaten bezieht, oder in denen die Kerntätigkeit eines Unternehmens ungeachtet seiner Größe Verarbeitungsvorgänge sensibler Daten einschließt, oder Verarbeitungsvorgänge, die einer regelmäßigen und systematischen Überwachung bedürfen, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person unterstützt werden. Bei der Feststellung, ob Daten einer großen Zahl von betroffenen Personen verarbeitet werden, sollten archivierte Daten, die in einer Art und Weise beschränkt sind, dass sie nicht den gewöhnlichen Datenzugangs- und Verarbeitungsoperationen des für die Verarbeitung Verantwortlichen unterworfen sind und nicht mehr geändert werden können, nicht berücksichtigt werden. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich um Angestellte des für die Verarbeitung Verantwortlichen handelt oder nicht, und unabhängig davon, ob sie diese Aufgabe in Vollzeit wahrnehmen, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können und einen besonderen Kündigungsschutz genießen. Letztendlich sollte das Management einer Organisation verantwortlich bleiben. Der Datenschutzbeauftragte sollte insbesondere vor der Planung, der Ausschreibung, Entwicklung und Einrichtung von Systemen der automatischen Verarbeitung personenbezogener Daten konsultiert werden, um die Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen zu gewährleisten.

(75a) Der Datenschutzbeauftragte sollte zumindest die folgenden Qualifikationen besitzen: umfassende Kenntnisse des Datenschutzrechts und seiner Anwendung, einschließlich technischer und organisatorischer Maßnahmen und Verfahren; Beherrschung der fachlichen Anforderungen an den Datenschutz durch Technik, die datenschutzfreundlichen Voreinstellungen und die Datensicherheit; sektorspezifisches Wissen entsprechend der Größe des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters und der Sensibilität der zu verarbeitenden Daten; die Fähigkeit, Überprüfungen, Konsultationen, Dokumentationen und Protokolldateianalysen durchzuführen; sowie die Fähigkeit, mit

Arbeitnehmervertretungen zu arbeiten. Der für die Verarbeitung Verantwortliche sollte dem Datenschutzbeauftragten ermöglichen, an Weiterbildungsmaßnahmen teilzunehmen, um das für die Durchführung seiner Aufgaben erforderliche Spezialwissen zu bewahren. Die Benennung als Datenschutzbeauftragter erfordert nicht unbedingt eine Vollzeittätigkeit des Mitarbeiters.

(76) Verbände oder andere Vertreter bestimmter Kategorien von für die Verarbeitung Verantwortlichen sollten ermutigt werden, nach Anhörung der Arbeitnehmervertreter im Einklang mit dieser Verordnung stehende Verhaltenskodizes zu erstellen, um eine wirksame Anwendung dieser Verordnung zu erleichtern, bei der den Eigenheiten der in bestimmten Sektoren erfolgenden Verarbeitungen Rechnung getragen wird. Derartige Verhaltenskodizes sollten ein Handeln der Unternehmen in Übereinstimmung mit dieser Verordnung vereinfachen.

(77) Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und standardisierte Datenschutzprüfzeichen eingeführt werden, die den betroffenen Personen einen raschen, zuverlässigen und überprüfbaren Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen. Ein „Europäisches Datenschutzsiegel“ sollte auf europäischer Ebene eingeführt werden, um unter betroffenen Personen Vertrauen und für die für die Verarbeitung Verantwortlichen Rechtssicherheit zu schaffen sowie gleichzeitig die Verbreitung europäischer Datenschutzstandards außerhalb der EU zu fördern, indem es nicht-europäischen Unternehmen vereinfacht wird, Zugang zu europäischen Märkten zu erhalten, indem sie sich zertifizieren lassen.

(78) Der grenzüberschreitende Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels und der grenzübergreifenden Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Der durch diese Verordnung unionsweit garantierte Schutz natürlicher Personen sollte jedoch bei der Übermittlung von personenbezogenen Daten aus der Union in Drittländer oder an internationale Organisationen nicht unterminiert werden. In jedem Fall sollten derartige Datenübermittlungen an Drittländer nur unter strikter Einhaltung dieser Verordnung zulässig sein.

(79) Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt, wodurch ein angemessener Schutz der Grundrechte für die Bürgerinnen und Bürger sichergestellt wird.

(80) Die Kommission kann mit Wirkung für die gesamte Union beschließen, dass bestimmte Drittländer oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation einen angemessenen Datenschutz bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, einen solchen Schutz zu bieten, in der gesamten Union für Rechtssicherheit und eine einheitliche Rechtsanwendung sorgen. Die Kommission kann sich, nach Benachrichtigung und Abgabe einer vollständigen Begründung an das Drittland, auch für die Aufhebung eines solchen Beschlusses entscheiden.

(81) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Inaugenscheinnahme eines Drittlandes berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, ein Rechtschutz existiert und die internationalen Menschenrechtsbestimmungen eingehalten werden.

(82) Die Kommission kann ebenso per Beschluss feststellen, dass bestimmte Drittländer oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation keinen angemessenen Datenschutz bieten. Rechtsvorschriften, die den extraterritorialen Zugang zu personenbezogenen Daten, die in der EU verarbeitet werden, ohne die Zulässigkeit nach dem Recht der Union oder der Mitgliedstaaten vorsehen, sollten als Anhaltspunkt für fehelende Angemessenheit betrachtet werden. Die Übermittlung personenbezogener Daten an derartige Drittländer sollte daher verboten werden. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden.

(83) Bei Fehlen eines Angemessenheitsbeschlusses sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese Garantien können darin bestehen, dass auf verbindliche unternehmensinterne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Durch diese geeigneten Garantien sollte die Achtung der Rechte betroffener Personen wie bei der Verarbeitung innerhalb der EU gewahrt werden, insbesondere hinsichtlich der Begrenzung des Zwecks sowie des Rechts auf Zugang, Berichtigung, Löschung und Forderung von Schadenersatz. Diese Garantien sollten insbesondere die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten und die Rechte der betroffenen Personen gewährleisten, wirksame Rechtsbehelfe bereithalten, sicherstellen, dass die Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen befolgt werden sowie gewährleisten, dass es einen Datenschutzbeauftragten gibt.

(84) Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter offen stehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln zurückzugreifen, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter keinesfalls daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen zu verwenden oder ihnen weitere Klauseln oder ergänzende Garantien hinzuzufügen, solange letztere weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Freiheiten der betroffenen Personen beschneiden. Die von der Kommission angenommenen Standarddatenschutzklauseln könnten unterschiedliche Situationen erfassen, insbesondere die Übermittlungen von für die Verarbeitung Verantwortlichen mit Sitz in der Europäischen Union an für die Verarbeitung Verantwortlichen mit Sitz außerhalb der Europäischen Union und von für die Verarbeitung Verantwortlichen mit Sitz in der Europäischen Union an Auftragsverarbeiter und Unterverarbeiter mit Sitz außerhalb der Europäischen Union. Den für die Verarbeitung Verantwortlichen und Auftragsverarbeitern sollte nahegelegt

werden, mit zusätzlichen vertraglichen Verpflichtungen, welche die Standard-Schutzklauseln ergänzen, noch wirksamere Garantien zu bieten.

(85) Jede Unternehmensgruppe sollte für ihre grenzüberschreitenden Datenübermittlungen aus der Union an Organisationen der gleichen Unternehmensgruppe genehmigte verbindliche unternehmensinterne Datenschutzvorschriften anwenden dürfen, sofern in diesen unternehmensinternen Vorschriften alle Grundprinzipien und durchsetzbaren Rechte enthalten sind, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.

(86) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre Einwilligung erteilt hat, wenn die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaates festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn die Übermittlung aus einem gesetzlich vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In diesem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.

(87) Diese Ausnahmeregelung sollte insbesondere für Datenübermittlungen gelten, die zur Wahrung eines wichtigen öffentlichen Interesses erforderlich sind, beispielsweise für den grenzüberschreitenden Datenaustausch zwischen Wettbewerbs-, Steuer-, Zoll- oder Finanzaufsichtsbehörden, zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten oder zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, einschließlich für die Verhinderung von Geldwäsche und die Bekämpfung der Terrorismusfinanzierung, zuständigen Behörden. Die Übermittlung von personenbezogenen Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen Person zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben. Die Übermittlung personenbezogener Daten aus solch einem wichtigen öffentlichen Interesse sollte lediglich für gelegentliche Übermittlungen verwendet werden. In jedem Fall sollte eine sorgfältige Beurteilung aller Umstände der Übermittlung erfolgen.

(88) Bei der Verarbeitung zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden.

(89) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Schutzes vorliegt, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, durch die rechtlich verbindlich sichergestellt wird, dass die betroffenen Personen die für die Verarbeitung ihrer personenbezogenen Daten in der Union geltenden Rechte und Garantien genießen, sobald die Daten übermittelt sind, soweit die Verarbeitung

weder massiv noch wiederholt oder strukturiert ist. Diese Garantie sollte finanzielle Entschädigungsleistungen in Fällen des Verlusts oder eines unerlaubten Zugangs oder einer unerlaubten Verarbeitung von Daten sowie eine vom einzelstaatlichen Recht unabhängige Verpflichtung enthalten, vollständige Angaben über den Zugang zu den Daten durch Behörden im Drittstaat enthalten.

(90) Manche Drittländer erlassen Gesetze, Verordnungen und sonstige Rechtsakte, durch die die Datenverarbeitungstätigkeiten von natürlichen und juristischen Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar reguliert werden. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets derartiger Drittländer kann gegen internationales Recht verstoßen und dem durch diese Verordnung in der Union gewährleisteten Schutz natürlicher Personen zuwiderlaufen. Datenübermittlungen sollten daher nur zulässig sein, wenn die in dieser Verordnung festgelegten Bedingungen für Datenübermittlungen in Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Weitergabe aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist. Die Bedingungen für das Bestehen eines wichtigen öffentlichen Interesses sollten von der Kommission in einem delegierten Rechtsakt näher festgelegt werden. In Fällen, in denen die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter mit unvereinbaren Anforderungen an die Einhaltung der Regelungen der EU einerseits und denjenigen eines Drittlands andererseits konfrontiert sind, sollte die Kommission dafür sorgen, dass Unionsrecht immer vorgeht. Die Kommission sollte dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter Orientierung und Hilfestellung bieten, und sie sollte versuchen, den Regelungskonflikt mit dem betreffenden Drittland zu lösen.

(91) Bei der Übermittlung personenbezogener Daten über Grenzen hinweg ist der Einzelne womöglich weniger in der Lage, seine Datenschutzrechte wahrzunehmen und sich insbesondere gegen die unrechtmäßige Nutzung oder Weitergabe dieser Informationen zu schützen. Zugleich können die Aufsichtsbehörden unter Umständen nicht in der Lage sein, Beschwerden nachzugehen oder Untersuchungen in Bezug auf Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats durchzuführen. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, nicht übereinstimmende rechtliche Regelungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Daher bedarf es der Förderung einer engeren Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können.

(92) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die ihre Aufgabe völlig unabhängig erfüllen, ist ein wesentliches Element des Schutzes des Einzelnen im Hinblick auf die Verarbeitung personenbezogener Daten. Die Mitgliedstaaten können mehr als eine Aufsichtsbehörde errichten, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht. Die Behörden müssen über angemessene finanzielle und personelle Ressourcen verfügen, um ihre Rolle vollständig wahrzunehmen, wobei die Bevölkerungszahl und der Umfang der Verarbeitung personenbezogener Daten zu berücksichtigen ist.

(93) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er durch ein Rechtsinstrument sicherstellen, dass diese Aufsichtsbehörden am Kohärenz-Verfahren beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Kommission gewährleistet.

(94) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal (unter besonderer Berücksichtigung der Sicherstellung angemessener technischer und rechtlicher Kenntnisse und Fähigkeiten des Personals), Räumlichkeiten und einer Infrastruktur ausgestattet werden, die für die effektive Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und der Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig und angemessen sind.

(95) Die allgemeinen Anforderungen an die Mitglieder der Aufsichtsbehörde sollten gesetzlich von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung des Mitgliedstaats ernannt werden, wobei dafür Sorge getragen wird, dass die Möglichkeit der politischen Einflussnahme minimiert wird; ferner sollten sie Bestimmungen über die persönliche Eignung der Mitglieder, die Vermeidung von Interessenskonflikten und die Stellung der Mitglieder enthalten.

(96) Die Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen im Hinblick auf die Verarbeitung ihrer Daten zu schützen und den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.

(97) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat statt, sollte eine einzige Aufsichtsbehörde als zentrale Anlaufstelle und federführende Behörde für die Überwachung der Tätigkeit des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der gesamten Union zuständig sein und die entsprechenden Beschlüsse fassen, damit die einheitliche Anwendung der Vorschriften verbessert, Rechtssicherheit gewährleistet und der Verwaltungsaufwand der für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verringert wird.

(98) Die federführende Behörde, die die Aufgaben einer solchen zentralen Kontaktstelle übernimmt, sollte die Aufsichtsbehörde des Mitgliedstaats sein, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung oder eine Vertretung hat. In bestimmten Fällen kann die federführende Behörde auf Antrag einer zuständigen Behörde im Rahmen des Kohärenzverfahrens vom Europäischen Datenausschuss bestimmt werden.

(98a) Betroffene Personen, deren personenbezogene Daten von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter in einem anderen Mitgliedstaat verarbeitet werden, sollten sich bei einer Aufsichtsbehörde ihrer Wahl

beschweren können. Die federführende Datenschutzbehörde sollte ihre Arbeit mit der Arbeit der anderen betroffenen Behörden koordinieren.

(99) Obgleich diese Verordnung auch für die Tätigkeit der nationalen Gerichte gilt, sollten - damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben unangetastet bleibt - die Aufsichtsbehörden nicht für personenbezogene Daten zuständig sein, die von Gerichten in ihrer gerichtlichen Eigenschaft verarbeitet werden. Diese Ausnahme sollte allerdings streng begrenzt werden auf rein justizielle Tätigkeiten in Gerichtsverfahren und sich nicht auf andere Tätigkeiten beziehen, mit denen je nach dem nationalen Recht Richter betraut sein können.

(100) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und Befugnisse haben, darunter, insbesondere im Fall von Beschwerden Einzelner, Untersuchungsbefugnisse sowie rechtsverbindliche Interventions-, Beschluss- und Sanktionsbefugnisse sowie die Befugnis, Gerichtsverfahren anzustrengen. Die Aufsichtsbehörden sollten ihre Untersuchungsbefugnisse, was den Zugang zu Räumlichkeiten anbelangt, im Einklang mit dem Unionsrecht und dem einzelstaatlichen Recht ausüben. Dies betrifft vor allem das Erfordernis einer vorherigen richterlichen Genehmigung.

(101) Jede Aufsichtsbehörde sollte Beschwerden von betroffenen Personen oder von Verbänden, die im öffentlichen Interesse handeln, entgegennehmen und die Angelegenheit untersuchen. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person oder den Verband innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde vonnöten sein, sollte die betroffene Person auch hierüber informiert werden.

(102) Die Aufklärungsmaßnahmen der Aufsichtsbehörden für die breite Öffentlichkeit sollten an die für die Verarbeitung Verantwortlichen, die Auftragsverarbeiter einschließlich Kleinst-, Klein- und Mittelunternehmen und die betroffenen Personen gerichtete spezifische Maßnahmen einschließen.

(103) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist.

(104) Jede Aufsichtsbehörde sollte berechtigt sein, an gemeinsamen Maßnahmen von Aufsichtsbehörden teilzunehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer festgelegten Frist antworten müssen.

(105) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) eingeführt werden, das die Aufsichtsbehörden verpflichtet, untereinander und mit der Kommission zusammenzuarbeiten. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme in Bezug auf Verarbeitungsvorgänge zu treffen, die mit dem Angebot von Waren oder

Dienstleistungen für Personen in mehreren Mitgliedstaaten oder der Beobachtung dieser Personen im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten erheblich beeinträchtigen könnten. Ferner sollte es zur Anwendung kommen, wenn eine Aufsichtsbehörde oder die Kommission beantragen, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Darüber hinaus sollten die betroffenen Personen das Recht haben, dass die Kohärenz durchgesetzt wird, wenn sie der Ansicht sind, dass eine Maßnahme einer Datenschutzbehörde eines Mitgliedstaats dieses Kriterium nicht erfüllt hat. Dieses Verfahren sollte andere Maßnahmen, die die Kommission möglicherweise in Ausübung ihrer Befugnisse nach den Verträgen trifft, unberührt lassen.

(106) Bei Anwendung des Kohärenzverfahrens sollte der Europäische Datenschutzausschuss, falls von der einfachen Mehrheit seiner Mitglieder so entschieden wird oder falls eine andere Aufsichtsbehörde oder die Kommission darum ersuchen, binnen einer festgelegten Frist eine Stellungnahme abgeben.

(106a) Um die einheitliche Anwendung dieser Verordnung sicherzustellen, kann der Europäische Datenschutzausschuss in Einzelfällen einen Beschluss fassen, der für die zuständigen Aufsichtsbehörden verbindlich ist.

(107) entfällt

(108) Es kann dringender Handlungsbedarf zum Schutz der Interessen von betroffenen Personen bestehen, insbesondere wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht. Daher sollten die Aufsichtsbehörden bei der Anwendung des Kohärenzverfahrens einstweilige Maßnahmen mit einer festgelegten Geltungsdauer treffen können.

(109) Die Anwendung dieses Verfahrens sollte eine Bedingung für die rechtliche Gültigkeit und die Durchsetzung des entsprechenden Beschlusses durch eine Aufsichtsbehörde sein. In anderen Fällen von grenzübergreifender Relevanz können die betroffenen Aufsichtsbehörden auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Untersuchungen durchführen, ohne auf das Kohärenz-Verfahren zurückzugreifen.

(110) Auf Unionsebene sollte ein Europäischer Datenschutzausschuss eingerichtet werden. Dieser ersetzt die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten gebildet werden. Der Europäische Datenschutzausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Organe der Europäischen Union beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern, einschließlich der Koordinierung gemeinsamer Maßnahmen. Der Europäische Datenschutzausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln. Der Europäische Datenschutzausschuss sollte den Dialog mit den betroffenen Interessenträgern, wie Verbände betroffener Personen, Verbraucherorganisationen, für die Verarbeitung Verantwortliche sowie weitere relevante Interessenträger und Experten, stärken.

(111) Betroffene Personen, die sich in ihren Rechten verletzt sehen, die ihnen aufgrund dieser Verordnung zustehen, sollten das Recht auf Beschwerde bei einer

Aufsichtsbehörde in einem Mitgliedstaat sowie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf im Sinne von Artikel 47 der Charta der Grundrechte haben, wenn die Aufsichtsbehörde auf die Beschwerde nicht reagiert oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist.

(112) Einrichtungen, Organisationen oder Verbände, die im öffentlichen Interesse handeln und die nach dem Recht eines Mitgliedstaats gegründet sind, sollten das Recht haben, im Namen der betroffenen Person mit deren Einwilligung Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen, wenn sie von der betroffenen Person dazu beauftragt werden, oder unabhängig von der Beschwerde einer betroffenen Person eine eigene Beschwerde zu erheben, wenn ihrer Ansicht nach Vorschriften dieser Verordnung verletzt wurde.

(113) Jede natürliche oder juristische Person sollte das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde haben. Für Verfahren gegen eine Aufsichtsbehörde sollten die Gerichte des Mitgliedstaats zuständig sein, in dem die Aufsichtsbehörde ihren Sitz hat.

(114) Um den gerichtlichen Schutz der betroffenen Person in Situationen zu stärken, in denen die zuständige Aufsichtsbehörde ihren Sitz in einem anderen Mitgliedstaat als dem Mitgliedstaat hat, in dem die betroffene Person ansässig ist, sollte die betroffene Person eine Einrichtung, Organisation oder einen Verband, die/der im öffentlichen Interesse handelt, beauftragen können, vor dem zuständigen Gericht in dem anderen Mitgliedstaat Klage gegen die Aufsichtsbehörde zu erheben.

(115) In Fällen, in denen die zuständige Aufsichtsbehörde mit Sitz in einem anderen Mitgliedstaat nicht tätig wird oder unzureichende Maßnahmen in Bezug auf eine Beschwerde getroffen hat, sollte die betroffene Person die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen können, vor dem zuständigen Gericht im anderen Mitgliedstaat Klage gegen die dortige Aufsichtsbehörde zu erheben. Dies gilt nicht für Personen, die außerhalb der EU ansässig sind. Die ersuchte Aufsichtsbehörde sollte entscheiden können, ob es angemessen ist, dem Ersuchen stattzugeben; diese Entscheidung sollte von einem Gericht nachgeprüft werden können.

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

(117) Gibt es Hinweise auf in verschiedenen Mitgliedstaaten anhängige Parallelverfahren, sollten die Gerichte verpflichtet sein, sich miteinander in Verbindung zu setzen. Die Gerichte sollten die Möglichkeit haben, ein Verfahren auszusetzen, wenn in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist. Die Mitgliedstaaten sollten sicherstellen, dass effiziente Klagemöglichkeiten vorhanden sind, mit denen rasch Maßnahmen zur Abstellung oder Verhinderung eines Verstoßes gegen diese Verordnung erwirkt werden können.

(118) Finanzielle oder sonstige Schäden, die einer Person aufgrund einer rechtswidrigen Verarbeitung entstehen, sollten von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter ersetzt werden, die nur dann von ihrer Haftung befreit werden können, wenn sie nachweisen, dass ihnen der Schaden nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt.

(119) Gegen jede – privatem oder öffentlichem Recht unterliegende – Person, die gegen diese Verordnung verstößt, sollten Sanktionen verhängt werden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sind, und alle Maßnahmen zu ihrer Anwendung treffen. Die Vorschriften über Sanktionen sollten angemessenen Verfahrensgarantien nach Maßgabe der allgemeinen Grundsätze des Unionsrechts und der Charta der Grundrechte unterliegen, einschließlich des Rechts auf einen wirksamen gerichtlichen Rechtsbehelf und ein ordnungsgemäßes Verfahren und des Verbots der doppelten Strafverfolgung (ne bis in idem).

(119a) Bei der Anwendung der Sanktionen sollten die Mitgliedstaaten angemessenen Verfahrensgarantien, einschließlich des Rechts auf einen wirksamen gerichtlichen Rechtsbehelf und ein ordnungsgemäßes Verfahren und ein Verbot der doppelten Strafverfolgung (ne bis in idem) uneingeschränkte Beachtung schenken.

