# EU-DSGVO - 173 Erwägungsgründe

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

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (4) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

(4) Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

(5) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt. Der unionsweite Austausch personenbezogener Daten zwischen öffentlichen und privaten Akteuren einschließlich natürlichen Personen, Vereinigungen und Unternehmen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten, zusammenzuarbeiten und personenbezogene Daten auszutauschen, damit sie ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen können.

(6) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.

(7) Diese Entwicklungen erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, da es von großer Wichtigkeit ist, eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen. Natürliche Personen, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.

(8) Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.

(9) Die Ziele und Grundsätze der Richtlinie 95/46/EG besitzen nach wie vor Gültigkeit, doch hat die Richtlinie nicht verhindern können, dass der Datenschutz in der Union unterschiedlich gehandhabt wird, Rechtsunsicherheit besteht oder in der Öffentlichkeit die Meinung weit verbreitet ist, dass erhebliche Risiken für den Schutz natürlicher Personen bestehen, insbesondere im Zusammenhang mit der Benutzung des Internets. Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, können den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.

(10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern. Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „sensible Daten“). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

(11) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie — in den Mitgliedstaaten — gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.

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

(13) Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Das reibungslose Funktionieren des Binnenmarkts erfordert, dass der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener

Daten eingeschränkt oder verboten wird. Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinstunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission (5) maßgebend sein.

(14) Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.

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

(16) Diese Verordnung gilt nicht für Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Verkehrs personenbezogener Daten im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten. Diese Verordnung gilt nicht für die von den Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchgeführte Verarbeitung personenbezogener Daten.

(17) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates (6) gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst und im Lichte der vorliegenden Verordnung angewandt werden. Um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu gewährleisten, sollten die erforderlichen Anpassungen der Verordnung (EG) Nr. 45/2001 im Anschluss an den Erlass der vorliegenden Verordnung vorgenommen werden, damit sie gleichzeitig mit der vorliegenden Verordnung angewandt werden können.

(18) Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

(19) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016/680 des

Europäischen Parlaments und des Rates (7) unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016/680 mit Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt, als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung.

(20) Diese Verordnung gilt zwar unter anderem für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten.

(21) Die vorliegende Verordnung berührt nicht die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates (8) und insbesondere die der Vorschriften der Artikel 12 bis 15 jener Richtlinie zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste. Die genannte Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt.

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

(23) Damit einer natürlichen Person der gemäß dieser Verordnung gewährleistete Schutz nicht vorenthalten wird, sollte die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen betroffenen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten. Um festzustellen, ob dieser Verantwortliche oder

Auftragsverarbeiter betroffenen Personen, die sich in der Union befinden, Waren oder Dienstleistungen anbietet, sollte festgestellt werden, ob der Verantwortliche oder Auftragsverarbeiter offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten. Während die bloße Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt ist, können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich in der Union befinden, darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen in der Union Waren oder Dienstleistungen anzubieten.

(24) Die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.

(25) Ist nach Völkerrecht das Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, so sollte die Verordnung auch auf einen nicht in der Union niedergelassenen Verantwortlichen Anwendung finden.

(26) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

(27) Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

(28) Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der „Pseudonymisierung“ in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.

(29) Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei

demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um — für die jeweilige Verarbeitung — die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche, sollte die befugten Personen bei diesem Verantwortlichen angeben.

(30) Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.

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

(32) Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.

(33) Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.

(34) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen, Desoxyribonukleinsäure (DNS)-

oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.

(35) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates (9) für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

(36) Die Hauptniederlassung des Verantwortlichen in der Union sollte der Ort seiner Hauptverwaltung in der Union sein, es sei denn, dass Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung des Verantwortlichen in der Union getroffen werden; in diesem Fall sollte die letztgenannte als Hauptniederlassung gelten. Zur Bestimmung der Hauptniederlassung eines Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werden. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird. Das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten oder Verarbeitungstätigkeiten begründen an sich noch keine Hauptniederlassung und sind daher kein ausschlaggebender Faktor für das Bestehen einer Hauptniederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, oder — wenn er keine Hauptverwaltung in der Union hat — der Ort, an dem die wesentlichen Verarbeitungstätigkeiten in der Union stattfinden. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter betroffen, so sollte die Aufsichtsbehörde des Mitgliedstaats, in dem der Verantwortliche seine Hauptniederlassung hat, die zuständige federführende Aufsichtsbehörde bleiben, doch sollte die Aufsichtsbehörde des Auftragsverarbeiters als betroffene Aufsichtsbehörde betrachtet werden und diese Aufsichtsbehörde sollte sich an dem in dieser Verordnung vorgesehenen Verfahren der Zusammenarbeit beteiligen. Auf jeden Fall sollten die Aufsichtsbehörden des Mitgliedstaats oder der Mitgliedstaaten, in dem bzw. denen der Auftragsverarbeiter eine oder mehrere Niederlassungen hat, nicht als betroffene Aufsichtsbehörden betrachtet werden, wenn sich der Beschlussentwurf nur auf den Verantwortlichen bezieht. Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.