(120) Um die verwaltungsrechtlichen Sanktionen, die bei Verstößen gegen diese Verordnung verhängt werden können, zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, verwaltungsrechtliche Vergehen zu ahnden. Diese Vergehen sollten in dieser Verordnung zusammen mit der Obergrenze der entsprechenden Geldbußen aufgeführt werden, die in jedem Einzelfall im Verhältnis zu den besonderen Umständen des Falls und unter Berücksichtigung insbesondere der Art, Schwere und Dauer des Verstoßes festzusetzen sind. Abweichungen bei der Anwendung verwaltungsrechtlicher Sanktionen können im Kohärenzverfahren behandelt werden.

(121) Sofern erforderlich, sollten für die Verarbeitung personenbezogener Daten Ausnahmen oder Abweichungen von bestimmten Vorschriften dieser Verordnung vorgesehen werden, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf freie Meinungsäußerung und insbesondere dem Recht, Informationen zu empfangen und weiterzugeben, wie es unter anderem in Artikel 11 der Charta der Grundrechte der Europäischen Union garantiert ist, in Einklang zu bringen. Die Mitgliedstaaten sollten deshalb Rechtsvorschriften zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von Daten in Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden sowie in Bezug auf die Zusammenarbeit, einheitliche Rechtsanwendung und spezifische Datenverarbeitungssituationen regeln. Die Mitgliedstaaten sollten dies jedoch nicht zum Anlass nehmen, Ausnahmeregelungen für die anderen Bestimmungen dieser Verordnung vorzusehen. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, sind Begriffe, die sich auf diese Freiheit beziehen, weit auszulegen, um alle Tätigkeiten, die auf die Weitergabe von

Informationen, Meinungen und Vorstellungen an die Öffentlichkeit abzielen, unabhängig davon, welche Medien dafür herangezogen werden, zu erfassen und auch technologischen Fortschritt zu berücksichtigen. Diese Tätigkeiten sind mit oder ohne Erwerbszweck möglich und sollten nicht auf Medienunternehmen beschränkt werden.

(122) Für die Verarbeitung von personenbezogenen Gesundheitsdaten als besonderer Datenkategorie, die eines höheren Schutzes bedarf, lassen sich häufig berechtigte Gründe zugunsten des Einzelnen wie der Gesellschaft insgesamt anführen, insbesondere wenn es darum geht, die Kontinuität der Gesundheitsversorgung über die Landesgrenzen hinaus zu gewährleisten. Diese Verordnung sollte daher vorbehaltlich besonderer und geeigneter Garantien zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen die Bedingungen für die Verarbeitung personenbezogener Gesundheitsdaten harmonisieren. Dies schließt das Recht natürlicher Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.

(122a) Eine Person, die beruflich personenbezogene Gesundheitsdaten verarbeitet, sollte, wenn möglich, anonymisierte oder pseudonymisierte Daten erhalten, sodass die Identität nur dem Hausarzt oder Spezialisten bekannt ist, der eine solche Verarbeitung von Daten angefordert hat.

(123) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, personenbezogene Gesundheitsdaten auch ohne Einwilligung der betroffenen Person zu verarbeiten. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen.

(123a) Die Verarbeitung personenbezogener Gesundheitsdaten als eine Sonderkategorie von Daten kann für historische oder statistische Zwecke oder zum Zweck der wissenschaftlichen Forschung erforderlich sein. Daher sieht diese Verordnung eine Ausnahme von dem Erfordernis der Einwilligung in Fällen der Forschung von hohem öffentlichem Interesse vor.

(124) Die allgemeinen Grundsätze des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten sollten auch im Kontext von Beschäftigung und sozialer Sicherheit gelten. Die Mitgliedstaaten sollten gemäß den in dieser Verordnung festgelegten Vorschriften und Mindeststandards die Verarbeitung personenbezogener Daten im Beschäftigungskontext und die Verarbeitung personenbezogener Daten im Bereich der sozialen Sicherheit regeln können. Ist in einem Mitgliedsstaat eine gesetzliche Grundlage zur Regelung von Angelegenheiten des Beschäftigungsverhältnisses durch Vereinbarung zwischen den

Arbeitnehmervertretern und der Leitung des Unternehmens oder des herrschenden Unternehmens einer Unternehmensgruppe (Kollektivvereinbarung) oder nach Maßgabe der Richtlinie 2009/38/EG des Europäischen Parlaments und des Rates[1] vorgesehen, kann die Verarbeitung personenbezogener Daten im Beschäftigungskontext auch durch eine solche Vereinbarung geregelt werden können.

(125) Die Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung sollte, um rechtmäßig zu sein, auch anderen einschlägigen Rechtsvorschriften unter anderem zu klinischen Versuchen genügen.

(125a) Personenbezogene Daten können anschließend auch durch Archivdienste verarbeitet werden, deren Hauptaufgabe oder rechtliche Pflicht darin besteht, Archivgut im Interesse der Öffentlichkeit zu erfassen, zu erhalten, bekanntzumachen, auszuwerten und zu verbreiten. Das Recht der Mitgliedstaaten sollte das Recht auf Schutz personenbezogener Daten mit den Rechtsvorschriften über Archive und den öffentlichen Zugang zu Verwaltungsinformationen in Einklang bringen. Die Mitgliedstaaten sollten sich dafür einsetzen, dass – insbesondere durch die Europäische Archivgruppe – Regeln erarbeitet werden, die die Vertraulichkeit von Daten gegenüber Dritten sowie die Authentizität, Vollständigkeit und ordnungsgemäße Erhaltung der Daten sicherstellen.

(126) Wissenschaftliche Forschung im Sinne dieser Verordnung sollte Grundlagenforschung, angewandte Forschung und privat finanzierte Forschung einschließen und darüber hinaus dem in Artikel 179 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder wissenschaftlichen Forschungszwecken sollte nicht dazu führen, dass personenbezogene Daten zu anderen Zwecken verarbeitet werden, es sei denn, die betroffene Person stimmt ihr zu oder die Verarbeitung erfolgt auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats.

(127) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten gesetzlich regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen.

(128) Im Einklang mit Artikel 17 des Vertrags über die Arbeitsweise der Europäischen Union achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht. Wendet eine Kirche in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung angemessene Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, sollten diese Regeln weiter gelten, wenn sie mit dieser Verordnung in Einklang gebracht und als vereinbar anerkannt werden.

(129) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, Rechtsakte nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union zu erlassen. Delegierte Rechtsakte sollten insbesondere erlassen werden in Bezug auf die Festlegung der Bedingungen der Übermittlung auf Icons gestützter Informationen, das Recht auf Löschung, die Erklärung, dass Verhaltenskodizes mit der Verordnung vereinbar sind, die Festlegung der Kriterien und Anforderungen für Zertifizierungsverfahren, die Festlegung der Angemessenheit des Schutzniveaus in einem Drittland oder einer internationalen Organisation, die Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften, verwaltungsrechtliche Sanktionen, die Datenverarbeitung für Gesundheitszwecke und die Verarbeitung im Beschäftigungskontext. Es ist besonders wichtig, dass die Kommission im Rahmen ihrer Vorarbeiten auch auf Sachverständigenebene geeignete Konsultationen durchführt, insbesondere mit dem Europäischen Datenschutzausschuss. Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission gewährleisten, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat zeitgleich, rechtzeitig und in geeigneter Weise übermittelt werden.

(130) Um einheitliche Bedingungen für die Anwendung dieser Verordnung sicherzustellen, sollten der Kommission Durchführungsbefugnisse übertragen werden zur Festlegung von: Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung für die Verarbeitung personenbezogener Daten von Kindern, Standardvorlagen für die Benachrichtigung der betroffenen Personen zur Wahrnehmung ihrer Rechte, Standardvorlagen für die Unterrichtung der betroffenen Person, Standardvorlagen für das Auskunftsrecht, einschließlich der Mitteilung der personenbezogenen Daten an die betroffene Person, Standardvorlagen betreffend die von dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter aufzubewahrende Dokumentation, die Standardvorlage für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und Dokumentation der Verletzung des Schutzes von personenbezogenen Daten, Vorlagen für die vorherige Konsultation und Benachrichtigung der Aufsichtsbehörde. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[1] ausgeübt werden. Die Kommission sollte besondere Maßnahmen für Kleinst-, Klein- und Mittelunternehmen erwägen.

(131) Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung für die Verarbeitung personenbezogener Daten von Kindern, Standardvorlagen für die Benachrichtigung der betroffenen Personen zur Wahrnehmung ihrer Rechte, Standardvorlagen für die Unterrichtung der betroffenen Person, Standardvorlagen für das Auskunftsrecht, einschließlich der Mitteilung der personenbezogenen Daten an die betroffene Person, Standardvorlagen betreffend die von dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter aufzubewahrende Dokumentation, die Standardvorlage für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und Dokumentation der Verletzung des Schutzes von personenbezogenen Daten, Vorlagen für die vorherige Konsultation und Benachrichtigung der Aufsichtsbehörde sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.

(132) entfällt

(133) Da die Ziele dieser Verordnung, nämlich ein gleiches Maß an Datenschutz für den Einzelnen und freier Datenverkehr in der Union, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem Subsidiaritätsprinzip gemäß Artikel 5 des Vertrags über die Europäische Union tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht diese Verordnung nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(134) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Die Genehmigungen der Aufsichtsbehörden und die Beschlüsse der Kommission auf der Grundlage der Richtlinie 95/46/EG sollten jedoch in Kraft bleiben. Die Beschlüsse der Kommission und die Genehmigungen der Aufsichtsbehörden in Bezug auf die Übermittlung von personenbezogenen Daten an Drittstaaten gemäß Artikel 41 Absatz 8 sollten für einen Übergangszeitraum von fünf Jahren nach Inkrafttreten dieser Verordnung in Kraft bleiben, es sei denn, sie werden vor Ende dieses Zeitraums von der Kommission geändert, ersetzt oder aufgehoben.

(135) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG festgelegten spezifischen Pflichten, die dasselbe Ziel verfolgen, unterliegen einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Um das Verhältnis zwischen dieser Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden.

(136) Für Island und Norwegen stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.

(137) Für die Schweiz stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.

(138) Für Lichtenstein stellt diese Verordnung, soweit sie auf die Verarbeitung personenbezogener Daten durch Behörden Anwendung findet, die an der Umsetzung des Schengen-Besitzstands beteiligt sind, eine Weiterentwicklung dieses Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und

der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar.

(139) Diese Verordnung steht, in Anbetracht des Umstands, dass, wie der Gerichtshof der Europäischen Union betont hat, das Recht auf Schutz der personenbezogenen Daten keine uneingeschränkte Geltung beanspruchen kann, sondern im Hinblick auf seine gesellschaftliche Funktion gesehen werden und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss, im Einklang mit allen Grundrechten und Grundsätzen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere mit dem Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, dem Recht auf Schutz personenbezogener Daten, der Gedanken-, Gewissens- und Religionsfreiheit, der Freiheit der Meinungsäußerung und der Informationsfreiheit, der unternehmerischen Freiheit, dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren sowie mit der Achtung der Vielfalt der Kulturen, Religionen und Sprachen –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

## KAPITEL I

## ALLGEMEINE BESTIMMUNGEN

### Artikel 1

### Gegenstand und Ziele

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

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

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

### Artikel 2

### Sachlicher Anwendungsbereich

1. Diese Verordnung gilt, unabhängig von der Verarbeitungsmethode, für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird

a) im Rahmen einer Tätigkeit, die nicht dem Unionsrecht unterliegt,

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

c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union fallen,

d) von einer natürlichen Person zu ausschließlich persönlichen oder familiären Zwecken; Die Ausnahme gilt auch für die Veröffentlichung personenbezogener Daten, bei denen davon auszugehen ist, dass sie nur einer begrenzten Anzahl von Personen zugänglich sein werden.

e) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.

3. Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und insbesondere deren Artikel 12 bis 15, in dem die Verantwortlichkeit von Anbietern von Vermittlungsdiensten geregelt ist, unberührt.

## Artikel 3

## Räumlicher Anwendungsbereich

1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union erfolgt.

2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung

a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist; oder

b) der Überwachung dieser betroffenen Personen dient.

3. Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

## Artikel 4

## Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck

(1) entfällt;

(2) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer eindeutigen Kennung oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen, sozialen oder geschlechtlichen Identität dieser Person sind;

(2a) „pseudonymisierte Daten“ personenbezogene Daten, die ohne Heranziehung zusätzlicher Informationen keiner spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die die Nichtzuordnung gewährleisten;

(2b) „verschlüsselte Daten“ personenbezogene Daten, die durch technische Schutzmaßnahmen für Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht wurden;

(3) „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung sowie das Löschen oder Vernichten der Daten;

(3a) „Profiling“ jede Form automatisierter Verarbeitung personenbezogener Daten, die zu dem Zweck vorgenommen wird, bestimmte personenbezogene Aspekte, die einen Bezug zu einer natürlichen Person haben, zu bewerten oder insbesondere die Leistungen der betreffenden Person bei der Arbeit, ihre wirtschaftliche Situation, ihren Aufenthaltsort, ihre Gesundheit, ihre persönlichen Vorlieben, ihre Zuverlässigkeit oder ihr Verhalten zu analysieren oder vorauszusagen;

(4) „Datei" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

(5) „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten durch mitgliedstaatliches oder Unionsrecht vorgegeben, können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach mitgliedstaatlichem oder Unionsrecht bestimmt werden;

(6) „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

(7) „Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden;

(7a) „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

(8) „Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte ausdrückliche Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

(9) „Verletzung des Schutzes personenbezogener Daten“ die Vernichtung, der Verlust, die Veränderung, ob unbeabsichtigt oder widerrechtlich, oder die unbefugte Weitergabe von beziehungsweise der unbefugte Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

(10) „genetische Daten“ alle personenbezogenen Daten betreffend die genetischen Merkmale eines Menschen, die ererbt oder erworben wurden, die aus einer Analyse einer biologischen Probe des betreffenden Menschen resultieren, insbesondere durch DNA- oder RNA-Analyse oder Analyse eines anderen Elements, wodurch entsprechende Informationen erlangt werden können;

(11) „biometrische Daten“ personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten;

(12) „Gesundheitsdaten“ personenbezogene Daten, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die betreffende Person beziehen;

(13) „Hauptniederlassung“ der Ort der Niederlassung eines Unternehmens oder einer Unternehmensgruppe in der Union – wobei es sich um den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter handeln kann –, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten getroffen werden. Unter anderem können die folgenden objektiven Kriterien in Betracht gezogen werden: der Standort des für die Verarbeitung Verantwortlichen oder die Hauptverwaltung des Auftragsverarbeiters, der Standort derjenigen Einheit in einer Unternehmensgruppe, die im Hinblick auf Leitungsfunktionen und administrative Zuständigkeiten am besten in der Lage ist, die Vorschriften dieser Verordnung anzuwenden und durchzusetzen, der Standort, an dem effektive und tatsächliche Managementtätigkeiten ausgeübt werden und die Datenverarbeitung im Rahmen fester Einrichtungen festgelegt wird.

(14) „Vertreter“ jede in der Union niedergelassene natürliche oder juristische Person, die von dem für die Verarbeitung Verantwortlichen ausdrücklich bestellt wurde und ihn in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen vertritt;

(15) „Unternehmen“ jedes Gebilde, das eine wirtschaftliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, das heißt vor allem natürliche und juristische Personen sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

(16) „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

(17) „verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet;

(18) „Kind“ jede Person bis zur Vollendung des achtzehnten Lebensjahres;

(19) „Aufsichtsbehörde“ eine von einem Mitgliedstaat nach Maßgabe von Artikel 46 eingerichtete staatliche Stelle.

## KAPITEL II GRUNDSÄTZE

### Artikel 5

### Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz);

b) für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung);

c) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein; sie dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können (Datenminimierung);

d) sachlich richtig und, wenn nötig, auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im

Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden (Richtigkeit);

e) in einer Form gespeichert werden, die die direkte oder indirekte Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Realisierung der Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten ausschließlich zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke oder Archivzwecke im Einklang mit den Vorschriften und Modalitäten der Artikel 83 und 83a verarbeitet werden und die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen überprüft wird und angemessene technische und organisatorische Maßnahmen ergriffen werden, um den Zugang zu den Daten lediglich auf diese Zwecke zu begrenzen (Speicherminimierung);

ea) in einer Weise verarbeitet werden, die es den betroffenen Personen erlaubt, wirksam ihre Rechte wahrzunehmen (Wirksamkeit);

eb) in einer Weise verarbeitet werden, die vor unbefugter oder unrechtmäßiger Verarbeitung und vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen schützt (Integrität);

f) unter der Verantwortung und Haftung des für die Verarbeitung Verantwortlichen verarbeitet werden, der dafür zu sorgen hat, dass die Vorschriften dieser Verordnung eingehalten werden, und in der Lage sein muss, den Nachweis hierfür zu erbringen (Rechenschaftspflicht).

## Artikel 6

## Rechtmäßigkeit der Verarbeitung

1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

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

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

c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.

d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.

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

f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen – oder, im Fall der Weitergabe, der berechtigten Interessen eines Dritten, an den die Daten weitergegeben wurden – , die die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllen, erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.

3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e müssen eine Rechtsgrundlage haben im

a) Unionsrecht oder

b) Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.

Die einzelstaatliche Regelung muss ein im öffentlichen Interesse liegendes Ziel verfolgen oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem mit der Verarbeitung verfolgten legitimen Zweck stehen. Im Rahmen dieser Verordnung können im Recht der Mitgliedstaaten Einzelheiten der Rechtmäßigkeit der Verarbeitung, insbesondere zu den für die Verarbeitung Verantwortlichen, zur Zweckbestimmung der Verarbeitung und Zweckbindung, zur Art der Daten und zu den betroffenen Personen, zu Verarbeitungsvorgängen und -verfahren, zu Empfängern sowie zur Speicherdauer geregelt werden.

4. entfällt

5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Absatz 1 Buchstabe f für verschiedene Bereiche und Verarbeitungssituationen einschließlich Situationen, die die Verarbeitung personenbezogener Daten von Kindern betreffen, näher zu regeln.

## Artikel 7

## Einwilligung

1. Im Fall der Verarbeitung auf Grundlage einer Einwilligung trägt der für die Verarbeitung Verantwortliche die Beweislast dafür, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für eindeutig festgelegte Zwecke erteilt hat.

2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich klar erkennbar von dem anderen Sachverhalt getrennt werden. Bestimmungen über die

Einwilligung der betroffenen Person, die diese Verordnung teilweise verletzen, sind in vollem Umfang nichtig.

3. Unbeschadet anderer Rechtsgrundlagen für die Verarbeitung hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Die betroffene Person wird von dem für die Verarbeitung Verantwortlichen informiert, wenn der Widerruf der Einwilligung zu einer Einstellung der erbrachten Dienstleistungen oder der Beendigung der Beziehungen zu dem für die Verarbeitung Verantwortlichen führen kann.

4. Die Einwilligung ist zweckgebunden und wird unwirksam, wenn der Zweck nicht mehr gegeben ist oder die Verarbeitung der personenbezogenen Daten zur Erreichung des Zwecks, für den die Daten ursprünglich erhoben wurden, nicht mehr erforderlich ist. Die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung darf nicht von der Einwilligung in eine Verarbeitung von Daten abhängig gemacht werden, die für die Erfüllung des Vertrages oder die Erbringung der Dienstleistung nicht im Sinne von Artikel 6 Absatz 1 Buchstabe b erforderlich ist.

## Artikel 8

## Verarbeitung personenbezogener Daten eines Kindes

1. Für die Zwecke dieser Verordnung ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Waren oder Dienstleistungen angeboten werden, nur rechtmäßig, wenn und insoweit die Einwilligung hierzu von den Eltern oder Sorgeberechtigten oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um diese Einwilligung zu überprüfen, ohne eine sonst unnötige Verarbeitung personenbezogener Daten zu verursachen.

1a. Informationen, die im Hinblick auf die Abgabe einer Einwilligung Kindern, Eltern und Sorgeberechtigten bereitgestellt werden, einschließlich solcher über die Erhebung und Verwendung personenbezogener Daten durch den für die Verarbeitung Verantwortliche, sollten in einer eindeutigen und den Adressaten angemessenen Sprache abgefasst sein.

2. Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind, unberührt.

3. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken in Bezug auf die Überprüfung der Einwilligung gemäß Absatz 1 nach Maßgabe von Artikel 66 zu veröffentlichen.

4. entfällt

## Artikel 9

Besondere Datenkategorien

1. Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, sexuelle Orientierung oder Geschlechtsidentität oder die Mitgliedschaft und Betätigung in einer Gewerkschaft hervorgehen, sowie von genetischen oder biometrischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten oder mutmaßliche Straftaten, Verurteilungen oder damit zusammenhängende Sicherungsmaßregeln ist untersagt.

2. Absatz 1 gilt nicht, wenn eines der folgenden Kriterien zutrifft:

a) Die betroffene Person hat für einen oder mehrere spezifische Zwecke in die Verarbeitung der genannten personenbezogenen Daten vorbehaltlich der in den Artikeln 7 und 8 genannten Bedingungen eingewilligt, es sei denn, nach den Rechtsvorschriften der Union oder eines Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, oder

aa) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Verlangen der betroffenen Person erfolgt;

b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche seine ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen arbeitsrechtlichen Pflichten nachkommen kann, soweit dies nach den Vorschriften der Union, dem Recht der Mitgliedstaaten, oder Kollektivvereinbarungen, die angemessene Garantien der Grundrechte und Interessen der betroffenen Person, wie etwa des Rechts auf Nichtdiskriminierung, vorbehaltlich der Bedingungen und Garantien des Artikels 82, vorsehen, zulässig ist; oder

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

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

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

f) die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich oder

g) die Verarbeitung ist erforderlich, um auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene Garantien zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, eine Aufgabe zu erfüllen, an der ein hohes öffentliches Interesse besteht; oder

h) die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Artikels 81 für Gesundheitszwecke erforderlich oder

i) die Verarbeitung ist vorbehaltlich der Bedingungen und Garantien des Artikels 83 für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung erforderlich oder

ia) die Verarbeitung ist – vorbehaltlich der in Artikel 83a genannten Bedingungen und Garantien – für Archivdienste erforderlich, oder

j) die Verarbeitung von Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten, Verurteilungen oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung einer Aufgabe, der ein wichtiges öffentliches Interesse zugrunde liegt, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen muss, zulässig ist. Strafregister dürfen nur unter behördlicher Aufsicht geführt werden.

3. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken für die Verarbeitung der in Absatz 1 genannten besonderen Kategorien von personenbezogenen Daten und die in Absatz 2 genannten Ausnahmen nach Maßgabe von Artikel 66 näher zu regeln.

## Artikel 10

## Verarbeitung, ohne dass die betroffene Person bestimmt werden kann

1. Kann der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter anhand der von ihm verarbeiteten Daten eine natürliche Person weder direkt noch indirekt bestimmen, oder bestehen die von ihm verarbeiteten Daten nur aus pseudonymisierten Daten, so ist es ihm nicht gestattet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten zu verarbeiten oder einzuholen, um die betroffene Person zu bestimmen.

2. Kann der für die Verarbeitung Verantwortliche eine Vorschrift dieser Verordnung wegen Absatz 1 nicht einhalten, ist er nicht verpflichtet, die konkrete Vorschrift dieser Verordnung einzuhalten. Kann infolgedessen der für die Verarbeitung Verantwortliche dem Verlangen einer betroffenen Person nicht entsprechen, informiert er die betroffene Person dementsprechend.

## Artikel 10a
## Allgemeine Grundsätze für die Rechte der betroffenen Person

1. Grundlage des Datenschutzes bilden klare und eindeutige Rechte der betroffenen Person, die von dem für die Verarbeitung Verantwortlichen zu achten sind. Mit dieser Verordnung sollen diese Rechte gestärkt, geklärt, gewährleistet und erforderlichenfalls kodifiziert werden.

2. Zu diesen Rechten gehören unter anderem die Bereitstellung klarer und leicht verständlicher Informationen über die Verarbeitung der personenbezogenen Daten der betroffenen Person, das Recht auf Zugang, Berichtigung und Löschung ihrer Daten, das Recht auf Herausgabe von Daten, das Recht, dem Profiling zu widersprechen, das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde und Klageerhebung sowie das Recht auf Ersatz des Schadens, der durch eine rechtswidrige Verarbeitung entsteht. Die Ausübung dieser Rechte darf grundsätzlich mit keinen Kosten verbunden sein. Der für die Verarbeitung Verantwortliche hat die Anträge der betroffenen Personen innerhalb einer angemessenen Frist zu bearbeiten.

## KAPITEL III
## RECHTE DER BETROFFENEN PERSON

### ABSCHNITT 1

### TRANSPARENZ UND MODALITÄTEN

#### Artikel 11

#### Transparente Information und Kommunikation

1. Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine prägnante, nachvollziehbare, klare und für jedermann leicht zugängliche Strategie.

2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in verständlicher Form unter Verwendung einer klaren und einfachen Sprache zur Verfügung, besonders dann, wenn die Information an ein Kind gerichtet ist.

#### Artikel 12

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

1. Im Falle der automatischen Verarbeitung personenbezogener Daten sorgt der für die Verarbeitung Verantwortliche dafür, dass die Maßnahme nach Möglichkeit elektronisch beantragt werden kann.

2. Der für die Verarbeitung Verantwortliche kommt seiner Informationspflicht gegenüber der betroffenen Person unverzüglich nach und teilt ihr spätestens innerhalb von 40 Kalendertagen nach Eingang eines Antrags mit, ob eine Maßnahme nach Artikel 13 oder den Artikeln 15 bis 19 ergriffen wurde, und erteilt die erbetene

Auskunft. Diese Frist kann um einen Monat verlängert werden, wenn mehrere betroffene Personen von ihren Rechten Gebrauch machen und ihre Zusammenarbeit bis zu einem vertretbaren Maß notwendig ist, um einen unnötigen und unverhältnismäßig hohen Aufwand seitens des für die Verarbeitung Verantwortlichen zu vermeiden. Die Unterrichtung hat schriftlich zu erfolgen und der für die Verarbeitung Verantwortliche kann, soweit durchführbar, Fernzugriff zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Stellt die betroffene Person den Antrag in elektronischer Form, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

3. Wird der für die Verarbeitung Verantwortliche entgegen dem Antrag der betroffenen Person nicht tätig, so unterrichtet er die betroffene Person über die Gründe für die Untätigkeit und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.

4. Die Unterrichtung und die auf Antrag ergriffenen Maßnahmen gemäß Absatz 1 sind kostenlos. Bei offenkundig unverhältnismäßigen Anträgen und besonders im Fall ihrer Häufung kann der für die Verarbeitung Verantwortliche ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Durchführung der beantragten Maßnahme berücksichtigt werden. In diesem Fall trägt der für die Verarbeitung Verantwortliche die Beweislast für die offenkundige Unverhältnismäßigkeit des Antrags.

5. entfällt

6. entfällt

## Artikel 13

## Benachrichtigungspflicht bei Berichtigungen und Löschungen

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

## Artikel 13a

## Standardisierte Informationsmaßnahmen

1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche vor der Bereitstellung der Informationen gemäß Artikel 14 mit,

a) ob mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck der Verarbeitung erforderlich;

b) ob mehr personenbezogene Daten gespeichert werden, als für den jeweiligen Zweck der Verarbeitung erforderlich;

c) ob personenbezogene Daten zu anderen als den Zwecken verarbeitet werden, für die sie erhoben wurden;

d) ob personenbezogene Daten an gewerbliche Dritte weitergegeben werden;

e) ob personenbezogene Daten verkauft oder gegen Entgelt überlassen werden;

f) ob personenbezogene Daten verschlüsselt gespeichert werden.

2. Die in Absatz 1 genannten Hinweise sind nach Maßgabe des Anhangs X in Tabellenform geordnet mit Text und Symbolen wie folgt in drei Spalten aufzuführen:

a) In der ersten Spalte werden Piktogramme dargestellt, die diese Hinweise symbolisieren.

b) Die zweite Spalte enthält wesentliche Informationen, mit denen diese Hinweise erläutert werden.

c) In der dritten Spalte werden Piktogramme dargestellt, mit denen angezeigt wird, ob der betreffende Hinweis zutreffend ist oder nicht.

3. Die in den Absätzen 1 und 2 genannten Informationen sind in einer leicht erkennbaren und gut lesbaren Weise darzustellen und in einer Sprache abzufassen, die für die Verbraucher in den Mitgliedstaaten, an die sich die Informationen richten, leicht verständlich ist. Werden die Einzelheiten in elektronischer Form wiedergegeben, müssen sie maschinenlesbar sein.

4. Zusätzliche Einzelheiten dürfen nicht aufgeführt werden. Ausführliche Erklärungen oder weitere Anmerkungen zu den Hinweisen nach Absatz 1 können zusammen mit den Informationen nach Artikel 14 bereitgestellt werden.

5. Der Kommission wird die Befugnis übertragen, nach Einholung einer Stellungnahme des Europäischen Datenschutzausschusses delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Hinweise nach Absatz 1 und ihre Darstellung gemäß Absatz 2 und Anhang X genauer festzulegen.

## ABSCHNITT 2

## INFORMATIONSPFLICHT UND AUSKUNFTSRECHT

### Artikel 14

### Unterrichtung der betroffenen Person

1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche, nach der Bereitstellung der Hinweise gemäß Artikel 13a, zumindest Folgendes mit,

a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters und des Datenschutzbeauftragten,

b) die Zwecke, für die Daten verarbeitet werden, und Informationen über die Sicherheit in Bezug auf die Verarbeitung personenbezogener Daten, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, und gegebenenfalls Informationen über die Umsetzung und Erfüllung der Anforderungen gemäß Artikel 6 Absatz 1 Buchstabe f,

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

d) das Bestehen eines Rechts auf Auskunft sowie auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten und eines Rechts auf Herausgabe der Daten,

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

f) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,

g) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission, oder im Falle der in Artikel 42, Artikel 43 und Artikel 44 Absatz 1 Buchstabe h erwähnten Übermittlungen einen Verweis auf die entsprechenden Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten,

ga) gegebenenfalls Angaben über das Vorhandensein eines Profilings, auf Profiling gestützte Maßnahmen und die beabsichtigten Auswirkungen des Profilings auf die betroffene Person;

gb) aussagekräftige Informationen über die Logik einer automatisierten Datenverarbeitung;

h) sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben oder verarbeitet werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten, insbesondere das Vorliegen bestimmter Verarbeitungsaktivitäten oder Verarbeitungsvorgänge, für die in Datenschutz-Folgenabschätzungen ein mögliches hohes Risiko festgestellt wurde,

ha) gegebenenfalls Angaben dazu, ob im letzten zusammenhängenden Zwölfmonatszeitraum personenbezogene Daten an Behörden vorgelegt wurden.

2. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem mit, ob die Bereitstellung der Daten obligatorisch oder fakultativ ist und welche mögliche Folgen die Verweigerung der Daten hätte.

2a. Bei der Entscheidung über weitere Informationen, die notwendig sind, damit die Verarbeitung gemäß Absatz 1 Buchstabe h nach Treu und Glauben erfolgt, berücksichtigen die für die Verarbeitung Verantwortlichen die einschlägigen Leitlinien gemäß Artikel 38.

3. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem die Herkunft der spezifischen personenbezogenen Daten mit. Stammen die personenbezogenen Daten aus öffentlich zugänglichen Quellen, kann eine allgemeine Angabe erfolgen.

4. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1, 2 und 3

a) zum Zeitpunkt der Erhebung der personenbezogenen Daten bei der betroffenen Person oder unverzüglich, wenn Ersteres nicht möglich ist; oder

aa) auf Antrag einer Einrichtung, einer Organisation oder eines Verbands gemäß Artikel 73;

b) falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, zum Zeitpunkt ihrer Erfassung oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen, unter denen die Daten erhoben oder auf sonstige Weise verarbeitet wurden, Rechnung trägt, oder, falls die Weitergabe an einen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe, oder, wenn die Daten für die Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Kommunikation mit dieser Person; oder

ba) nur auf Antrag, wenn die Daten von kleinen oder Kleinstunternehmen, die die personenbezogenen Daten nur als Nebentätigkeit verarbeiten, verarbeitet werden.

5. Die Absätze 1 bis 4 finden in folgenden Fällen keine Anwendung:

a) Die betroffene Person verfügt bereits über die Informationen gemäß den Absätzen 1, 2 und 3 oder

b) die Daten werden vorbehaltlich der in Artikel 81 oder Artikel 83 genannten Bedingungen und Garantien für historische, statistische oder wissenschaftliche Forschungszwecke verarbeitet, und werden nicht bei der betroffenen Person erhoben und die Unterrichtung erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohen Aufwand verbunden und der für die Verarbeitung Verantwortliche hat die Informationen so veröffentlicht, dass sie von jedermann abgefragt werden können, oder

c) die Daten werden nicht bei der betroffenen Person erhoben und die Erfassung oder Weitergabe ist ausdrücklich in einem Gesetz geregelt, dem der für die Verarbeitung Verantwortliche unterliegt und das unter Berücksichtigung der aufgrund der Verarbeitung und der Art der personenbezogenen Daten bestehenden Risiken angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, oder

d) die Daten werden nicht bei der betroffenen Person erhoben und die Bereitstellung der Informationen greift nach Maßgabe des Unionsrechts oder des Rechts der Mitgliedstaaten gemäß Artikel 21 in die Rechte und Freiheiten anderer natürlicher Personen ein.

6. Im Fall des Absatzes 5 Buchstabe b ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der Rechte oder berechtigten Interessen der betroffenen Person.

7. entfällt

8. entfällt

## Artikel 15

### Recht der betroffenen Person auf Auskunft und auf Herausgabe der Daten

1. Die betroffene Person hat – vorbehaltlich des Artikels 12 Absatz 4 – das Recht, von dem für die Verarbeitung Verantwortlichen jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht, und folgende in einfacher und verständlicher Sprache abgefasste Informationen zu verlangen:

a) die Verarbeitungszwecke für jede Kategorie personenbezogener Daten;

b) die Kategorien personenbezogener Daten, die verarbeitet werden,

c) die Empfänger, an die die personenbezogenen Daten weitergegeben werden müssen oder weitergegeben worden sind, darunter auch bei Empfängern in Drittländern,

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

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchrechts gegen die Verarbeitung dieser Daten,

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

g) entfällt

h) die Tragweite der Verarbeitung und die mit ihr angestrebten Wirkungen,

ha) aussagekräftige Informationen über die Logik einer automatisierten Datenverarbeitung;

hb) im Falle der Weitergabe personenbezogener Daten an eine Behörde infolge eines Antrags einer Behörde, die Bestätigung, dass solch ein Antrag gestellt wurde, wobei Artikel 21 unberührt bleibt.

2. Die betroffene Person hat Anspruch darauf, dass ihr von dem für die Verarbeitung Verantwortlichen mitgeteilt wird, welche personenbezogenen Daten verarbeitet werden. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie in einem strukturierten elektronischen Format zu unterrichten, sofern sie nichts anderes angibt. Unbeschadet des Artikels 10 ergreift der für die Verarbeitung Verantwortliche alle zumutbaren Maßnahmen, um zu überprüfen, ob die Person, die Zugang zu Daten beantragt, die betroffene Person ist.

2a. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und werden diese elektronisch verarbeitet, hat sie das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der zur Verfügung gestellten personenbezogenen Daten in einem interoperablen gängigen elektronischen Format zu verlangen, das sie weiter verwenden kann, ohne dabei von dem für die Verarbeitung Verantwortlichen, von dem die personenbezogenen Daten herausgegeben werden, behindert zu werden. Soweit technisch machbar und verfügbar, werden die Daten auf Verlangen der betroffenen Person unmittelbar von dem für die Verarbeitung Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen übermittelt.

2b. Dieser Artikel gilt unbeschadet der Verpflichtung, nicht mehr benötigte Daten gemäß Artikel 5 Absatz 1 Buchstabe e zu löschen.

2c. Das Recht auf Auskunft nach Absatz 1 und 2 besteht nicht in Bezug auf Daten im Sinne von Artikel 14 Absatz 5 Buchstabe da, es sei denn, die betroffene Person ist befugt, die Geheimhaltung aufzuheben und handelt dementsprechend.

3. entfält

4. entfällt

## ABSCHNITT 3

## BERICHTIGUNG UND LÖSCHUNG

### Artikel 16

### Recht auf Berichtigung

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

### Artikel 17

### Recht auf Löschung

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten sowie von Dritten die Löschung aller Querverweise auf diese personenbezogenen Daten bzw. aller Kopien und Replikationen davon zu verlangen, sofern einer der folgenden Gründe zutrifft:

a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a stützte, oder die Speicherfrist, für die die Einwilligung gegeben wurde, ist abgelaufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.

c) Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.

ca) Ein Gericht oder eine Regulierungsbehörde innerhalb der Union hat rechtskräftig entschieden, dass die betreffenden Daten gelöscht werden müssen.

d) Die Daten wurden unrechtmäßig verarbeitet.

1a. Absatz 1 kommt nur zur Anwendung, wenn der für die Verarbeitung Verantwortliche in der Lage ist, zu überprüfen, ob die Person, die die Löschung beantragt, die betroffene Person ist.

2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten ohne Vorliegen eines Rechtfertigungsgrunds nach Artikel 6 Absatz 1 öffentlich gemacht, so hat er unbeschadet des Artikels 77 alle zumutbaren Maßnahmen zu ergreifen, um die Daten zu löschen und bei Dritten löschen zu lassen. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person, soweit möglich, über die von betroffenen Dritten ergriffenen Maßnahmen.

3. Der für die Verarbeitung Verantwortliche und gegebenenfalls der Dritte sorgen für eine umgehende Löschung der personenbezogenen Daten, soweit deren Speicherung nicht erforderlich ist

(a) zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80;

(b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81;

(c) für historische und statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83;

d) zur Erfüllung einer gesetzlichen Pflicht zur Vorhaltung der personenbezogenen Daten, der der für die Verarbeitung Verantwortliche nach dem Unionsrecht oder dem Recht eines Mitgliedstaats unterliegt; wobei das mitgliedstaatliche Recht ein im öffentlichen Interesse liegendes Ziel verfolgen, das

Recht auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen muss;

(e) in den in Absatz 4 genannten Fällen.

4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung in einer Art und Weise, die nicht den gewöhnlichen Datenzugangs- und Verarbeitungsoperationen unterliegt und die nicht mehr geändert werden kann, beschränken, wenn

a) ihre Richtigkeit von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen;

b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Erfüllung seiner Aufgabe nicht länger benötigt, sie aber für Beweiszwecke weiter aufbewahrt werden müssen;

c) die Verarbeitung unrechtmäßig ist, die betroffene Person aber Einspruch gegen ihre Löschung erhebt und stattdessen deren eingeschränkte Nutzung fordert;

ca) ein Gericht oder eine Regulierungsbehörde innerhalb der Union rechtskräftig entschieden hat, dass die betreffenden Daten einer beschränkten Verarbeitung unterworfen werden müssen;

d) die betroffene Person gemäß Artikel 15 Absatz 2a die Übertragung der personenbezogenen Daten auf ein anderes automatisiertes Verarbeitungssystem fordert;

5. Die in Absatz 4 genannten personenbezogenen Daten dürfen mit Ausnahme ihrer Speicherung nur verarbeitet werden, wenn sie für Beweiszwecke erforderlich sind, wenn die betroffene Person ihre Einwilligung gegeben hat oder die Rechte einer anderen natürlichen oder juristischen Person geschützt werden müssen oder wenn dies im öffentlichen Interesse liegt.

6. Unterliegt die Verarbeitung personenbezogener Daten gemäß Absatz 4 einer Beschränkung, teilt der für die Verarbeitung Verantwortliche der betroffenen Person im Voraus mit, dass die Beschränkung aufgehoben werden soll.

7. entfällt

8. Wird eine Löschung vorgenommen, darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht auf sonstige Weise verarbeiten.

8a. Der für die Verarbeitung Verantwortliche trifft Vorkehrungen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden.

9. Der Kommission wird die Befugnis übertragen, nach Einholung einer Stellungnahme des Europäischen Datenschutzausschusses delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf

a) die Kriterien und Anforderungen im Hinblick auf die Anwendung von Absatz 1 für bestimmte Bereiche und spezielle Verarbeitungssituationen,

b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten,

c) die Kriterien und Bedingungen für die Beschränkung der Verarbeitung personenbezogener Daten gemäß Absatz 4.

Artikel 18 entfällt

ABSCHNITT 4

WIDERSPRUCHSRECHT UND PROFILING

Artikel 19

Widerspruchsrecht

1. Die betroffene Person hat das Recht, jederzeit gegen die Verarbeitung personenbezogener Daten, die auf der Grundlage von Artikel 6 Absatz 1 Buchstaben d und e erfolgt, Widerspruch einzulegen, sofern der für die Verarbeitung Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

2. Wird die Verarbeitung personenbezogener Daten auf Artikel 6 Absatz 1 Buchstabe f gestützt, hat die betroffene Person jederzeit und ohne weitere Begründung das Recht, dagegen im Allgemeinen oder für jeden spezifischen Zweck unentgeltlich Widerspruch einzulegen.

2a. Die betroffene Person muss ausdrücklich in einer verständlichen Weise und Form unter Verwendung einer klaren und einfachen Sprache, insbesondere bei eigens an Kinder gerichteten Informationen, auf das Recht gemäß Absatz 2 hingewiesen werden, wobei sich dieser Hinweis von anderen Informationen deutlich unterscheiden muss.

2b. Im Zusammenhang mit der Verwendung von Diensten der Informationsgesellschaft und unbeschadet der Richtlinie 2002/58/EG kann das Widerspruchsrecht mit Hilfe automatisierter Verfahren ausgeübt werden, die einen technischen Standard verwenden, der den betroffenen Personen ermöglicht, ihre Wünsche eindeutig auszudrücken.

3. Im Falle eines Widerspruchs gemäß den Absätzen 1 und 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten für die im Widerspruch genannten Zwecke nicht weiter nutzen oder anderweitig verarbeiten.

Artikel 20

Profiling

1. Unbeschadet der Bestimmungen des Artikels 6 hat jede natürliche Person das Recht, dem Profiling gemäß Artikel 19 zu widersprechen. Die betroffene Person ist über ihr Recht, dem Profiling zu widersprechen, in deutlich sichtbarer Weise zu unterrichten.

2. Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person dem Profiling, das Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat, nur unterworfen werden, wenn die Verarbeitung

a) für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist und der Abschluss oder die Erfüllung des Vertrags auf Wunsch der betroffenen Person erfolgt ist und geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, oder

b) ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person enthalten oder

c) mit Einwilligung der betroffenen Person nach Maßgabe von Artikel 7 und vorbehaltlich entsprechender Garantien erfolgt.

3. Ein Profiling, das zur Folge hat, dass Menschen aufgrund von Rasse, ethnischer Herkunft, politischer Überzeugung, Religion oder Weltanschauung, Mitgliedschaft in einer Gewerkschaft, sexueller Orientierung oder Geschlechtsidentität diskriminiert werden, oder das zu Maßnahmen führt, die eine solche Wirkung haben, ist untersagt. Der für die Verarbeitung Verantwortliche hat für einen wirksamen Schutz gegen mögliche Diskriminierung aufgrund von Profiling zu sorgen. Profiling darf sich nicht ausschließlich auf die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten stützen.

4. entfällt

5. Profiling, das Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat, darf sich nicht ausschließlich oder vorrangig auf automatisierte Verarbeitung stützen und muss eine persönliche Prüfung, einschließlich einer Erläuterung der nach einer solchen Prüfung getroffenen Entscheidung enthalten. Zu den geeigneten Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 gehören das Recht auf persönliche Prüfung und die Erläuterung der nach einer solchen Prüfung getroffenen Entscheidung.

5a. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken in Bezug auf die weitere Festlegung der

Kriterien und Bedingungen für das Profiling gemäß Absatz 2 nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b zu veröffentlichen.

## ABSCHNITT 5

## BESCHRÄNKUNGEN

### Artikel 21

### Beschränkungen

1. Die Union oder die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß den Artikeln 11 bis 19 sowie gemäß Artikel 32 beschränken, sofern eine solche Beschränkung ein eindeutig festgelegtes im öffentlichen Interesse liegendes Ziel verfolgt, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahrt, in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck steht und die Grundrechte und Interessen der betroffenen Person achtet, sowie in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist

a) zum Schutz der öffentlichen Sicherheit

b) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten

c) Steuerfragen

d) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe

e) für Kontroll-, Überwachungs- und Ordnungsfunktionen im Rahmen der Tätigkeit einer zuständigen öffentlichen Behörde für die unter den Buchstaben a, b, c und d genannten Zwecke

f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

2. Jede Legislativmaßnahme im Sinne des Absatzes 1 muss notwendig und verhältnismäßig in einer demokratischen Gesellschaft sein und spezifische Vorschriften enthalten zumindest zu

a) den mit der Verarbeitung verfolgten Zielen;

b) der Bestimmung des für die Verarbeitung Verantwortlichen;

c) den konkreten Zwecken und Mitteln der Verarbeitung;

d) den Schutzvorkehrungen gegen Missbrauch oder unrechtmäßigem Zugang oder unrechtmäßiger Weitergabe;

e) dem Recht betroffener Personen, über die Einschränkung informiert zu werden.

2a. Die in Absatz 1 genannten legislativen Maßnahmen dürfen private für die Verarbeitung Verantwortliche weder dazu ermächtigen noch dazu verpflichten, Daten zu speichern, die über das für das Erreichen des ursprünglichen Zwecks erforderliche Maß hinausgehen.

## KAPITEL IV

## FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

### ABSCHNITT 1

### ALLGEMEINE PFLICHTEN

#### Artikel 22

#### Pflichten und Rechenschaftspflicht des für die Verarbeitung Verantwortlichen

1. Der für die Verarbeitung Verantwortliche stellt durch geeignete und nachweisbare technische und organisatorische Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er in transparenter Weise den Nachweis dafür erbringen kann, dies erfolgt unter Berücksichtigung des Stands der Technik, der Art der Verarbeitung personenbezogener Daten, dem Zusammenhang, der Tragweite und der Zwecke der Verarbeitung, der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie der Art der Organisation sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung selbst.

1a. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung des Stands der Technik und der Implementierungskosten alle angemessenen Schritte, um Maßnahmen und Verfahren zur Einhaltung umzusetzen, durch die die autonome Wahl betroffener Personen kontinuierlich respektiert wird. Diese Maßnahmen zur Einhaltung werden mindestens alle zwei Jahre überprüft und erforderlichenfalls aktualisiert.

2. entfällt

3. Der für die Verarbeitung Verantwortliche muss in der Lage sein, die Angemessenheit und Wirksamkeit der in den Absätzen 1 und 2 genannten Maßnahmen nachzuweisen. Regelmäßige Berichte über die Tätigkeiten des für die Verarbeitung Verantwortlichen, wie die obligatorischen Berichte von kapitalmarktorientierten Unternehmen beinhalten eine zusammenfassende Beschreibung der in Absatz 1 genannten Strategien und Maßnahmen.

3a. Der für die Verarbeitung Verantwortliche hat das Recht, personenbezogene Daten innerhalb einer Unternehmensgruppe in der EU, zu der der für die Verarbeitung Verantwortliche gehört, zu übermitteln, wenn die Verarbeitung für berechtigte interne administrative Zwecke von verbundenen Geschäftsbereichen in der Unternehmensgruppe erforderlich ist, und ein angemessenes Niveau des Datenschutzes sowie die Interessen der betroffenen Personen im Rahmen von

internen Datenschutzbestimmungen oder gleichwertigen Verhaltensregeln im Sinne von Artikel 38 hinreichend berücksichtigt werden.

4. entfällt

Artikel 23

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1. Der für die Verarbeitung Verantwortliche und gegebenenfalls der Auftragsverarbeiter führt unter Berücksichtigung neuester technischer Errungenschaften, des Stands der Technik, bewährter internationaler Verfahren und den von der Verarbeitung ausgehenden Risiken sowohl zum Zeitpunkt der Festlegung der Zwecke und Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung geeignete und verhältnismäßige technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden, insbesondere, was die in Artikel 5 aufgeführten Grundsätze betrifft. Beim Datenschutz durch Technik wird dem gesamten Lebenszyklusmanagement personenbezogener Daten von der Erhebung über die Verarbeitung bis zur Löschung besondere Aufmerksamkeit geschenkt und der Schwerpunkt systematisch auf umfassende Verfahrensgarantien hinsichtlich der Richtigkeit, Vertraulichkeit, Vollständigkeit, physischen Sicherheit und Löschung personenbezogener Daten gelegt. Hat der für die Verarbeitung Verantwortliche eine Datenschutzfolgenabschätzung gemäß Artikel 33 vorgenommen, werden die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt.

1a. Zur Förderung einer breiten Umsetzung in verschiedenen Wirtschaftssektoren muss der Datenschutz durch Technik eine Voraussetzung für Angebote im Rahmen von Ausschreibungen gemäß der Richtlinie 2004/18/EG des Europäischen Parlaments und des Rates[1] sowie gemäß der Richtlinie 2004/17/EG des Europäischen Parlaments und des Rates[2] (Sektorenrichtlinie) sein.

2. Der für die Verarbeitung Verantwortliche stellt sicher, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen, gespeichert oder verbreitet werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und dass die betroffenen Personen in der Lage sind, die Verbreitung ihrer personenbezogenen Daten zu kontrollieren.

3. entfällt

4. entfällt

Artikel 24

Gemeinsam für die Verarbeitung Verantwortliche

In allen Fällen, in denen mehrere für die Verarbeitung Verantwortliche Zwecke und Mittel der Verarbeitung personenbezogener Daten gemeinsam festlegen, vereinbaren diese gemeinsam für die Verarbeitung Verantwortlichen, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die Verfahren und Mechanismen betrifft, die den betroffenen Person die Wahrnehmung ihrer Rechte ermöglichen. Die Vereinbarung spiegelt die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam für die Verarbeitung Verantwortlichen gegenüber betroffenen Personen gebührend wider und der Kern der Vereinbarung wird den betroffenen Personen zur Verfügung gestellt. Im Fall unklarer Verantwortlichkeiten haften die für die Verarbeitung Verantwortlichen gesamtschuldnerisch.

Artikel 25

Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen

1. Jeder für die Verarbeitung Verantwortliche, der sich in der in Artikel 3 Absatz 2 beschriebenen Situation befindet, benennt einen Vertreter in der Union.

2. Diese Pflicht gilt nicht für

a) für die Verarbeitung Verantwortliche, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz im Sinne von Artikel 41 bietet; oder

b) für die Verarbeitung Verantwortliche, die Daten in Bezug auf weniger als 5 000 betroffene Personen innerhalb eines Zeitraumes von zwölf aufeinanderfolgenden Monaten verarbeiten, wobei die Verarbeitung nicht in Bezug auf besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1, Standortdaten, Daten über Kinder oder Arbeitnehmerdaten aus groß angelegten Ablagesystemen stattfindet; oder

c) Behörden oder öffentliche Einrichtungen; oder

d) für die Verarbeitung Verantwortliche, die betroffenen Personen in der Union nur gelegentlich Waren oder Dienstleistungen anbieten, es sei denn, die Verarbeitung personenbezogener Daten betrifft in Artikel 9 Absatz 1 genannte besonderen Kategorien personenbezogener Daten, Standortdaten, Daten über Kinder oder Arbeitnehmerdaten aus groß angelegten Ablagesystemen;

3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen das Angebot der Waren oder Dienstleistungen den betroffenen Personen unterbreitet oder deren Verhalten beobachtet wird.

4. Die Benennung eines Vertreters durch den für die Verarbeitung Verantwortlichen erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen.

## Artikel 26

## Auftragsverarbeiter

1. Der für die Verarbeitung Verantwortliche wählt für jede in seinem Auftrag durchzuführende Verarbeitung einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.

2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können ihre jeweiligen Funktionen und Aufgaben in Bezug auf die Anforderungen dieser Verordnung festlegen und sehen vor, dass der Auftragsverarbeiter:

a) nur auf Weisung des für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeitet, es sei denn, in Rechtsvorschriften der Union oder der Mitgliedstaaten ist etwas anderes bestimmt;

b) ausschließlich Mitarbeiter beschäftigt, die sich zur Vertraulichkeit verpflichtet haben oder der gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle in Artikel 30 genannten erforderlichen Maßnahmen ergreift;

d) sofern nichts anderes bestimmt ist, die Bedingungen festlegt, unter denen die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf,

e) soweit es verarbeitungsbedingt möglich ist, in Absprache mit dem für die Verarbeitung Verantwortlichen die geeigneten und zweckmäßigen technischen und organisatorischen Voraussetzungen dafür schafft, dass der für die Verarbeitung Verantwortliche seine Pflicht erfüllen kann, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) den Auftragsverarbeiter bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen unterstützt ;

g) nach Abschluss der Verarbeitung dem für die Verarbeitung Verantwortlichen sämtliche Ergebnisse zurückgibt, die personenbezogenen Daten auf keine andere Weise weiterverarbeitet und bestehende Kopien löscht, es sei denn, in Rechtsvorschriften der Union oder der Mitgliedstaaten ist die Speicherung der Daten vorgesehen;

h) dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen für den Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Nachprüfungen vor Ort zulässt.

3. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dokumentieren die Anweisungen des für die Verarbeitung Verantwortlichen und die in Absatz 2 aufgeführten Pflichten des Auftragsverarbeiters.

3a. Die hinreichenden Garantien gemäß Absatz 1 können durch die Einhaltung von Verhaltenskodizes oder Zertifizierungsverfahren gemäß Artikel 38 oder 39 dieser Verordnung nachgewiesen werden.

4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, oder die entscheidende Partei in Bezug auf die Zwecke und Mittel der Datenverarbeitung wird, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.

5. entfällt

## Artikel 27

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

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

## Artikel 28

## Dokumentation

1. Alle für die Verarbeitung Verantwortlichen und alle Auftragsverarbeiter halten die zur Erfüllung der in dieser Verordnung festgelegten Anforderungen notwendige Dokumentation vor und aktualisieren sie regelmäßig.

2. Darüber hinaus halten alle für die Verarbeitung Verantwortlichen und alle Auftragsverarbeiter Dokumentationen zu folgenden Informationen vor:

a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (oder etwaiger gemeinsam für die Verarbeitung Verantwortlicher) oder des Auftragsverarbeiters sowie eines etwaigen Vertreters;

b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;

c) entfällt

d) entfällt

e) Name und Kontaktdaten der etwaigen für die Verarbeitung Verantwortlichen, denen personenbezogene Daten mitgeteilt werden;

f) entfällt

g) entfällt

(h) entfällt

3. entfällt

4. entfällt

a) entfällt

b) entfällt

5. entfällt

6. entfällt

Artikel 29

Zusammenarbeit mit der Aufsichtsbehörde

1. Der für die Verarbeitung Verantwortliche, der etwaige Auftragsverarbeiter sowie der Vertreter des für die Verarbeitung Verantwortlichen arbeiten der Aufsichtsbehörde auf Verlangen zu, um ihr die Erfüllung ihrer Pflichten zu erleichtern, indem sie dieser insbesondere die in Artikel 53 Absatz 2 Buchstabe a genannten Informationen übermitteln und ihr den in Artikel 53 Absatz 2 Buchstabe b genannten Zugang gewähren.

2. Auf von der Aufsichtsbehörde im Rahmen der Ausübung ihrer Befugnisse erteilte Anordnungen gemäß Artikel 53 Absatz 2 antworten der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter der Aufsichtsbehörde binnen einer von der Aufsichtsbehörde zu setzenden angemessenen Frist. Die Antwort muss auch eine Beschreibung der im Anschluss an die Bemerkungen der Aufsichtsbehörde getroffenen Maßnahmen und der damit erzielten Ergebnisse beinhalten.

ABSCHNITT 2

DATENSICHERHEIT

Artikel 30

Sicherheit der Verarbeitung

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten

technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken unter Berücksichtigung der Ergebnisse der Datenschutz-Folgenabschätzung gemäß Artikel 33 angemessen ist.

1a. Eine solche Sicherheitspolitik umfasst – unter Berücksichtigung des Stands der Technik und der Implementierungskosten – Folgendes:

a) die Fähigkeit zu gewährleisten, dass die Vollständigkeit der personenbezogenen Daten bestätigt wird;

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

c) die Fähigkeit, die Verfügbarkeit und den Zugang zu Daten rasch im Falle eines physischen oder technischen Vorfalls, der sich auf die Verfügbarkeit, Vollständigkeit und Vertraulichkeit der Informationssysteme und -dienste auswirkt, wiederherzustellen;

d) zusätzliche Sicherheitsmaßnahmen im Falle der Verarbeitung sensibler personenbezogener Daten nach Artikel 8 und 9, um ein situationsbezogenes Risikobewusstsein sicherzustellen, sowie die Fähigkeit, Präventiv- und Abhilfemaßnahmen sowie abmildernde Maßnahmen zeitnah gegen festgestellte Schwachstellen oder Vorfälle zu ergreifen, die ein Risiko für die Daten darstellen könnten;

e) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen, -verfahren und -pläne, die aufgestellt werden, um die Wirksamkeit auf Dauer sicherzustellen;

2. Die in Absatz 1 genannten Maßnahmen bewirken zumindest, dass

a) sichergestellt wird, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten,

b) gespeicherte oder übermittelte personenbezogene Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe geschützt werden, und

c) die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten gewährleistet wird.

3. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b in Bezug auf die in den Absätzen 1 und 2 genannten technischen und organisatorischen Maßnahmen zu veröffentlichen und den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen, wobei er insbesondere die technologische Entwicklung sowie Lösungen für einen

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen berücksichtigt.

4. entfällt

a) entfällt

b) entfällt

c) entfällt

## Artikel 31

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

1. Bei einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde unverzüglich.

2. Der Auftragsverarbeiter alarmiert und informiert den für die Verarbeitung Verantwortlichen unverzüglich nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.

3. Die in Absatz 1 genannte Benachrichtigung enthält mindestens folgende Informationen:

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

b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;

c) Empfehlungen für Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten;

e) eine Beschreibung der vom für die Verarbeitung Verantwortlichen vorgeschlagenen oder ergriffenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und zur Minderung ihrer Auswirkungen.

Die Information kann, wenn nötig, auch stufenweise erfolgen.

4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss ausreichend sein, um der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses

Artikels und von Artikel 30 ermöglichen. Die Dokumentation enthält nur die zu diesem Zweck erforderlichen Informationen.

4a. Die Aufsichtsbehörde führt ein öffentliches Verzeichnis der Arten der gemeldeten Verletzungen.

5. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b in Bezug auf die Feststellung der Verletzungen des Schutzes personenbezogener Daten zu veröffentlichen sowie die Unverzüglichkeit gemäß Absatz 1 und 2 und die konkreten Umstände, unter denen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben, festzulegen.

6. entfällt

## Artikel 32

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

1. Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung nach Artikel 31 die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten, wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten, die Privatsphäre, die Rechte oder die berechtigten Interessen der betroffenen Person durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird.

Die in Absatz 1 genannte Benachrichtigung der betroffenen Person ist umfassend, klar und für jedermann verständlich. Sie beschreibt die Art der Verletzung des Schutzes der personenbezogenen Daten und umfasst mindestens die in Artikel 31 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen sowie Informationen über die Rechte betroffener Personen einschließlich der Rechtsbehelfe.

2. entfällt

3. Die Benachrichtigung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten ist nicht erforderlich, wenn der für die Verarbeitung Verantwortliche zur Zufriedenheit der Aufsichtsbehörde nachweist, dass er geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Durch diese technischen Sicherheitsvorkehrungen sind die betreffenden Daten für alle Personen zu verschlüsseln, die nicht zum Zugriff auf die Daten befugt sind.

4. Unbeschadet der dem für die Verarbeitung Verantwortlichen obliegenden Pflicht, der betroffenen Person die Verletzung des Schutzes personenbezogener Daten mitzuteilen, kann die Aufsichtsbehörde, falls der für die Verarbeitung Verantwortliche die betroffene Person noch nicht in Kenntnis gesetzt hat, nach

Prüfung der zu erwartenden negativen Auswirkungen der Verletzung den für die Verarbeitung Verantwortlichen auffordern, dies zu tun.

Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b in Bezug auf die Kriterien und Anforderungen in Bezug auf die Umstände zu veröffentlichen, unter denen sich eine Verletzung des Schutzes personenbezogener Daten negativ auf die in Absatz 1 genannten personenbezogenen Daten, die Privatsphäre, die Rechte oder die berechtigten Interessen der betroffenen Person auswirken kann.

5. entfällt

6. entfällt

Artikel 32a

Einhaltung der Risikogrundsätze

1. Der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter führt eine Risikoanalyse zu den möglichen Auswirkungen der beabsichtigten Datenverarbeitung auf die Rechte und Freiheiten der betroffenen Personen durch, um zu bewerten, ob seine Verarbeitungsvorgänge konkrete Risiken bergen können.

2. Folgende Verarbeitungsvorgänge können konkrete Risiken beinhalten:

a) Verarbeitung personenbezogener Daten von mehr als 5 000 betroffenen Personen innerhalb eines Zeitraums von zwölf aufeinanderfolgenden Monaten;

b) Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1, Standortdaten, Daten über Kinder oder Arbeitnehmerdaten in groß angelegten Ablagesystemen;

c) Profiling, das als Grundlage für Maßnahmen dient, welche Rechtswirkungen gegenüber der betroffenen Person entfalten oder ähnlich erhebliche Auswirkungen für diese mit sich bringen;

d) Verarbeitung personenbezogener Daten für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten, wenn die betreffenden Daten in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen;

e) automatisierte weiträumige Überwachung öffentlich zugänglicher Bereiche;

f) sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab der Datenschutzbeauftragte oder die Aufsichtsbehörde anzuhören ist;

g) Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten zu negativen Auswirkungen auf den Schutz der personenbezogenen Daten, die Privatsphäre, die Rechte oder die legitimen Interessen der betroffenen Person führt;

h) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen;

i) personenbezogene Daten werden einer großen Zahl von Personen zugänglich gemacht, von der vernünftigerweise nicht erwartet werden kann, dass sie begrenzt wird.

3. Ergibt die Risikoanalyse, dass

a) Verarbeitungsvorgänge gemäß Absatz 2 Buchstabe a oder b vorliegen, müssen die für die Verarbeitung Verantwortlichen, die keine Niederlassung in der Europäischen Union haben, gemäß den Voraussetzungen und Ausnahmen in Artikel 25 einen Vertreter in der Europäischen Union benennen;

b) Verarbeitungsvorgänge gemäß Absatz 2 Buchstabe a, b oder h vorliegen, müssen die für die Verarbeitung Verantwortlichen gemäß den Voraussetzungen und Ausnahmen in Artikel 35 einen Datenschutzbeauftragten benennen;

c) Verarbeitungsvorgänge gemäß Absatz 2 Buchstabe a, b, c, d, e, f, g oder h vorliegen, müssen die für die Verarbeitung Verantwortlichen oder die in ihrem Auftrag handelnden Auftragsverarbeiter eine Datenschutz-Folgenabschätzung gemäß Artikel 33 durch;

d) Verarbeitungsvorgänge gemäß Absatz 2 Buchstabe f vorliegen, müssen die für die Verarbeitung Verantwortlichen den Datenschutzbeauftragten oder wenn kein Datenschutzbeauftragter benannt wurde, die Aufsichtsbehörde gemäß Artikel 34 zu Rate ziehen;

4. Die Risikoanalyse wird spätestens nach einem Jahr überprüft oder unverzüglich, wenn sich das Wesen, der Umfang oder der Zweck der Datenverarbeitungsvorgänge wesentlich ändern. Ist der für die Verarbeitung Verantwortliche gemäß Absatz 3 Buchstabe c nicht verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wird die Risikoanalyse dokumentiert.

## ABSCHNITT 3

## LEBENSZYKLUSMANAGEMENT IN BEZUG AUF DEN DATENSCHUTZ

### Artikel 33

### Datenschutz-Folgenabschätzung

1. Wenn dies nach Maßgabe von Artikel 32a Absatz 3 erforderlich ist, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die Rechte und Freiheiten der betroffenen Personen, insbesondere für ihr Recht auf den Schutz personenbezogener Daten durch. Eine einzige Abschätzung ist für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlichen Risiken ausreichend.

2. entfällt

a) entfällt

b) entfällt

c) entfällt

d) entfällt

e) entfällt

3. Die Folgenabschätzung bezieht sich auf das gesamte Lebenszyklusmanagement personenbezogener Daten, von der Erhebung über die Verarbeitung bis zur Löschung. Zumindest Folgendes ist enthalten:

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

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

c) eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken, einschließlich des Diskriminierungsrisikos, das mit dem Vorgang verbunden ist oder durch diesen erhöht wird;

d) eine Beschreibung der geplanten Abhilfemaßnahmen und Maßnahmen zur Minimierung der Menge der verarbeiteten personenbezogenen Daten;

e) eine Aufstellung der Garantien, Sicherheitsvorkehrungen und Verfahren – wie die Pseudonymisierung –, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung getragen wird;

f) eine allgemeine Angabe der Fristen für die Löschung der verschiedenen Datenkategorien;

h) eine Erklärung, welche Maßnahmen in Bezug auf den Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 23 umgesetzt wurden;

i) eine Aufstellung der Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

j) gegebenenfalls eine Liste mit Angaben über geplante Datenübermittlungen in Drittländer oder an internationale Organisationen, einschließlich deren Namen, sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen ein Beleg dafür, dass geeignete Sicherheitsgarantien vorgesehen wurden;

k) eine Bewertung des Zusammenhangs der Datenverarbeitung.

3a. Wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter einen Datenschutzbeauftragten benannt hat, ist dieser am Verfahren der Folgenabschätzung zu beteiligen.

3b. Die Folgenabschätzung wird dokumentiert und es wird ein Plan für regelmäßige Überprüfungen der Einhaltung der Datenschutzbestimmungen gemäß Artikel 33a Absatz 1 festgelegt. Die Folgenabschätzung wird ohne unangemessene Verzögerung aktualisiert, wenn die Ergebnisse der Überprüfung der Einhaltung der Datenschutzbestimmungen gemäß Artikel 33a Unstimmigkeiten bei der Einhaltung aufzeigen. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen die Folgenabschätzung der Aufsichtsbehörde auf Anforderung zur Verfügung.

4. entfällt

5. entfällt

6. entfällt

7. entfällt

## Artikel 33a

## Überprüfung der Einhaltung der Datenschutzbestimmungen

1. Der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter führt spätestens zwei Jahre nach der Durchführung einer Folgenabschätzung nach Artikel 33 Absatz 1 eine Überprüfung der Einhaltung der Datenschutzbestimmungen durch. Mit dieser Überprüfung wird nachgewiesen, dass die Verarbeitung personenbezogener Daten in Einklang mit der Datenschutz-Folgenabschätzung durchgeführt wird.

2. Die Überprüfung der Einhaltung der Datenschutzbestimmungen wird in regelmäßigen Abständen mindestens alle zwei Jahre durchgeführt oder unverzüglich, wenn sich die mit Verarbeitungsvorgängen verbundenen spezifischen Risiken ändern.

3. Wenn die Ergebnisse der Überprüfung der Einhaltung der Datenschutzbestimmungen Unstimmigkeiten bei der Einhaltung aufzeigen, enthält die Überprüfung Empfehlungen, wie eine vollständige Einhaltung erreicht werden kann.

4. Die Überprüfung der Einhaltung der Datenschutzbestimmungen und die einschlägigen Empfehlungen werden dokumentiert. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen der Aufsichtsbehörde auf Anforderung die Überprüfung der Einhaltung der Datenschutzbestimmungen zur Verfügung.

5. Wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter einen Datenschutzbeauftragten benannt hat, ist dieser am Verfahren zur Überprüfung der Einhaltung der Datenschutzbestimmungen zu beteiligen.

## Artikel 34

## Vorherige Konsultation

1. entfällt

2. Der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter zieht vor der Verarbeitung personenbezogener Daten den Datenschutzbeauftragten, oder wenn kein Datenschutzbeauftragter benannt wurde, die Aufsichtsbehörde zu Rate, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die für die betroffenen Personen bestehenden Risiken zu mindern; dies gilt für alle Fälle, in denen

a) aus einer Datenschutz-Folgenabschätzung nach Artikel 33 hervorgeht, dass die geplanten Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke hohe konkrete Risiken bergen können; oder

b) der Datenschutzbeauftragte oder die Aufsichtsbehörde eine vorherige Konsultation bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält.

3. Falls die zuständige Aufsichtsbehörde im Rahmen ihrer Befugnisse feststellt, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, untersagt sie die geplante Verarbeitung und unterbreitet geeignete Vorschläge, wie diese Mängel beseitigt werden könnten.

4. Der Europäische Datenschutzausschuss erstellt eine Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Konsultation nach Absatz 2 sind, und veröffentlicht diese.

5. entfällt

6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter legt der Aufsichtsbehörde die Datenschutz-Folgenabschätzung nach Artikel 33 vor und übermittelt ihr auf Aufforderung alle sonstigen Informationen, die sie benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den

Schutz der personenbezogenen Daten der betroffenen Person bestehenden Risiken und die diesbezüglichen Sicherheitsgarantien bewerten zu können.

7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung einer von ihren nationalen Parlamenten zu erlassenden Legislativmaßnahme oder einer sich auf eine solche Legislativmaßnahme gründenden Maßnahme, durch die die Art der Verarbeitung definiert wird, zu Rate, damit die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sichergestellt ist und insbesondere die für die betreffenden Personen bestehenden Risiken gemindert werden.

8. entfällt

9. entfällt

## ABSCHNITT 4

## DATENSCHUTZBEAUFTRAGTER

### Artikel 35

### Benennung eines Datenschutzbeauftragten

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls

a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder

b) die Verarbeitung von einer juristischen Person durchgeführt wird und sich auf mehr als 5 000 betroffene Personen innerhalb eines Zeitraumes von zwölf aufeinanderfolgenden Monaten bezieht; oder

c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen; oder

d) die Kernaktivitäten des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters aus der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 Absatz 1, Standortdaten, Daten über Kinder oder Arbeitnehmerdaten in groß angelegten Ablagesystemen bestehen.

2. Eine Gruppe von Unternehmen kann einen Hauptdatenschutzbeauftragten ernennen, wenn sichergestellt ist, dass von jedem Standort aus ein Datenschutzbeauftragter leicht zugänglich ist.

3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann der Datenschutzbeauftragte unter Berücksichtigung der Struktur der Behörde beziehungsweise der öffentlichen Einrichtung für mehrere Bereiche benannt werden.

4. In anderen als den in Absatz 1 genannten Fällen können der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen.

5. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt den Datenschutzbeauftragten nach Maßgabe der beruflichen Qualifikation und insbesondere des Fachwissens, das dieser auf dem Gebiet des Datenschutzrechts und der einschlägigen Praktiken besitzt, sowie nach Maßgabe von dessen Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben. Der Grad des erforderlichen Fachwissens richtet sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten.

6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass etwaige sonstige berufliche Pflichten des Datenschutzbeauftragten mit den Aufgaben und Pflichten, die diesem in seiner Funktion als Datenschutzbeauftragter obliegen, vereinbar sind und zu keinen Interessenkonflikten führen.

7. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt einen Datenschutzbeauftragten für einen Zeitraum von mindestens vier Jahren im Fall eines Arbeitnehmers oder zwei Jahren im Fall eines externen Dienstleisters. Der Datenschutzbeauftragte kann für weitere Amtszeiten wiederernannt werden. Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt.

8. Der Datenschutzbeauftragte kann durch den für die Verarbeitung Verantwortlichen oder durch den Auftragsverarbeiter beschäftigt werden oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

9. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter teilt der Aufsichtsbehörde und der Öffentlichkeit den Namen und die Kontaktdaten des Datenschutzbeauftragten mit.

10. Betroffene Personen haben das Recht, den Datenschutzbeauftragten zu allen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehenden Fragen zu Rate zu ziehen und die Wahrnehmung ihrer Rechte gemäß dieser Verordnung zu beantragen.

11. entfällt

## Artikel 36

## Stellung des Datenschutzbeauftragten

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit

dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

2. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte seinen Pflichten und Aufgaben unabhängig nachkommen kann und keine Anweisungen bezüglich der Ausübung seiner Tätigkeit erhält. Der Datenschutzbeauftragte berichtet unmittelbar der obersten Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen zu diesem Zweck ein Mitglied der obersten Leitung, das die Verantwortung für die Einhaltung der Bestimmungen dieser Verordnung trägt.

3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und stellt alle Mittel, darunter das erforderliche Personal, die erforderlichen Räumlichkeiten, die erforderliche Ausrüstung und alle sonstigen Ressourcen, die für die Erfüllung der in Artikel 37 genannten Pflichten und Aufgaben und zur Pflege der Fachkenntnisse erforderlich sind, zur Verfügung.

## Artikel 37

## Aufgaben des Datenschutzbeauftragten

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter betraut den Datenschutzbeauftragten mit mindestens folgenden Aufgaben:

a) Sensibilisierung, Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters über dessen aus dieser Verordnung erwachsenden Pflichten sowie Dokumentation dieser Tätigkeit und der erhaltenen Antworten, insbesondere in Bezug auf technische und organisatorische Maßnahmen und Verfahren;

b) Überwachung der Umsetzung und Anwendung der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Überwachung der Umsetzung und Anwendung dieser Verordnung, insbesondere ihrer Anforderungen an einen Datenschutz durch Technik und an datenschutzfreundliche Voreinstellungen, an die Datensicherheit, an die Benachrichtigung der betroffenen Personen und an die Anträge der betroffenen Personen zur Wahrnehmung der ihren nach dieser Verordnung zustehenden Rechte;

d) Sicherstellung, dass die in Artikel 28 genannte Dokumentation vorgenommen wird;

e) Überwachung der Dokumentation und Meldung von Verletzungen des Schutzes personenbezogener Daten sowie die Benachrichtigung davon gemäß den Artikeln 31 und 32;

f) Überwachung der von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter durchgeführten Datenschutz-Folgenabschätzung sowie der Beantragung einer vorherigen Konsultation gemäß den Artikeln 32a, 33 und 34;

g) Überwachung der auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutzbeauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;

(h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen sowie gegebenenfalls Zurateziehung der Aufsichtsbehörde auf eigene Initiative.

i) Überprüfung der Einhaltung der Verordnung gemäß dem vorherigen Konsultierungsverfahren nach Artikel 34.

j) Unterrichtung der Arbeitnehmervertreter über die Verarbeitung von Daten der Arbeitnehmer.

2. entfällt

## ABSCHNITT 5

## VERHALTENSREGELN UND ZERTIFIZIERUNG

### Artikel 38

### Verhaltensregeln

1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln oder die Annahme von durch eine Aufsichtsbehörde ausgearbeiteten Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen:

a) faire und transparente Datenverarbeitung,

aa) Achtung der Rechte der Verbraucher;

b) Datenerhebung,

c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;

d) von betroffenen Personen in Ausübung ihrer Rechte gestellte Anträge;

e) Unterrichtung und Schutz von Kindern;

f) Datenübermittlung in Drittländer oder an internationale Organisationen;

g) Mechanismen zur Überwachung und zur Sicherstellung der Einhaltung der Verhaltensregeln durch die diesen unterliegenden für die Verarbeitung Verantwortlichen;

(h) außergerichtliche Verfahren und sonstige Streitschlichtungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der den betroffenen Personen aus den Artikeln 73 und 75 erwachsenden Rechte.

2. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten und beabsichtigen, eigene Verhaltensregeln aufzustellen oder bestehende Verhaltensregeln zu ändern oder zu erweitern, können diesbezügliche Vorschläge der Aufsichtsbehörde in dem betreffenden Mitgliedstaat zur Stellungnahme vorlegen. Die Aufsichtsbehörde nimmt unverzüglich zu der Frage Stellung, ob die Verarbeitung nach dem betreffenden Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde hört die betroffenen Personen oder ihre Vertreter zu diesen Vorschlägen an.

3. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von Verhaltensregeln sowie Vorschläge zur Änderung oder Ausweitung bestehender Verhaltensregeln vorlegen.

4. Die Kommission wird ermächtigt, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat, im Wege delegierter Rechtsakte gemäß Artikel 86 zu beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln im Einklang mit dieser Verordnung stehen und allgemeine Gültigkeit in der Union besitzen. Mit diesen delegierten Rechtsakten werden den betroffenen Personen durchsetzbare Rechte übertragen.

5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

## Artikel 39

## Zertifizierung

1. entfällt

1a. Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird, insbesondere mit den Grundsätzen der Artikel 5, 23 und 30, den Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter und den Rechten der betroffenen Person.

1b. Die Zertifizierung ist freiwillig, erschwinglich und über ein transparentes und nicht übermäßig aufwändiges Verfahren zugänglich.

1c. Die Aufsichtsbehörden und der Europäische Datenschutzausschuss arbeiten im Rahmen des Kohärenzverfahrens gemäß Artikel 57 zusammen, um ein harmonisiertes datenschutzspezifisches Zertifizierungsverfahren zu gewährleisten, einschließlich harmonisierter Gebühren innerhalb der Union.

1d. Während des Zertifizierungsverfahrens kann die Aufsichtsbehörde spezialisierte dritte Prüfer akkreditieren, die Prüfung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für sie durchzuführen. Dritte Prüfer verfügen über ausreichend Personal, sind unparteiisch und in Bezug auf ihre Aufgaben frei von Interessenskonflikten. Aufsichtsbehörden entziehen die Akkreditierung, wenn es Grund zu der Annahme gibt, dass der Prüfer seine Aufgaben nicht korrekt erfüllt. Die endgültige Zertifizierung erteilt die Aufsichtsbehörde.

1e. Die Aufsichtsbehörden erteilen den für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, denen nach der Prüfung zertifiziert wird, dass sie personenbezogene Daten im Einklang mit dieser Verordnung verarbeiten, das standardisierte Datenschutzzeichen mit der Bezeichnung „Europäisches Datenschutzsiegel“.

1f. Das „Europäische Datenschutzsiegel“ ist so lange gültig, wie die Verarbeitungsprozesse des zertifizierten für die Verarbeitung Verantwortlichen oder des zertifizierten Auftragsverarbeiters weiter vollständig dieser Verordnung entsprechen.

1g. Unbeschadet des Absatzes 1f ist die Zertifizierung höchstens fünf Jahre gültig.

1h. Der Europäische Datenschutzausschuss richtet ein öffentliches elektronisches Register ein, in dem die Öffentlichkeit Einsicht in alle gültigen und ungültigen Zertifikate, die von den Mitgliedstaaten ausgestellt wurden, nehmen kann.

1i. Der Europäische Datenschutzausschuss kann auf eigene Initiative zertifizieren, dass ein technischer Standard zur Verbesserung des Datenschutzes mit dieser Verordnung vereinbar ist.

2. Die Kommission wird ermächtigt, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat und nach Anhörung von Interessenträgern, insbesondere Industrieverbände und nichtstaatliche Organisationen, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in den Absätzen 1a bis 1h genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Akkreditierung der Prüfer, der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen. Mit diesen delegierten Rechtsakten werden den betroffenen Personen durchsetzbare Rechte übertragen.

3. entfällt

## KAPITEL V

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

### Artikel 40

### Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.

### Artikel 41

### Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

1. Eine Datenübermittlung darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.

2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission

a) die Rechtsstaatlichkeit, die geltenden allgemeinen und sektorspezifischen Vorschriften, insbesondere über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, die Umsetzung dieser Rechtsvorschriften, die in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation geltenden Standesregeln und Sicherheitsvorschriften, juristische Präzedenzfälle sowie die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen und insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden;

b) die Existenz und die Wirksamkeit einer oder mehrerer in dem betreffenden Drittland beziehungsweise in der betreffenden internationalen Organisation tätiger unabhängiger Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften, einschließlich hinreichender Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind; und

c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation eingegangenen internationalen Verpflichtungen, insbesondere rechtlich verbindliche Übereinkommen oder Instrumente in Bezug auf den Schutz personenbezogener Daten.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um festzustellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. Diese delegierten Rechtsakte sehen, wenn sie den Verarbeitungssektor betreffen, eine Verfallsklausel vor und werden, sobald ein angemessenes Niveau des Schutze gemäß dieser Verordnung nicht mehr gewährleistet ist, gemäß Artikel 5 aufgehoben.

4. In jedem delegierten Rechtsakt werden der territoriale und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben.

5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um festzustellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bietet oder nicht mehr bietet; dies gilt insbesondere für Fälle, in denen die in dem betreffenden Drittland beziehungsweise der betreffenden internationalen Organisation geltenden allgemeinen und sektorspezifischen Vorschriften keine wirksamen und durchsetzbaren Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für in der Union ansässige betroffene Personen und insbesondere für betroffene Personen, deren personenbezogene Daten übermittelt werden, garantieren.

6. Wenn die Kommission die in Absatz 5 genannte Feststellung trifft, wird dadurch jedwede Übermittlung personenbezogener Daten an das betreffende Drittland beziehungsweise an ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder an die betreffende internationale Organisation unbeschadet der Bestimmungen der Artikel 42 bis 44 untersagt. Die Kommission nimmt zu geeigneter Zeit Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation auf, um Abhilfe für die Situation, die aus dem gemäß Absatz 5 erlassenen Beschluss entstanden ist, zu schaffen.

6a. Vor Erlass der delegierten Rechtsakte gemäß den Absätzen 3 und 5 ersucht die Kommission den Europäischen Datenschutzausschuss um eine Stellungnahme zur Angemessenheit des Datenschutzniveaus. Zu diesem Zweck versorgt die Kommission den Europäischen Datenschutzausschuss mit allen erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlands, Gebiets oder Verarbeitungssektors eines Drittlands oder der internationalen Organisation.

7. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren von Drittländern und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese einen beziehungsweise keinen angemessenen Schutz personenbezogener Daten bieten.

8. Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben fünf Jahre nach Inkrafttreten dieser Verordnung in Kraft, es sei denn, sie wird durch die Kommission vor Ende dieses Zeitraums geändert, ersetzt oder aufgehoben.

## Artikel 42

## Datenübermittlung auf der Grundlage geeigneter Garantien

1. Hat die Kommission keinen Beschluss nach Artikel 41 erlassen oder hat sie festgestellt, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Datenschutz im Einklang mit Artikel 41 Absatz 5 bietet, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter nur dann personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermitteln, wenn er in einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.

2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere bestehen in Form

a) verbindlicher unternehmensinterner Vorschriften nach Artikel 43; oder

aa) eines gültigen europäischen Datenschutzsiegels gemäß Artikel 39 Absatz 1e für den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter; oder

b) entfällt

c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommener Standarddatenschutzklauseln, sofern diesen von der Kommission allgemeine Gültigkeit gemäß Artikel 62 Absatz 1 Buchstabe b zuerkannt wurde, oder

d) von Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden.

3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, aa, b oder c genannten Standarddatenschutzklauseln, eines europäischen Datenschutzsiegels oder unternehmensinternen Vorschriften erfolgen, bedürfen keiner besonderen Genehmigung.

4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung der Aufsichtsbehörde ein. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.

5. Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben zwei Jahre nach Inkrafttreten dieser Verordnung oder so lange in Kraft, es sei denn, sie werden durch die Aufsichtsbehörde vor Ende dieses Zeitraums geändert, ersetzt oder aufgehoben.

## Artikel 43

## Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften

1. Die Aufsichtsbehörde kann nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens verbindliche unternehmensinterne Vorschriften genehmigen, sofern diese

a) rechtsverbindlich sind, für alle Mitglieder der Unternehmensgruppe des für die Verarbeitung Verantwortlichen oder der externen Subunternehmer, die in den Anwendungsbereich der verbindlichen unternehmensinternen Vorschriften fallen, sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden;

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen;

c) die in Absatz 2 festgelegten Anforderungen erfüllen.

1a. In Bezug auf Beschäftigungsdaten werden die Arbeitnehmervertreter unterrichtet und gemäß Rechtsvorschriften und Praktiken der Union oder der Mitgliedstaaten in die Erarbeitung verbindlicher unternehmensinterner Vorschriften gemäß Artikel 43 einbezogen.

2. Alle verbindlichen unternehmensinternen Vorschriften enthalten mindestens folgende Informationen:

a) Struktur und Kontaktdaten der Unternehmensgruppe und ihrer Mitglieder und der externen Subunternehmer, die in den Anwendungsbereich der verbindlichen unternehmensinternen Vorschriften fallen;

b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Kategorien personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Vorschriften;

d) die allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, die Datenminimierung, begrenzte Aufbewahrungsfristen, die Datenqualität, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, die Rechtsgrundlage für die Verarbeitung sowie die Bestimmungen für etwaige Verarbeitungen sensibler personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese Vorschriften gebundene Organisationen;

e) die Rechte der betroffenen Personen und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

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

g) die Art und Weise, wie die betroffenen Personen gemäß Artikel 11 über die verbindlichen unternehmensinternen Vorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

(h) die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;

i) die innerhalb der Unternehmensgruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften;

j) die Verfahren für die Meldung und Erfassung von Änderungen der Unternehmenspolitik und ihre Meldung an die Aufsichtsbehörde;

k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe gewährleisten, wie insbesondere die Offenlegung der Ergebnisse der Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Format, Verfahren, die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung, einschließlich Transparenz für betroffene Personen, und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.

4. entfällt

## Artikel 43a

Übermittlung oder Weitergabe, die nicht im Einklang mit dem Unionsrecht stehen

1. Unbeschadet eines Abkommens über Amtshilfe oder eines zwischen dem ersuchenden Drittstaat und der Union oder einem Mitgliedstaat geltenden internationalen Übereinkommens werden Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verlangen, personenbezogene Daten weiterzugeben, weder anerkannt noch in irgendeiner Weise vollstreckt.

2. Verlangt ein Urteil eines Gerichts oder eine Entscheidung einer Verwaltungsbehörde eines Drittstaats von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, personenbezogene Daten weiterzugeben, so unterrichtet der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter bzw. ein etwaiger Vertreter des für die Verarbeitung Verantwortlichen die Aufsichtsbehörde unverzüglich über das Ersuchen und muss von der Aufsichtsbehörde die vorherige Genehmigung für die Übermittlung oder Weitergabe erhalten.

3. Die Aufsichtsbehörde prüft die Vereinbarkeit der beantragten Weitergabe mit der Verordnung und insbesondere, ob die Weitergabe gemäß Artikel 44 Absatz 1 Buchstabe d und e sowie Artikel 44 Absatz 5 erforderlich und rechtlich vorgeschrieben ist. Sind betroffene Personen anderer Mitgliedstaaten betroffen, bringt die Aufsichtsbehörde das in Artikel 57 beschriebene Kohärenzverfahren zur Anwendung.

4. Die Aufsichtsbehörde unterrichtet die zuständige einzelstaatliche Behörde über das Ersuchen. Unbeschadet des Artikels 21 unterrichtet der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter auch die betroffene Person über das Ersuchen und über die Genehmigung der Aufsichtsbehörde sowie gegebenenfalls darüber, ob personenbezogene Daten innerhalb der letzten zwölf aufeinanderfolgenden Monate gemäß Artikel 14 Absatz 1 Buchstabe ha an Behörden übermittelt wurden.

## Artikel 44

## Ausnahmen

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 vorliegt noch geeignete Garantien nach Artikel 42 bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur zulässig, wenn

a) die betroffene Person der vorgeschlagenen Datenübermittlung zugestimmt hat, nachdem sie über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführter Datenübermittlungen informiert wurde,

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

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

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

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

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

g) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

(h) entfällt

2. Datenübermittlungen gemäß Absatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

3. entfällt

4. Absatz 1 Buchstaben b und c gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

5. Das in Absatz 1 Buchstabe d genannte öffentliche Interesse muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.

6. entfällt

7. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken in Bezug auf die weitere Festlegung der Kriterien und Bedingungen für die Übermittlung von Daten gemäß Absatz 1 nach Maßgabe von Artikel 66 Absatz 1 Buchstabe b zu veröffentlichen.

## Artikel 45

## Internationale Zusammenarbeit zum Schutz personenbezogener Daten

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur

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

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

c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,

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

da) Klärung und Beratung von Zuständigkeitskonflikten mit Drittländern.

2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen und insbesondere zu deren Aufsichtsbehörden, wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese einen angemessenen Schutz bieten.

### Artikel 45a

### Bericht der Kommission

Die Kommission legt dem Europäischen Parlament und dem Rat spätestens vier Jahre nach dem in Artikel 91 Absatz 1 genannten Termin in regelmäßigen Abständen einen Bericht über die Anwendung der Artikel 40 bis 45 vor. Hierzu kann die Kommission von den Mitgliedstaaten und den Aufsichtsbehörden Informationen einholen, die unverzüglich zu übermitteln sind. Dieser Bericht wird veröffentlicht.

## KAPITEL VI

## UNABHÄNGIGE AUFSICHTSBEHÖRDEN

### ABSCHNITT 1

### UNABHÄNGIGKEIT

### Artikel 46

### Aufsichtsbehörde

1. Jeder Mitgliedstaat trägt dafür Sorge, dass eine oder mehrere Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind und einen Beitrag zur ihrer einheitlichen Anwendung in der gesamten Union leisten, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer

Daten geschützt und der freie Verkehr dieser Daten in der Union erleichtert werden. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.

2. Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die als zentrale Kontaktstelle für die wirksame Beteiligung dieser Behörden im Europäischen Datenschutzausschuss fungiert und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 57 einhalten.

3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

## Artikel 47

## Unabhängigkeit

1. Die Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben und Befugnisse völlig unabhängig und unparteilich, vorbehaltlich der Vorkehrungen für Zusammenarbeit und Kohärenz gemäß Kapitel VII dieser Verordnung.

2. Die Mitglieder der Aufsichtsbehörde ersuchen in Ausübung ihres Amtes weder um Weisung noch nehmen sie Weisungen entgegen.

3. Die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres 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. Die Mitglieder der Aufsichtsbehörde verhalten sich nach Ablauf ihrer Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen ehrenhaft und zurückhaltend.

5. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde mit angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und mit der erforderlichen Infrastruktur ausgestattet wird, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.

6. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde über eigenes Personal verfügt, das vom Leiter der Aufsichtbehörde ernannt wird und seiner Leitung untersteht.

7. Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörde über einen eigenen jährlichen Haushalt verfügt. Die Haushaltspläne werden veröffentlicht.

7a. Die Mitgliedstaaten stellen jeweils sicher, dass die Aufsichtsbehörde gegenüber dem einzelstaatlichen Parlament im Rahmen der Haushaltskontrolle rechenschaftspflichtig ist.

Artikel 48

Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

1. Die Mitgliedstaaten tragen dafür Sorge, dass die Mitglieder der Aufsichtsbehörde entweder vom Parlament oder von der Regierung des betreffenden Mitgliedstaats ernannt werden.

2. Die Mitglieder werden aus einem Kreis von Personen ausgewählt, an deren Unabhängigkeit kein Zweifel besteht, und die nachweislich über die für die Erfüllung ihrer Aufgaben erforderliche Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

3. Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder seiner Enthebung aus dem Amt gemäß Absatz 4.

4. Ein Mitglied kann vom zuständigen nationalen Gericht seines Amtes enthoben oder seiner Ruhegehaltsansprüche oder an ihrer Stelle gewährten Vergünstigungen für verlustig erklärt werden, wenn es die Voraussetzungen für die Ausübung seines Amtes nicht mehr erfüllt oder eine schwere Verfehlung begangen hat.

5. Endet die Amtszeit des Mitglieds oder tritt es zurück, übt es sein Amt so lange weiter aus, bis ein neues Mitglied ernannt ist.

Artikel 49

Errichtung der Aufsichtsbehörde

Jeder Mitgliedstaat regelt durch Gesetz in den Grenzen dieser Verordnung

a) die Errichtung der Aufsichtsbehörde und ihre Stellung,

b) die Qualifikation, Erfahrung und fachliche Eignung, die für die Wahrnehmung der Aufgaben eines Mitglieds der Aufsichtsbehörde notwendig ist,

c) die Vorschriften und Verfahren für die Ernennung der Mitglieder der Aufsichtsbehörde und zur Bestimmung der Handlungen und Tätigkeiten, die mit dem Amt unvereinbar sind,

d) die Amtszeit der Mitglieder der Aufsichtsbehörde, die mindestens vier Jahre beträgt; dies gilt nicht für die erste Amtszeit nach Inkrafttreten dieser Verordnung, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;

e) ob die Mitglieder der Aufsichtsbehörde wiederernannt werden können,

f) die Regelungen und allgemeinen Bedingungen für das Amt eines Mitglieds und die Aufgaben der Bediensteten der Aufsichtsbehörde,

g) die Regeln und Verfahren für die Beendigung der Amtszeit der Mitglieder der Aufsichtsbehörde, auch für den Fall, dass sie die Voraussetzungen für die Ausübung ihres Amtes nicht mehr erfüllen oder eine schwere Verfehlung begangen haben.

Artikel 50

Verschwiegenheitspflicht

Die Mitglieder und Bediensteten der Aufsichtsbehörde sind während ihrer Amts- beziehungsweise Dienstzeit und auch nach deren Beendigung gemäß den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben bekannt geworden sind, Verschwiegenheit zu bewahren und ihre Aufgaben mit der Unabhängigkeit und Transparenz gemäß dieser Verordnung wahrzunehmen.

ABSCHNITT 2

AUFGABEN UND BEFUGNISSE

Artikel 51

Zuständigkeit

1. Jede Aufsichtsbehörde führt unbeschadet der Artikel 73 und 74 die ihr in dieser Verordnung übertragenen Aufgaben durch und übt im Hoheitsgebiet ihres Mitgliedstaats die ihr mit dieser Verordnung übertragenen Befugnisse aus. Datenverarbeitung durch Behörden wird nur durch die Aufsichtsbehörde dieses Mitgliedstaats überwacht.

2. entfällt

3. Die Aufsichtsbehörde ist nicht zuständig für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 52

Aufgaben

1. Aufgaben der Aufsichtsbehörde sind

a) die Überwachung und Gewährleistung der Anwendung dieser Verordnung,

b) die Befassung mit Beschwerden betroffener Personen oder von Verbänden gemäß Artikel 73, die Untersuchung der Angelegenheit in angemessenem Umfang und Unterrichtung der betroffenen Personen oder Verbände über den Fortgang und das Ergebnis der Beschwerde innerhalb einer angemessenen Frist, vor allem, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,

c) der Informationsaustausch mit anderen Aufsichtsbehörden und die Amtshilfe sowie die Gewährleistung der einheitlichen Anwendung und Durchsetzung dieser Verordnung,

d) die Durchführung von Untersuchungen auf eigene Initiative, aufgrund einer Beschwerde oder einer konkreten und dokumentierten Information, die unrechtmäßige Verarbeitung behauptet oder auf Ersuchen einer anderen Aufsichtsbehörde und, falls die betroffene Person eine Beschwerde bei dieser Aufsichtsbehörde eingereicht hat, deren Unterrichtung über die Ergebnisse der Untersuchungen innerhalb einer angemessenen Frist,

e) die Verfolgung relevanter Entwicklungen, soweit als sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere der Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,

f) die Beratung der Organe und Einrichtungen der Mitgliedstaaten im Hinblick auf Rechts- und Verwaltungsmaßnahmen, die den Schutz der Rechte und Freiheiten der natürlichen Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand haben,

g) die Beratung in Bezug auf die in Artikel 34 genannten Verarbeitungsvorgänge und deren Genehmigung,

h) die Abgabe von Stellungnahmen zu den Entwürfen von Verhaltensregeln gemäß Artikel 38 Absatz 2,

i) die Genehmigung verbindlicher unternehmensinterner Vorschriften gemäß Artikel 43,

j) die Mitwirkung im Europäischen Datenschutzausschuss.

ja) die für die Verarbeitung Verantwortliche und Auftragsverarbeiter gemäß Artikel 39 zu zertifizieren.

2. Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über angemessene Maßnahmen für den Schutz personenbezogener Daten. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.

2a. Jede Aufsichtsbehörde fördert gemeinsam mit den Europäischen Datenschutzausschuss das Bewusstsein der für die Verarbeitung Verantwortlichen, und der Auftragsverarbeiter über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten. Dazu gehört das Führen eines Registers der Sanktionen und Verstöße. Dieses Register sollte so detailliert wie möglich alle Warnungen und Sanktionen sowie die Lösungen der Verstöße enthalten. Jede Aufsichtsbehörde stellt kleinsten, kleinen und mittleren für die Verarbeitung Verantwortlichen und Auftragsverarbeitern auf Antrag allgemeine Information über ihre Verantwortlichkeiten und Verpflichtungen gemäß dieser Verordnung mit.

3. Die Aufsichtsbehörde berät auf Antrag jede betroffene Person bei der Wahrnehmung der ihr nach dieser Verordnung zustehenden Rechte und arbeitet zu diesem Zweck gegebenenfalls mit den Aufsichtsbehörden anderer Mitgliedstaaten zusammen.

4. Für die in Absatz 1 Buchstabe b genannten Beschwerden stellt die Aufsichtsbehörde ein Beschwerdeformular zur Verfügung, das elektronisch oder auf anderem Wege ausgefüllt werden kann.

5. Die Leistungen der Aufsichtsbehörde sind für die betroffene Person kostenlos.

6. Bei offensichtlich missbräuchlichen Anträgen, insbesondere bei wiederholt gestellten Anträgen, kann die Aufsichtsbehörde eine angemessene Gebühr verlangen oder davon absehen, die von der betroffenen Person beantragte Maßnahme zu treffen. Diese Gebühr übersteigt nicht die Kosten der beantragten Maßnahmen. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offensichtlich missbräuchlichen Charakter des Antrags.

## Artikel 53

## Befugnisse

1. Jede Aufsichtsbehörde ist im Einklang mit dieser Verordnung befugt,

a) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter auf einen behaupteten Verstoß gegen die Vorschriften zum Schutz personenbezogener Daten hinzuweisen und ihn gegebenenfalls anzuweisen, diesem Verstoß in einer bestimmten Weise abzuhelfen, um den Schutz der betroffenen Person zu verbessern, oder den für die Verarbeitung Verantwortlichen zu verpflichten, die Verletzung des Schutzes personenbezogener Daten der betroffenen Person mitzuteilen;

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

c) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben zweckdienlich sind,

d) die Befolgung der Genehmigungen und Auskünfte im Sinne von Artikel 34 sicherzustellen,

e) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter zu ermahnen oder zu verwarnen,

f) die Berichtigung, Löschung oder Vernichtung aller Daten, die unter Verletzung der Bestimmungen dieser Verordnung verarbeitet wurden, anzuordnen, und solche Maßnahmen Dritten, an die diese Daten weitergegeben wurden, mitzuteilen,

g) die Verarbeitung vorübergehend oder endgültig zu verbieten,

h) die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation zu unterbinden,

i) Stellungnahmen zu allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten abzugeben,

ia) für die Verarbeitung Verantwortliche und Auftragsverarbeiter nach Artikel 39 zu zertifizieren;

j) das nationale Parlament, die Regierung oder sonstige politische Institutionen sowie die Öffentlichkeit über Fragen im Zusammenhang mit dem Schutz personenbezogener Daten zu informieren;

ja) wirksame Vorkehrungen zu treffen, um vertrauliche Meldungen über Verletzungen der Verordnung zu fördern, wobei die Leitlinien des Europäischen Datenschutzausschusses gemäß Artikel 66 Absatz 4b berücksichtigt werden.

2. Jede Aufsichtsbehörde kann kraft ihrer Untersuchungsbefugnis vom für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter ohne Vorankündigung Folgendes verlangen:

a) Zugriff auf alle personenbezogenen Daten und auf alle Dokumente und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind,

b) Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte.

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

3. Jede Aufsichtsbehörde ist insbesondere gemäß Artikel 74 Absatz 4 und Artikel 75 Absatz 2 befugt, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Klage zu erheben.

4. Jede Aufsichtsbehörde ist befugt, Ordnungswidrigkeiten nach Artikel 79 zu ahnden. Diese Befugnis wird in einer wirksamen, verhältnismäßigen und abschreckenden Art und Weise ausgeübt.

## Artikel 54

## Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt mindestens alle zwei Jahre einen Bericht über ihre Tätigkeit. Der Bericht wird dem jeweiligen Parlament vorgelegt und der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

## Artikel 54a

## Federführende Behörde

1. Findet die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union statt, wobei der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, oder werden die personenbezogenen Daten von Einwohnern mehrerer Mitgliedstaaten verarbeitet, so fungiert die Aufsichtsbehörde der Hauptniederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters gemäß der Bestimmungen von Kapitel VII dieser Verordnung als zentrale Anlaufstelle für die Aufsicht über die Verarbeitungsvorgänge des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in allen Mitgliedstaaten.

2. Die federführende Behörde ergreift angemessene Maßnahmen für die Aufsicht über die Verarbeitungstätigkeiten des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters, für den es zuständig ist, erst nach Konsultation aller anderen zuständigen Aufsichtsbehörden im Sinne von Artikel 51 Absatz 1 und bemüht sich dabei, einen Konsens zu erreichen. Zu diesem Zweck leitet sie insbesondere alle maßgeblichen Informationen weiter und konsultiert die anderen Behörden, bevor sie Maßnahmen, die im Sinne von Artikel 51 Absatz 1 Rechtswirkungen in Bezug auf die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter entfalten sollen, ergreift. Die federführende Behörde schenkt den Stellungnahmen der beteiligten Behörden größtmögliche Beachtung. Die federführende Behörde ist die einzige Behörde, die befugt ist, Maßnahmen, die Rechtswirkungen in Bezug auf die Verarbeitungstätigkeiten der für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, für die sie zuständig ist, entfalten sollen, ergreift.

3. Der Europäische Datenschutzausschuss gibt auf Antrag einer zuständigen Aufsichtsbehörde eine Stellungnahme zu der Feststellung der federführenden Behörde, die für einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter zuständig ist, ab, wenn

a) aus dem Sachverhalt nicht hervorgeht, wo sich der Hauptsitz des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befindet, oder

b) sich die zuständigen Behörden nicht darauf einigen können, welche Behörde als federführende Behörde fungieren soll; oder

c) der für die Verarbeitung Verantwortliche nicht in der Union niedergelassen ist, und in unterschiedlichen Mitgliedstaaten ansässige Personen von den Verarbeitungsoperationen im Rahmen dieser Verordnung betroffen sind.

3a. Wird der für die Verarbeitung Verantwortliche auch als Auftragsverarbeiter tätig, so fungiert die Aufsichtsbehörde der Hauptniederlassung des für die Verarbeitung Verantwortlichen als federführende Behörde für die Aufsicht über die Verarbeitungstätigkeiten.

4. Der Europäische Datenschutzausschuss kann die federführende Behörde bestimmen.

## KAPITEL VII

## ZUSAMMENARBEIT UND KOHÄRENZ

ABSCHNITT 1

ZUSAMMENARBEIT

Artikel 55

Amtshilfe

1. Die Aufsichtsbehörden übermitteln einander zweckdienliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Konsultation, die Vornahme von Nachprüfungen und Untersuchungen sowie die zügige Unterrichtung über die Befassung mit einer Angelegenheit und über weitere Entwicklungen in Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über Niederlassungen in mehreren Mitgliedstaaten verfügt oder in denen Personen in mehreren Mitgliedstaaten voraussichtlich von Verarbeitungsvorgängen betroffen sind. Die federführende Behörde gemäß Artikel 54a stellt die Abstimmung mit den beteiligten Aufsichtsbehörden sicher und fungiert als zentrale Kontaktstelle für den für die Verarbeitung Verantwortlichen bzw. den Auftragsverarbeiter.

2. Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu können insbesondere auch die Übermittlung zweckdienlicher Informationen über den Verlauf einer Untersuchung oder Durchsetzungsmaßnahmen gehören, um die Einstellung oder das Verbot von Verarbeitungsvorgängen zu erwirken, die gegen diese Verordnung verstoßen.

3. Das Amtshilfeersuchen enthält alle erforderlichen Informationen, darunter Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für die Angelegenheit verwendet, für die sie angefordert wurden.

4. Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn

a) sie für das Ersuchen nicht zuständig ist oder

b) das Ersuchen gegen die Bestimmungen dieser Verordnung verstoßen würde.

5. Die Aufsichtsbehörde, an die das Ersuchen gerichtet wurde, informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen.

6. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, auf elektronischem Wege und so schnell wie möglich unter Verwendung eines standardisierten Formats.

7. Maßnahmen, die aufgrund eines Amtshilfeersuchens getroffen werden, sind für die ersuchende Aufsichtsbehörde gebührenfrei.

8. Wird eine ersuchte Aufsichtsbehörde nicht binnen eines Monats auf das Amtshilfeersuchen einer anderen Aufsichtsbehörde hin tätig, so ist die ersuchende Aufsichtsbehörde befugt, einstweilige Maßnahmen im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen und die Angelegenheit dem Europäischen Datenschutzausschuss gemäß dem Verfahren von Artikel 57 vorzulegen. Die ersuchende Aufsichtsbehörde kann einstweilige Maßnahmen nach Artikel 53 im Hoheitsgebiet ihres Mitgliedstaats ergreifen, wenn aufgrund der noch nicht abgeschlossenen Hilfeleistung eine endgültige Maßnahme noch nicht getroffen werden kann.

9. Die Aufsichtsbehörde legt fest, wie lange diese einstweilige Maßnahme gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission von diesen Maßnahmen unverzüglich unter Angabe aller Gründe gemäß dem in Artikel 57 vorgesehenen Verfahren in Kenntnis.

10. Der Europäische Datenschutzausschuss kann Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere das in Absatz 6 genannte standardisierte Format, festlegen.

## Artikel 56

## Gemeinsame Maßnahmen der Aufsichtsbehörden

1. Zur Stärkung der Zusammenarbeit und Amtshilfe erfüllen die Aufsichtsbehörden gemeinsame untersuchungsspezifische Aufgaben, führen gemeinsame Durchsetzungsmaßnahmen und andere gemeinsame Maßnahmen durch, an denen benannte Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.

2. In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über Niederlassungen in mehreren Mitgliedstaaten verfügt oder in denen voraussichtlich Personen in mehreren Mitgliedstaaten von Verarbeitungsvorgängen betroffen sind, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, an den gemeinsamen untersuchungsspezifischen Aufgaben oder den gemeinsamen Maßnahmen teilzunehmen. Die federführende Aufsichtsbehörde gemäß Artikel 54a bezieht die Aufsichtsbehörde jedes dieser Mitgliedstaaten in die betreffenden gemeinsamen untersuchungsspezifischen Aufgaben oder gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme. Die federführende Aufsichtsbehörde fungiert als zentrale Kontaktstelle für den für die Verarbeitung Verantwortlichen bzw. den Auftragsverarbeiter.

3. Jede Aufsichtsbehörde kann als einladende Aufsichtsbehörde gemäß ihren nationalen Rechtsvorschriften und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder

Bediensteten der unterstützenden Aufsichtsbehörde Durchführungsbefugnisse einschließlich untersuchungsspezifischer Aufgaben übertragen oder, soweit dies nach dem Recht der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Durchführungsbefugnisse nach dem Recht der unterstützenden Aufsichtsbehörde auszuüben. Diese Durchführungsbefugnisse können nur unter der Leitung und in der Regel in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem nationalen Recht der einladenden Aufsichtsbehörde. Die einladende Aufsichtsbehörde haftet für ihre Handlungen.

4. Die Aufsichtsbehörden regeln die praktischen Aspekte spezifischer Kooperationsmaßnahmen.

5. Kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 nach, so sind die anderen Aufsichtsbehörden befugt, eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 zu ergreifen.

6. Die Aufsichtsbehörde legt fest, wie lange die einstweilige Maßnahme nach Absatz 5 gültig ist. Dieser Zeitraum darf drei Monate nicht überschreiten. Die Aufsichtsbehörde teilt dem Europäischen Datenschutzausschuss und der Kommission diese Maßnahmen unverzüglich unter Angabe aller Gründe mit und nimmt für diese Sache das in Artikel 57 genannte Verfahren in Anspruch.

## ABSCHNITT 2

## KOHÄRENZ

### Artikel 57

### Kohärenzverfahren

Zu den in Artikel 46 Absatz 1 genannten Zwecken arbeiten die Aufsichtsbehörden sowohl in allgemeinen Fragen als auch in Einzelfällen gemäß den Vorschriften des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und mit der Kommission zusammen.

### Artikel 58

### Kohärenz in Angelegenheiten mit allgemeiner Geltung

1. Bevor eine Aufsichtsbehörde eine Maßnahme nach Absatz 2 erlässt, übermittelt sie die geplante Maßnahme dem Europäischen Datenschutzausschuss und der Kommission.

2. Die in Absatz 1 genannte Verpflichtung gilt für Maßnahmen, die Rechtswirkung entfalten sollen und

a) entfällt

b) entfällt

c) entfällt

d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dienen oder

e) der Genehmigung von Vertragsklauseln gemäß Artikel 42 Absatz 2 Buchstabe d dienen oder

f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dienen.

3. Jede Aufsichtsbehörde und der Europäische Datenschutzausschuss können beantragen, dass eine Angelegenheit mit allgemeiner Geltung im Rahmen des Kohärenzverfahrens behandelt wird, insbesondere, wenn eine Aufsichtsbehörde die in Absatz 2 genannte geplante Maßnahme nicht vorlegt oder den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht nachkommt.

4. Um die ordnungsgemäße und kohärente Anwendung dieser Verordnung sicherzustellen, kann die Kommission beantragen, dass eine Angelegenheit mit allgemeiner Geltung im Rahmen des Kohärenzverfahrens behandelt wird.

5. Die Aufsichtsbehörden und die Kommission übermitteln unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme und die Gründe, warum eine solche Maßnahme ergriffen werden muss.

6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats die Mitglieder des Datenschutzausschusses und die Kommission über zweckdienliche Informationen, die ihm zugegangen sind. Soweit erforderlich stellt das Sekretariat des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung.

6a. Der Europäische Datenschutzausschuss gibt eine Stellungnahme zu Angelegenheiten, mit denen er gemäß Absatz 2 befasst wird, ab.

7. Der Europäische Datenschutzausschuss kann mit einfacher Mehrheit entscheiden, ob er eine Stellungnahme zu einer gemäß Absatze 3 und 4 vorgelegten Angelegenheit abgibt, wobei zu berücksichtigen ist,

a) ob die Angelegenheit neue Elemente umfasst, wobei rechtliche oder sachliche Entwicklungen berücksichtigt werden, insbesondere in der Informationstechnologie und in Anbetracht des Fortschritts in der Informationsgesellschaft; und

b) ob der Europäische Datenschutzausschuss bereits eine Stellungnahme zu der gleichen Angelegenheit abgegeben hat.

8. Der Europäische Datenschutzausschuss nimmt Stellungnahmen gemäß Artikel 6a und 7 mit der einfachen Mehrheit seiner Mitglieder an. Diese Stellungnahmen werden veröffentlicht.

Artikel 58a

Kohärenz in Einzelfällen

1. Vor dem Ergreifen von Maßnahmen, die im Sinne von Artikel 54a Rechtswirkung entfalten sollen, teilt die federführende Behörde alle zweckdienlichen Informationen und legt den Entwurf der Maßnahme allen anderen zuständigen Behörden vor. Die federführende Behörde darf keine Maßnahme ergreifen, wenn eine zuständige Behörde innerhalb von drei Wochen ernsthafte Einwände gegen die Maßnahme anzeigt.

2. Hat eine zuständige Behörde ernsthafte Einwände gegen den Entwurf einer Maßnahme der federführenden Behörde angezeigt oder hat die federführende Behörde keinen Entwurf einer Maßnahme gemäß Absatz 1 vorlegt oder kommt sie den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht nach, wird die Angelegenheit vom Europäischen Datenschutzausschuss geprüft.

3. Die federführende Behörde und/oder andere beteiligte zuständige Behörden und die Kommission übermitteln dem Europäischen Datenschutzausschuss unverzüglich auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme, die Gründe, warum eine solche Maßnahme ergriffen werden muss, die Einwände gegen sie und die Auffassung anderer betroffener Aufsichtsbehörden.

4. Der Europäische Datenschutzausschuss prüft die Angelegenheit, wobei die Auswirkungen der geplanten Maßnahme auf die Grundrechte und Freiheiten der betroffenen Personen berücksichtigt werden, und entscheidet mit der einfachen Mehrheit seiner Mitglieder, ob eine Stellungnahme zu der Angelegenheit innerhalb von zwei Wochen nach Eingang der zweckdienlichen Informationen nach Absatz 3 abgegeben wird.

5. Entscheidet der Europäische Datenschutzausschuss, eine Stellungnahme abzugeben, wird diese innerhalb von sechs Wochen abgegeben und veröffentlicht.

6. Die federführende Behörde trägt der Stellungnahme des Europäischen Datenschutzausschusses größtmögliche Rechnung und teilt dessen Vorsitz und der Kommission binnen zwei Wochen nach ihrer Unterrichtung über die Stellungnahme durch den Vorsitz des Europäischen Datenschutzausschusses elektronisch mit, ob sie die geplante Maßnahme beibehält oder ändert; gegebenenfalls übermittelt unter Verwendung eines standardisierten Formats die geänderte geplante Maßnahme. Wenn die federführende Behörde beabsichtigt, der Stellungnahme des Europäischen Datenschutzausschusses nicht Folge zu leisten, begründet sie dies.

7. In Fällen, in denen der Europäische Datenschutzausschuss nach wie vor Einwände gegen die Maßnahme der Aufsichtsbehörde gemäß Absatz 5 erhebt, kann

er innerhalb eines Monats mit Zweidrittelmehrheit eine Maßnahme beschließen, die für die Aufsichtsbehörde bindend ist.

## Artikel 59

## Stellungnahme der Kommission

entfällt

## Artikel 60

## Aussetzung einer geplanten Maßnahme

entfällt

## Artikel 60a

## Unterrichtung des Europäischen Parlaments und des Rats

Die Kommission unterrichtet das Europäische Parlament und den Rat regelmäßig, mindestens halbjährlich auf Grundlage eines Berichts des Vorsitzes des Europäischen Datenschutzausschusses über die im Rahmen des Kohärenzmechanismus behandelten Angelegenheiten und zeigt dabei die von Kommission und Europäischen Datenschutzausschuss gezogenen Schlussfolgerungen zur Gewährleistung der einheitlichen Durchführung und Anwendung dieser Verordnung auf.

## Artikel 61

## Dringlichkeitsverfahren

1. Unter außergewöhnlichen Umständen kann eine Aufsichtsbehörde abweichend vom Verfahren nach Artikel 58a sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer treffen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um die Interessen von betroffenen Personen, vor allem, wenn die Durchsetzung ihrer Rechte durch eine Veränderung der bestehenden Lage erheblich behindert zu werden droht, zu schützen, um größere Nachteile abzuwenden oder aus anderen Gründen. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission unverzüglich unter Angabe aller Gründe von diesen Maßnahmen in Kenntnis.

2. Hat eine Aufsichtsbehörde eine Maßnahme nach Absatz 1 ergriffen und ist sie der Auffassung, dass dringend endgültige Maßnahmen erlassen werden müssen, kann sie unter Angabe von Gründen, auch für die Dringlichkeit der endgültigen Maßnahmen, im Dringlichkeitsverfahren um eine Stellungnahme des Europäischen Datenschutzausschusses ersuchen.

3. Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme ersuchen, wenn die zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs

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

4. Die Stellungnahme im Dringlichkeitsverfahren nach den Absätzen 2 und 3 wird binnen zwei Wochen durch einfache Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen.

Artikel 62

Durchführungsrechtsakte

1. Die Kommission kann, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat, zu folgenden Zwecken Durchführungsrechtsakte mit allgemeiner Geltung erlassen:

a) entfällt

b) Beschluss darüber, ob Standard-Datenschutzklauseln nach Artikel 42 Absatz 2 Buchstabe d allgemeine Gültigkeit zuerkannt wird,

c) entfällt

d) entfällt

2. entfällt

3. Unabhängig davon, ob die Kommission eine Maßnahme nach Maßgabe dieses Abschnitts erlassen hat, kann sie auf der Grundlage der Verträge andere Maßnahmen erlassen.

Artikel 63 D

urchsetzung

1. Für die Zwecke dieser Verordnung wird eine durchsetzbare Maßnahme der Aufsichtsbehörde eines Mitgliedstaats in allen anderen betroffenen Mitgliedstaaten durchgesetzt.

2. Nimmt eine Aufsichtsbehörde für eine geplante Maßnahme entgegen Artikel 58 Absätze 1 und 2 nicht das Kohärenzverfahren in Anspruch oder nimmt sie eine Maßnahme trotz der Anzeige von ernsthafte n Einwänden gemäß Artikel 58a Absatz 1 an, so ist die Maßnahme der Aufsichtsbehörde nicht rechtsgültig und durchsetzbar.

ABSCHNITT 3

EUROPÄISCHER DATENSCHUTZAUSSCHUSS

Artikel 64

Europäischer Datenschutzausschuss

1. Hiermit wird ein Europäischer Datenschutzausschuss eingerichtet.

2. Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten.

3. Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Richtlinie erlassenen Vorschriften zuständig, so wird der Leiter einer diese Aufsichtsbehörden zum gemeinsamen Vertreter ernannt.

4. Die Kommission ist berechtigt, an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen und bestimmt einen Vertreter. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die Kommission unverzüglich von allen Tätigkeiten des Europäischen Datenschutzausschusses.

## Artikel 65

## Unabhängigkeit

1. Der Europäische Datenschutzausschuss handelt bei der Erfüllung seiner Aufgaben gemäß den Artikeln 66 und 67 unabhängig.

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

## Artikel 66

## Aufgaben des Europäischen Datenschutzausschusses

1. Der Europäische Datenschutzausschuss stellt sicher, dass diese Verordnung einheitlich angewandt wird. Zu diesem Zweck geht der Europäische Datenschutzausschuss von sich aus oder auf Ersuchen des Europäischen Parlaments, des Rates oder der Kommission insbesondere folgenden Tätigkeiten nach:

a) Beratung der europäischen Organe in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, darunter auch etwaige Vorschläge zur Änderung dieser Verordnung;

b) von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen des Europäischen Parlaments, des Rates oder der Kommission vorgenommene Prüfung von die Anwendung dieser Verordnung betreffenden Fragen und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Praktiken für die Aufsichtsbehörden zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung, einschließlich der Ausübung von Durchsetzungsbefugnissen;

c) Überprüfung der praktischen Anwendung der unter Buchstabe b genannten Leitlinien, Empfehlungen und bewährten Praktiken und regelmäßige Berichterstattung über diese an die Kommission;

d) Abgabe von Stellungnahmen zu Beschlussentwürfen von Aufsichtsbehörden gemäß dem in Artikel 57 genannten Kohärenzverfahren;

da) Abgabe eine Stellungnahme darüber, welche Behörde die federführende Behörde gemäß Artikel 54a Absatz 3 sein sollte;

e) Förderung der Zusammenarbeit und eines effizienten bilateralen und multilateralen Austausches von Informationen und Praktiken zwischen den Aufsichtsbehörden, einschließlich der Koordinierung gemeinsamer Operationen und anderer gemeinsamer Aktivitäten, wenn der Ausschuss auf Ersuchen einer oder mehrerer Aufsichtsbehörden eine entsprechende Entscheidung trifft;

f) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit Aufsichtsstellen internationaler Organisationen;

g) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und –praktiken mit Datenschutzaufsichtsbehörden in aller Welt.

ga) Abgabe seiner Stellungnahme für die Kommission bei der Vorbereitung von delegierten Rechtsakten und Durchführungsrechtsakten auf der Grundlage dieser Verordnung;

gb) Abgabe seiner Stellungnahme zu den auf Unionsebene erarbeiteten Verhaltensregeln gemäß Artikel 38 Absatz 4;

gc) Abgabe seiner Stellungnahme zu den Kriterien und Anforderungen für das datenschutzspezifische Zertifizierungsverfahren gemäß Artikel 39 Absatz 3.

gd) Pflege eines öffentlichen elektronischen Registers über gültige und ungültige Zertifikate gemäß Artikel 39 Absatz 1h.

ge) nachentsprechendem Antrag Unterstützung der einzelstaatlichen Aufsichtsbehörden;

gf) Erstellen und Veröffentlichung einer Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Konsultation nach Artikel 34 sind;

gg) Pflege eines Registers über Sanktionen, die von den zuständigen Aufsichtsbehörden gegen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängt wurden.

2. Das Europäische Parlament, der Rat oder die Kommission können, wenn sie den Europäischen Datenschutzausschuss um Rat ersuchen, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist setzen.

3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken an das Europäische Parlament, den Rat und die Kommission sowie an den in Artikel 87 genannten Ausschuss weiter und veröffentlicht sie.

4. Die Kommission setzt den Europäischen Datenschutzausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die vom Europäischen Datenschutzausschuss herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken ergriffen hat.

4a. Der Europäische Datenschutzausschuss konsultiert gegebenenfalls interessierte Kreise und gibt ihnen Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Unbeschadet des Artikels 72 macht der Datenschutzausschuss die Ergebnisse des Anhörungsverfahrens der Öffentlichkeit zugänglich.

4b. Der Europäische Datenschutzausschuss wird beauftragt, Leitlinien, Empfehlungen und bewährte Praktiken nach Maßgabe von Absatz 1 Buchstabe b in Bezug auf die Festlegung gemeinsamer Verfahren zu veröffentlichen, um gemeinsame Verfahren für den Erhalt und die Untersuchung von Informationen über die mutmaßliche rechtswidrige Verarbeitung sowie die Sicherung der Vertraulichkeit von Informationen und den Schutz der Quellen von Informationen; festzulegen.

## Artikel 67

## Berichterstattung

1. Der Europäische Datenschutzausschuss informiert das Europäische Parlament, den Rat und die Kommission regelmäßig und zeitnah über die Ergebnisse seiner Tätigkeiten. Er erstellt mindestens alle zwei Jahre einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union und in Drittländern.

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

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

## Artikel 68

## Verfahrensweise

1. Der Europäische Datenschutzausschuss trifft seine Beschlüsse mit der einfachen Mehrheit seiner Mitglieder, sofern in seiner Geschäftsordnung nichts anderes vorgesehen ist.

2. Der Europäische Datenschutzausschuss gibt sich eine Geschäftsordnung und legt seine Arbeitsweise fest. Er sieht insbesondere vor, dass bei Ablauf der Amtszeit oder Rücktritt eines seiner Mitglieder die Aufgaben kontinuierlich weitererfüllt werden, dass für spezifische Fragen oder Sektoren Untergruppen

eingesetzt werden, und dass seine Verfahrensvorschriften im Einklang mit dem in Artikel 57 genannten Kohärenzverfahren stehen.

Artikel 69

Vorsitz

1. Der Europäische Datenschutzausschuss wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und mindestens zwei stellvertretende Vorsitzende.

2. Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre Wiederwahl ist zulässig.

2a. Die Stelle des Vorsitzes ist eine Vollzeitstelle.

Artikel 70

Aufgaben des Vorsitzenden

1. Der Vorsitzende hat folgende Aufgaben:

a) Einberufung der Sitzungen des Europäischen Datenschutzausschusses und Erstellung der Tagesordnungen;

b) Sicherstellung einer rechtzeitigen Erfüllung der Aufgaben des Europäischen Datenschutzausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 57.

2. Der Europäische Datenschutzausschuss legt die Verteilung der Aufgaben auf den Vorsitzenden und dessen zwei Stellvertreter in seiner Geschäftsordnung fest.

Artikel 71

Sekretariat

1. Der Europäische Datenschutzausschuss erhält ein Sekretariat. Dieses wird vom Europäischen Datenschutzbeauftragten gestellt.

2. Das Sekretariat leistet dem Europäischen Datenschutzausschuss unter Leitung von dessen Vorsitzendem rechtliche, analytische, administrative und logistische Unterstützung.

3. Das Sekretariat ist insbesondere verantwortlich für

a) das Tagesgeschäft des Europäischen Datenschutzausschusses;

b) die Kommunikation zwischen den Mitgliedern des Europäischen Datenschutzausschusses, seinem Vorsitz und der Kommission sowie die Kommunikation mit anderen Organen und mit der Öffentlichkeit;

c) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation;

d) die Übersetzung sachdienlicher Informationen;

e) die Vor- und Nachbereitung der Sitzungen des Europäischen Datenschutzausschusses;

f) Vorbereitung, Entwurf und Veröffentlichung von Stellungnahmen und sonstigen vom Europäischen Datenschutzausschuss angenommenen Dokumenten.

Artikel 72 Vertraulichkeit

1. Die Beratungen des Europäischen Datenschutzausschusses können, soweit notwendig, vertraulich sein, falls in der Geschäftsordnung nichts anderes vorgesehen ist. Die Tagesordnungen der Sitzungen des Europäischen Datenschutzausschusses werden öffentlich zugänglich gemacht.

2. Den Mitgliedern des Europäischen Datenschutzausschusses, Sachverständigen und den Vertretern von Dritten vorgelegte Dokumente sind vertraulich, sofern sie nicht gemäß der Verordnung (EG) Nr. 1049/2001 offengelegt oder auf andere Weise vom Europäischen Datenschutzausschuss der Öffentlichkeit zugänglich gemacht werden.

3. Die Mitglieder des Europäischen Datenschutzausschusses, die Sachverständigen und die Vertreter von Dritten beachten die Verpflichtung zur Wahrung der Vertraulichkeit gemäß diesem Artikel. Der Vorsitzende stellt sicher, dass die Sachverständigen und die Vertreter von Dritten von der ihnen auferlegten Vertraulichkeitspflicht in Kenntnis gesetzt werden.

## KAPITEL VIII

## RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

### Artikel 73

### Recht auf Beschwerde bei einer Aufsichtsbehörde

1. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs und des Kohärenzverfahrens das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.

2. Einrichtungen, Organisationen oder Verbände, die im öffentlichen Interesse handeln und die nach dem Recht eines Mitgliedstaats gegründet sind, haben das Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte infolge der Verarbeitung personenbezogener Daten verletzt wurden.

3. Unabhängig von der Beschwerde einer betroffenen Person haben Einrichtungen, Organisationen oder Verbände im Sinne des Absatzes 2 das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht sind, dass diese Verordnung verletzt wurde.

## Artikel 74

### Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

1. Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen administrativen oder außergerichtlichen Rechtsbehelfs das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde.

2. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder außergerichtlichen Rechtsbehelfs das Recht auf einen gerichtlichen Rechtsbehelf, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden, wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist oder wenn die Aufsichtsbehörde sie nicht gemäß Artikel 52 Absatz 1 Buchstabe b innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

3. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

4. Eine betroffene Person, die von einer Entscheidung einer Aufsichtsbehörde betroffen ist, die ihren Sitz in einem anderen Mitgliedstaat hat als dem, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, kann unbeschadet des Kohärenzverfahrens die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen, in ihrem Namen gegen die zuständige Aufsichtsbehörde in dem anderen Mitgliedstaat Klage zu erheben.

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

## Artikel 75

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

1. Jede natürliche Person hat unbeschadet eines verfügbaren administrativen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 73 das Recht auf einen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats

erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde der Union oder eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

3. Ist dieselbe Maßnahme, Entscheidung oder Vorgehensweise Gegenstand des Kohärenzverfahrens gemäß Artikel 58, kann das Gericht das Verfahren, mit dem es befasst wurde, aussetzen, es sei denn, es ist aufgrund der Dringlichkeit des Schutzes der Rechte der betroffenen Person nicht möglich, den Ausgang des Kohärenzverfahrens abzuwarten.

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

## Artikel 76

## Gemeinsame Vorschriften für Gerichtsverfahren

1. Einrichtungen, Organisationen oder Verbände im Sinne des Artikels 73 Absatz 2 haben das Recht, die in Artikel 74, 75 und 77 genannten Rechte wahrzunehmen, wenn sie von einer oder mehreren betroffenen Personen beauftragt werden.

2. Jede Aufsichtsbehörde hat das Recht, Klage zu erheben, um die Bestimmungen dieser Verordnung durchzusetzen oder um einen einheitlichen Schutz der personenbezogenen Daten innerhalb der Union sicherzustellen.

3. Hat ein zuständiges mitgliedstaatliches Gericht Grund zu der Annahme, dass in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist, setzt es sich mit dem zuständigen Gericht in diesem anderen Mitgliedstaat in Verbindung, um sich zu vergewissern, ob ein solches Parallelverfahren besteht.

4. Betrifft das Parallelverfahren in dem anderen Mitgliedstaat dieselbe Maßnahme, Entscheidung oder Vorgehensweise, kann das Gericht sein Verfahren aussetzen.

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

## Artikel 77

## Haftung und Recht auf Schadenersatz

1. Jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit dieser Verordnung nicht zu vereinbarenden Handlung ein Schaden, auch immaterieller Schaden, entstanden ist, hat das Recht, von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter Schadensersatz zu verlangen.

2. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter gesamtschuldnerisch für den gesamten Schaden, sofern nicht eine geeignete schriftliche Vereinbarung gemäß Artikel 24 zwischen ihnen existiert, die die Verantwortlichkeiten festlegt.

3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.

Artikel 78

Sanktionen

1. Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen diese Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen; dies gilt auch für den Fall, dass der für die Verarbeitung Verantwortliche seiner Pflicht zur Benennung eines Vertreters nicht nachgekommen ist. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

2. Hat der für die Verarbeitung Verantwortliche einen Vertreter benannt, wirken die Sanktionen gegen den Vertreter unbeschadet etwaiger Sanktionen, die gegen den für die Verarbeitung Verantwortlichen verhängt werden könnten.

3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

Artikel 79

Verwaltungsrechtliche Sanktionen

1. Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen. Die Aufsichtsbehörden arbeiten gemäß Artikel 46 und 57 zusammen, um ein harmonisiertes Niveau der Sanktionen innerhalb der Union zu gewährleisten.

2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.

2a. Die Aufsichtsbehörde verhängt gegen jeden, der seinen in dieser Verordnung festgelegten Pflichten nicht nachkommt, mindestens eine der folgenden Sanktionen:

a) eine schriftliche Verwarnung im Fall eines ersten und nicht vorsätzlichen Verstoßes;

b) regelmäßige Überprüfungen betreffend den Datenschutz;

c) eine Geldbuße, bis zu 100 000 000 EUR oder im Fall eines Unternehmens bis zu 5 % seines weltweiten Jahresumsatzes, je nachdem, welcher der Beträge höher ist.

2b. Ist der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter im Besitz eines europäischen Datenschutzsiegels gemäß Artikel 39, so wird nur bei Vorsatz oder Fahrlässigkeit eine Geldbuße nach Absatz 2a Buchstabe c verhängt.

2c. Bei Verhängung einer Ordnungsstrafe werden folgende Faktoren berücksichtigt:

a) die Art, Schwere und Dauer des Verstoßes;

b) der vorsätzliche oder fahrlässige Charakter des Verstoßes,

c) der Grad der Verantwortung der natürlichen oder juristischen Person und frühere Verstöße dieser Person,

d) der Wiederholungscharakter des Verstoßes,

e) der Umfang der Zusammenarbeit mit der Aufsichtsbehörde zur Wiedergutmachung des Verstoßes und zur Minderung seiner möglichen negativen Auswirkungen,

f) die spezifischen Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind,

g) der Umfang des Schadens, auch des immateriellen Schadens, für die betroffenen Personen,

h) die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

i) direkt oder indirekt aus dem Verstoß entstandene beabsichtigte oder erlangte finanzielle Vorteile oder vermiedene Verluste,

j) die technischen und organisatorischen Maßnahmen und Verfahren gemäß

- i) Artikel 23 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen);
- ii) Artikel 30 (Sicherheit der Verarbeitung);
- iii) Artikel 33 (Datenschutz-Folgenabschätzung);
- iv) Artikel 33a (Überprüfung der Einhaltung der Datenschutzbestimmungen);
- v) Artikel 35 (Benennung eines Datenschutzbeauftragten);

k) die Weigerung, mit der Aufsichtsbehörde zusammen zu arbeiten oder die Behinderung von ihr gemäß Artikel 53 durchgeführter Nachprüfungen, Überprüfungen und Kontrollen,

l) jegliche anderen erschwerenden oder mildernden Umstände im Einzelfall.

3. entfällt

4. entfällt

5. entfällt

6. entfällt

7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die absoluten Beträge der in Absatz 2a genannten Geldbußen unter Berücksichtigung der in den Absätzen 2 und 2c aufgeführten Kriterien und Umstände zu aktualisieren.

## KAPITEL IX

## VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN

### Artikel 80

### Verarbeitung personenbezogener Daten und freie Meinungsäußerung

1. Die Mitgliedstaaten sehen, wann immer dies notwendig ist, Abweichungen oder Ausnahmen von den allgemeinen Grundsätzen des Kapitels II, von den Rechten der betroffenen Person in Kapitel III, von den Bestimmungen über den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter in Kapitel IV, von der Übermittlung personenbezogener Daten in Drittländer und an internationale Organisationen in Kapitel V, von den Vorschriften über die Aufsichtsbehörden in Kapitel VI, von den Vorschriften über Zusammenarbeit und Kohärenz in Kapitel VII sowie von den Vorschriften über besondere Datenverarbeitungssituationen in Kapitel IX vor, um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften nach Maßgabe der Charta der Grundrechte der Europäischen Union in Einklang zu bringen.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlassen hat, und setzt sie unverzüglich von allen weiteren Änderungsgesetzen oder diese Rechtsvorschriften betreffenden Änderungen in Kenntnis.

### Artikel 80a

### Zugang zu Dokumenten

1. Personenbezogene Daten in Dokumenten einer Behörde oder einer öffentlichen Einrichtung können von dieser Behörde oder Einrichtung gemäß unionsrechtlichen oder mitgliedstaatlichen Vorschriften über den Zugang der Öffentlichkeit zu amtlichen Dokumenten offen gelegt werden, die das Recht auf den Schutz personenbezogener Daten mit dem Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten in Einklang bringen.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1

erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

## Artikel 81

## Verarbeitung personenbezogener Gesundheitsdaten

1. Die Verarbeitung personenbezogener Gesundheitsdaten erfolgt in Übereinstimmung mit den Bestimmungen dieser Verordnung und insbesondere mit Artikel 9 Absatz 2 Buchstabe h auf der Grundlage des Unionsrechts oder des mitgliedstaatlichen Rechts, das geeignete, einheitliche und besondere Maßnahmen zum Schutz der Interessen und der Grundrechte der betroffenen Person vorsieht; sofern diese notwendig und verhältnismäßig sind und dessen Auswirkungen für die betroffene Person vorhersehbar sein müssen:

a) für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten, sofern die Verarbeitung dieser Daten durch dem Berufsgeheimnis unterliegendes ärztliches Personal erfolgt oder durch sonstige Personen, die nach mitgliedstaatlichem Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, einer entsprechenden Geheimhaltungspflicht unterliegen;

b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit unter anderem zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards unter anderem für Arzneimittel oder Medizinprodukte und wenn die Verarbeitung dieser Daten durch eine Person erfolgt, die der Verschwiegenheitspflicht unterliegt; oder

c) aus anderen Gründen des öffentlichen Interesses in Bereichen wie der sozialen Sicherheit, insbesondere um die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen und die Bereitstellung von Gesundheitsleistungen sicherzustellen. Diese Verarbeitung personenbezogener Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass personenbezogene Daten zu anderen Zwecken verarbeitet werden, es sei denn, die betroffene Person stimmt ihr zu oder die Verarbeitung erfolgt auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats.

1a. Wenn die Zwecke gemäß Absatz 1 Buchstabe a bis c ohne die Verwendung personenbezogener Daten erreicht werden können, werden solche Daten für diese Zwecke nicht verarbeitet, es sei denn, die betroffene Person stimmt ihr zu oder die Verarbeitung erfolgt auf der Grundlage des Rechts eines Mitgliedstaats.

1b. In Fällen, in denen die Einwilligung der betroffenen Person zur Verarbeitung medizinischer Daten für den ausschließlichen Zwecke der Forschung zu Fragen der öffentlichen Gesundheit erforderlich ist, kann die Einwilligung für eine oder mehrere spezifische und ähnliche Forschungen gegeben werden. Die betroffene Person kann ihre Einwilligung jedoch jederzeit zu widerrufen.

1c. Für die Einwilligung in die Teilnahme an wissenschaftlicher Forschung im Zusammenhang mit klinischen Studien finden die einschlägigen Vorschriften der Richtlinie 2001/20/EG des Europäischen Parlaments und des Rates[1] Anwendung.

2. Die Verarbeitung personenbezogener Gesundheitsdaten, die zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung erforderlich ist, ist nur mit Einwilligung der betroffenen Person erlaubt und unterliegt den Bedingungen und Garantien gemäß Artikel 83.

2a. Im Hinblick auf Forschung, die einem großen öffentlichen Interesse dient, können in den Rechtsvorschriften der Mitgliedstaaten Ausnahmen von dem Erfordernis der Einwilligung im Bereich der Forschung gemäß Absatz 2 vorgesehen werden, wenn es unmöglich ist, diese Forschung auf andere Weise durchzuführen. Die betreffenden Daten sind zu anonymisieren, oder, falls dies für die Zwecke der Forschung nicht möglich ist, gemäß den höchsten technischen Standards zu pseudonymisieren, und es sind sämtliche notwendigen Maßnahmen zu ergreifen, um unbefugte Rückschlüsse auf die Identität der betroffenen Personen zu verhindern. Die betroffene Person hat jedoch das Recht, ihre Einwilligung jederzeit gemäß Artikel 19 zu widerrufen.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat, um die Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit im Sinne des Absatzes 1 Buchstabe b und des großen öffentlichen Interesse im Bereich der Forschung im Sinne des Absatzes 2a näher auszuführen.

## Artikel 82

## Mindestnormen für die Datenverarbeitung im Beschäftigungskontext

1. Die Mitgliedstaaten können im Einklang mit den Regelungen dieser Verordnung und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit durch Rechtsvorschriften die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext, insbesondere, jedoch nicht ausschließlich, für Zwecke der Einstellung und Bewerbung innerhalb des Unternehmensgruppe, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich und tarifvertraglich festgelegten Pflichten gemäß nationalen Rechtsvorschriften oder Gepflogenheiten, des Managements, der Planung und der Organisation der Arbeit, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses regeln. Die Mitgliedstaaten können Kollektivverträge für die weitere Konkretisierung der Vorschriften dieses Artikels vorsehen.

1a. Der Zweck der Verarbeitung solcher Daten muss mit dem Grund, aus dem die Daten erhoben wurden, in Zusammenhang stehen und auf den Beschäftigungskontext beschränkt bleiben. Die Profilerstellung oder Verwendung für sekundäre Zwecke ist nicht statthaft.

1b. Die Einwilligung eines Arbeitnehmers bietet keine Rechtsgrundlage für die Verarbeitung von Daten durch den Arbeitgeber, wenn die Einwilligung nicht freiwillig erteilt wurde.

1c. Unbeschadet der übrigen Vorschriften dieser Verordnung umfassen die in Absatz 1 genannten Rechtsvorschriften der Mitgliedstaaten wenigstens die folgenden Mindeststandards:

a) Die Verarbeitung von Beschäftigtendaten ohne Kenntnis der Arbeitnehmer ist unzulässig. Abweichend von Satz 1 können die Mitgliedstaaten per Gesetz unter Anordnung angemessener Löschungsfristen die Zulässigkeit für den Fall vorsehen, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Arbeitnehmer im Beschäftigungsverhältnis eine Straftat oder eine andere schwerwiegende Pflichtverletzung begangen hat, die Erhebung zur Aufdeckung erforderlich ist und Art und Ausmaß der Erhebung im Hinblick auf den Zweck erforderlich und verhältnismäßig sind. Die Privat- und Intimsphäre der Arbeitnehmer ist jederzeit zu wahren. Die Ermittlung ist Sache der zuständigen Behörden.

b) Die offene optisch-elektronische und/oder offene akustisch-elektronische Überwachung der nicht öffentlich zugänglichen Teile des Betriebs, die überwiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, insbesondere in Sanitär-, Umkleide-, Pausen- und Schlafräumen, ist unzulässig. Die heimliche Überwachung ist in jedem Fall unzulässig.

c) Erheben oder verarbeiten Unternehmen oder Behörden im Rahmen ärztlicher Untersuchungen und/oder Eignungstests personenbezogene Daten, so müssen sie dem Bewerber oder Arbeitnehmer vorher erläutern, wofür diese Daten genutzt werden, und sicherstellen, dass ihnen nachher diese zusammen mit den Ergebnissen mitgeteilt und auf Anfrage erklärt werden. Datenerhebung zum Zwecke von genetischen Tests und Analysen ist grundsätzlich untersagt.

d) Ob und in welchem Umfang die Nutzung von Telefon, E-Mail, Internet und anderen Telekommunikationsdiensten auch zu privaten Zwecken erlaubt ist, kann durch Kollektivvereinbarung geregelt werden. Besteht keine Regelung durch Kollektivvereinbarung, trifft der Arbeitgeber unmittelbar mit dem Arbeitnehmer eine entsprechende Vereinbarung. Soweit eine private Nutzung erlaubt ist, ist die Verarbeitung anfallender Verkehrsdaten insbesondere zur Gewährleistung der Datensicherheit, zur Sicherstellung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen und Telekommunikationsdiensten und zur Abrechnung zulässig.

Abweichend von Satz 3 können die Mitgliedstaaten per Gesetz unter Anordnung angemessener Löschungsfristen die Zulässigkeit für den Fall vorsehen, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Arbeitnehmer im Beschäftigungsverhältnis eine Straftat oder eine andere schwerwiegende Pflichtverletzung begangen hat, die Erhebung zur Aufdeckung erforderlich ist und Art und Ausmaß der Erhebung im Hinblick auf den Zweck erforderlich und verhältnismäßig sind. Die Privat- und Intimsphäre der Arbeitnehmer ist jederzeit zu wahren. Die Ermittlung ist Sache der zuständigen Behörden.

e) Die personenbezogenen Daten von Arbeitnehmern, vor allem sensible Daten wie politische Orientierung sowie Zugehörigkeit zu und Aktivitäten in Gewerkschaften, dürfen unter keinen Umständen dazu verwendet werden, Arbeitnehmer auf sogenannte „schwarze Listen“ zu setzen und sie einer Überprüfung zu unterziehen oder sie von einer künftigen Beschäftigung auszuschließen. Die Verarbeitung, die Verwendung im Beschäftigungskontext und die Erstellung und Weitergabe schwarzer Listen von Arbeitnehmern oder sonstige Formen der Diskriminierung sind nicht zulässig. Um die wirksame Durchsetzung dieses Punkts zu gewährleisten, führen die Mitgliedstaaten Kontrollen durch und legen nach Maßgabe von Artikel 79 Absatz 6 angemessene Sanktionen fest.

1d. Die Übermittlung und Verarbeitung von personenbezogenen Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen innerhalb einer Unternehmensgruppe und mit rechts- und steuerberatenden Berufsangehörigen ist zulässig, soweit sie für den Geschäftsbetrieb relevant ist und der Abwicklung von zweckgebundenen Arbeits- oder Verwaltungsvorgängen dient und sie den schutzwürdigen Interessen und Grundrechten des Betroffenen nicht entgegensteht. Erfolgt die Übermittlung von Beschäftigtendaten in ein Drittland und/oder an eine internationale Organisation, findet Kapitel V Anwendung.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 und 1b erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

3. Die Kommission wird ermächtigt, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.

## Artikel 82a

## Datenverarbeitung im Bereich der sozialen Sicherheit

1. Die Mitgliedstaaten können gemäß den Bestimmungen dieser Verordnung besondere Rechtsvorschriften erlassen, in denen die Bedingungen für die im öffentlichen Interesse erfolgende Verarbeitung personenbezogener Daten durch ihre öffentlichen Einrichtungen und Ämter im Bereich der sozialen Sicherheit genau festgelegt werden.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Vorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

## Artikel 83

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

1. Gemäß den Vorschriften dieser Verordnung dürfen personenbezogene Daten nur dann zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung verarbeitet werden, wenn

a) diese Zwecke nicht auf andere Weise durch die Verarbeitung von Daten erfüllt werden können, die eine Bestimmung der betroffenen Person nicht oder nicht mehr ermöglichen;

b) Daten, die die Zuordnung von Informationen zu einer bestimmten oder bestimmbaren betroffenen Person ermöglichen, von den übrigen Informationen gemäß den höchsten technischen Standards getrennt aufbewahrt werden und sämtliche notwendigen Maßnahmen ergriffen werden, um unbefugte Rückschlüsse auf die Identität der betroffenen Personen zu verhindern.

2. entfällt

3. entfällt

## Artikel 83a

## Verarbeitung personenbezogener Daten für Archivdienste

1. Personenbezogene Daten können über den Zeitraum hinaus, der für die Erreichung der Zwecke der ursprünglichen Verarbeitung, für die sie erhoben wurden, notwendig ist, durch Archivdienste verarbeitet werden, deren Hauptaufgabe oder rechtliche Pflicht darin besteht, Archivgut im Interesse der Öffentlichkeit zu erfassen, zu erhalten, zu ordnen, bekanntzumachen, aufzuwerten und zu verbreiten, vor allem im Hinblick auf die Geltendmachung der Rechte einer Person sowie zu historischen, statistischen oder wissenschaftlichen Zwecken. Diese Aufgaben werden unter Achtung der Regelungen wahrgenommen, die die Mitgliedstaaten im Bereich des Zugangs, der Bekanntmachung und der Verbreitung von Verwaltungs- oder Archivdokumenten vorgesehen haben, wobei die Vorschriften dieser Verordnung, insbesondere im Hinblick auf Einwilligung und Widerspruchsrecht zu beachten sind.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

## Artikel 84

## Geheimhaltungspflichten

1. Gemäß den Vorschriften dieser Verordnung sorgen die Mitgliedstaaten dafür, dass die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 53 Absatz 2 gegenüber den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeitern, die nach einzelstaatlichem Recht oder nach von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, geregelt sind, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in

Bezug auf personenbezogene Daten, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.

2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Vorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

Artikel 85

Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

1. Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung angemessene Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

2. Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 angemessene Datenschutzregeln anwenden, erhalten eine Vereinbarkeitsbescheinigung nach Artikel 38.

Artikel 85a

Achtung der Grundrechte

Diese Verordnung berührt nicht die Verpflichtung zur Achtung der Grundrechte und der allgemeinen Rechtsgrundsätze gemäß Artikel 6 EUV.

Artikel 85b

Standardvorlagen

1. Die Kommission kann Standardvorlagen zu folgenden Punkten festlegen, wobei sie die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt:

a) bestimmte Arten der Erlangung einer nachprüfbaren Einwilligung gemäß Artikel 8 Absatz 1,

b) Mitteilungen gemäß Artikel 12 Absatz 2, auch für solche in elektronischer Form,

c) Informationen gemäß Artikel 14 Absatz 1 bis3,

d) Auskunftsgesuche und die Erteilung der Auskünfte gemäß Artikel 15 Absatz 1, darunter auch die Mitteilung der personenbezogenen Daten an die betroffene Person,

e) Dokumentation gemäß Artikel 28 Absatz 1,

f) Mitteilungen über Verstöße gemäß Artikel 31 an die Aufsichtsbehörde und Dokumentation gemäß Artikel 31 Absatz 4,

g) vorherige Konsultation gemäß Artikel 34 und Unterrichtung der Aufsichtsbehörde gemäß Artikel 34 Absatz 6.

2. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen.

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

## KAPITEL X

## DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

### Artikel 86

### Befugnisübertragung

1. Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

2. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 13a Absatz 5, Artikel 17 Absatz 9, Artikel 38 Absatz 4, Artikel 39 Absatz 2, Artikel 41 Absatz 3, Artikel 41 Absatz 5, Artikel 43 Absatz 3, Artikel 79 Absatz 7, Artikel 81 Absatz 3 sowie Artikel 82 Absatz 3 wird der Kommission ab dem Tag des Inkrafttretens dieser Verordnung für unbestimmte Zeit übertragen.

3. Die Befugnisübertragung gemäß Artikel 13a Absatz 5, Artikel 17 Absatz 9, Artikel 38 Absatz 4, Artikel 39 Absatz 2, Artikel 41 Absatz 3, Artikel 41 Absatz 5, Artikel 43 Absatz 3, Artikel 79 Absatz 7, Artikel 81 Absatz 3 sowie Artikel 82 Absatz 3 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Der Beschluss wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Er berührt nicht die Gültigkeit von bereits in Kraft getretenen delegierten Rechtsakten.

4. Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

5. Ein delegierter Rechtsakt, der gemäß Artikel 13a Absatz 5, Artikel 17 Absatz 9, Artikel 38 Absatz 4, Artikel 39 Absatz 2, Artikel 41 Absatz 3, Artikel 41 Absatz 5, Artikel 43 Absatz 3, Artikel 79 Absatz 7, Artikel 81 Absatz 3 sowie Artikel 82 Absatz 3 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden.

Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um sechs Monate verlängert.

Artikel 87

Ausschussverfahren

1. Die Kommission wird von einem Ausschuss unterstützt. Bei diesem Ausschuss handelt es sich um einen Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

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

3. entfällt

KAPITEL XI

SCHLUSSBESTIMMUNGEN

Artikel 88

Aufhebung der Richtlinie 95/46/EG

1. Die Richtlinie 95/46/EG wird aufgehoben.

2. Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

Artikel 89

Verhältnis zur Richtlinie 2002/58/EG und Änderung dieser Richtlinie

1. Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

2. Artikel 1 Absatz 2, Artikel 4 und Artikel 15 der Richtlinie 2002/58/EG werden gestrichen.

2a. Die Kommission legt bis spätestens zu dem in Artikel 91 Absatz 2 genannten Datum und unverzüglich einen Vorschlag für die Überarbeitung des Rechtsrahmens für die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vor, um Übereinstimmung mit der vorliegenden Verordnung herzustellen und für kohärente und einheitliche Rechtsvorschriften für

das Grundrecht des Schutzes personenbezogener Daten in der Europäischen Union Sorge zu tragen.

Artikel 89a

Verhältnis zur Verordnung (EG) Nr. 45/2001 und Änderung dieser Verordnung

1. Die Vorschriften dieser Verordnung gelten für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union in Bezug auf Angelegenheiten, in denen sie nicht den zusätzlichen Vorschriften der Verordnung (EG) Nr. 45/2001 unterliegen.

2. Die Kommission legt bis spätestens zu dem in Artikel 91 Absatz 2 genannten Datum und unverzüglich einen Vorschlag für die Überarbeitung des Rechtsrahmens für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Dienststellen und Agenturen der Union vor.

Artikel 90 Bewertung

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

Artikel 91

Inkrafttreten und Anwendung

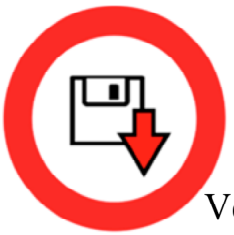
1. Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

2. Ihre Anwendung beginnt [zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt].

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

Anhang 1 – Darstellung der Hinweise nach Artikel 13a (neu)

1) Unter Berücksichtigung der Proportionen, auf die unter Punkt 6 verwiesen wird, sehen die Hinweise wie folgt aus:

| SYMBOL | WESENTLICHE INFORMATIONEN | ERFÜLLT |
|---|---|---|
|  | Es werden nicht mehr personenbezogene Daten **erhoben**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind. | |
|  | Es werden nicht mehr personenbezogene Daten **gespeichert**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind. | |
|  | Personenbezogene Daten werden nicht zu anderen als den Zwecken **verarbeitet**, für die sie erhoben wurden. | |
|  | Es werden keine personenbezogenen Daten an gewerbliche Dritte **weitergegeben**. | |
|  | Es werden keine personenbezogenen Daten **verkauft oder verpachtet**. | |
|  | Es werden keine personenbezogenen Daten **unverschlüsselt** aufbewahrt. | |

DIE EINHALTUNG DER BESTIMMUNGEN IN BEZUG AUF ZEILE 1–3 IST NACH EU-RECHT VORGESCHRIEBEI

2) Die folgenden Wörter in den angegebenen Zeilen der zweiten Spalte der Tabelle unter Punkt 1 mit dem Titel „WESENTLICHE INFORMATIONEN“ werden fett gedruckt:

a) das Wort „erhoben“ in der ersten Zeile der zweiten Spalte;

b) das Wort „aufbewahrt“ in der zweiten Zeile der zweiten Spalte;

c) das Wort „verarbeitet“ in der dritten Zeile der zweiten Spalte;

d) das Wort „weitergegeben“ in der vierten Zeile der zweiten Spalte;

e) die Wörter „verkauft und entgeltlich überlassen“ in der fünften Zeile der zweiten Spalte;

f) das Wort „unverschlüsselt“ in der sechsten Zeile der zweiten Spalte.

3) Unter Berücksichtigung der unter Punkt 6 genannten Proportionen wird in den Zeilen der dritten Spalte der Tabelle unter Punkt 1 mit dem Titel „ERFÜLLT“ entsprechend den unter Punkt 4 genannten Bedingungen jeweils eines der beiden folgenden Piktogramme dargestellt:

a)

b)

4)

a) Wenn nicht mehr personenbezogene Daten erhoben werden, als für die spezifischen Zwecke der Verarbeitung erforderlich sind, wird in der ersten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

b) Wenn mehr personenbezogene Daten erhoben werden, als für die spezifischen Zwecke der Verarbeitung erforderlich sind, wird in der ersten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm

dargestellt.

c) Wenn nicht mehr personenbezogene Daten gespeichert werden, als für die spezifischen Zwecke der Verarbeitung erforderlich sind, wird in der zweiten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

d) Wenn mehr personenbezogene Daten gespeichert werden, als für die spezifischen Zwecke der Verarbeitung erforderlich sind, wird in der zweiten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm dargestellt.

e) Wenn keine personenbezogenen Daten zu anderen als den Zwecken, für die sie erhoben wurden, verarbeitet werden, wird in der dritten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

f) Wenn personenbezogene Daten zu anderen als den Zwecken, für die sie erhoben wurden, verarbeitet werden, wird in der dritten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm dargestellt.

g) Werden keine personenbezogenen Daten an gewerbliche Dritte weitergegeben, wird in der vierten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

h) Werden personenbezogene Daten an gewerbliche Dritte weitergegeben, wird in der vierten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm dargestellt.

i) Werden keine personenbezogenen Daten verkauft oder verpachtet, wird in der fünften Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

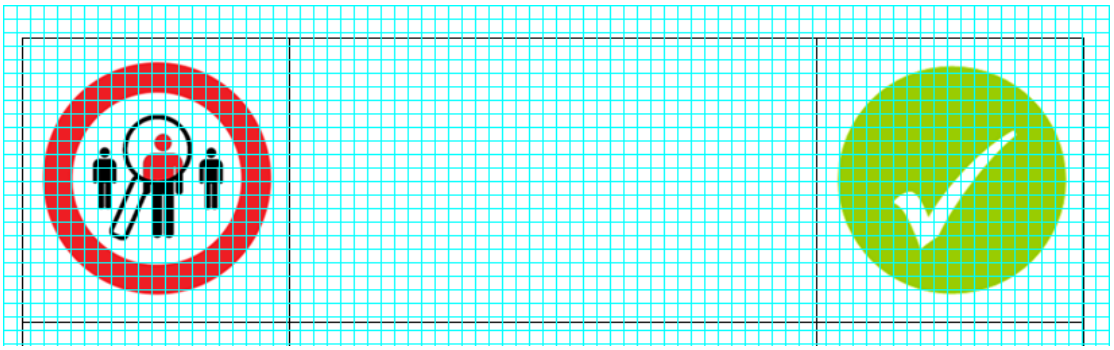
j) Werden personenbezogene Daten verkauft oder verpachtet, wird in der fünften Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm dargestellt.

k) Wenn keine personenbezogenen Daten in unverschlüsselter Form gespeichert werden, wird in der sechsten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3a angegebene Piktogramm dargestellt.

l) Wenn personenbezogene Daten in unverschlüsselter Form gespeichert werden, wird in der sechsten Zeile der dritten Spalte der Tabelle unter Punkt 1 das unter Punkt 3b angegebene Piktogramm dargestellt.

5) Die Pantone-Referenzfarben der Piktogramme unter Punkt 1 sind Pantone Schwarz Nr. 7547 und Pantone Rot Nr. 485. Die Pantone-Referenzfarbe des Piktogramms in Punkt 3a ist Pantone Grün Nr. 370. Die Pantone-Referenzfarbe des Piktogramms in Punkt 3b ist Pantone Rot Nr. 485.

6) Die sich aus dem abgebildeten Raster ergebenden Proportionen müssen eingehalten werden, auch wenn die Tabelle verkleinert oder vergrößert wird:



Geschehen zu Brüssel am

Im Namen des Europäischen Parlaments Im Namen des Rates

Der Präsident Der Präsident