(37) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.

(38) Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

(39) Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

(40) Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder — wann immer in dieser Verordnung darauf Bezug genommen wird — aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

(41) Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der

Europäischen Union (im Folgenden „Gerichtshof“) und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein.

(42) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates (10) sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

(43) Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

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

(45) Erfolgt die Verarbeitung durch den Verantwortlichen aufgrund einer ihm obliegenden rechtlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen. Mit dieser Verordnung wird nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt. Ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge kann ausreichend sein, wenn die Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt oder wenn die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnten in diesem Recht die allgemeinen Bedingungen dieser Verordnung zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten präzisiert und es könnte darin festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, ob es sich bei dem Verantwortlichen, der eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder, sofern dies durch das öffentliche Interesse einschließlich gesundheitlicher Zwecke, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, gerechtfertigt ist, eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln sollte.

(46) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen

Person zu schützen. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.

(47) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

(48) Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.

(49) Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams — CERT, beziehungsweise Computer Security Incident Response Teams — CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

(50) Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.
Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

(51) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs „rassische Herkunft“ in dieser Verordnung nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser

Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist. Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.

(52) Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien von personenbezogenen Daten sollten auch erlaubt sein, wenn sie im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen sind, und — vorbehaltlich angemessener Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte — wenn dies durch das öffentliche Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Eine solche Ausnahme kann zu gesundheitlichen Zwecken gemacht werden, wie der Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll, oder wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient. Die Verarbeitung solcher personenbezogener Daten sollte zudem ausnahmsweise erlaubt sein, wenn sie erforderlich ist, um rechtliche Ansprüche, sei es in einem Gerichtsverfahren oder in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, geltend zu machen, auszuüben oder zu verteidigen.

(53) Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse harmonisieren, insbesondere wenn die Verarbeitung dieser Daten für gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und angemessene Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden. Den Mitgliedstaaten sollte gestattet werden, weitere Bedingungen —

einschließlich Beschränkungen — in Bezug auf die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten beizubehalten oder einzuführen. Dies sollte jedoch den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten.

(54) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates (11) ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.

(55) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.

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

(57) Kann der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren. Allerdings sollte er sich nicht weigern, zusätzliche Informationen entgegenzunehmen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen. Die Identifizierung sollte die digitale Identifizierung einer betroffenen Person — beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden — einschließen.

(58) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

(59) Es sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung der Rechte, die ihr nach dieser Verordnung zustehen, erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, insbesondere wenn die

personenbezogenen Daten elektronisch verarbeitet werden. Der Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person unverzüglich, spätestens aber innerhalb eines Monats zu beantworten und gegebenenfalls zu begründen, warum er den Antrag ablehnt.

(60) Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Darüber hinaus sollte er die betroffene Person darauf hinweisen, dass Profiling stattfindet und welche Folgen dies hat. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Die betreffenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, so sollten sie maschinenlesbar sein.

(61) Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung mitgeteilt werden oder, falls die Daten nicht von ihr, sondern aus einer anderen Quelle erlangt werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die personenbezogenen Daten rechtmäßig einem anderen Empfänger offengelegt werden dürfen, sollte die betroffene Person bei der erstmaligen Offenlegung der personenbezogenen Daten für diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck zu verarbeiten als den, für den die Daten erhoben wurden, so sollte er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und andere erforderliche Informationen zur Verfügung stellen. Konnte der betroffenen Person nicht mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.

(62) Die Pflicht, Informationen zur Verfügung zu stellen, erübrigt sich jedoch, wenn die betroffene Person die Information bereits hat, wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist. Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein. Als Anhaltspunkte sollten dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien in Betracht gezogen werden.

(63) Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und

insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

(64) Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.

(65) Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein „Recht auf Vergessenwerden“, wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten — insbesondere die im Internet gespeicherten — später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist. Die weitere Speicherung der personenbezogenen Daten sollte jedoch rechtmäßig sein, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

(66) Um dem „Recht auf Vergessenwerden“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen — auch technischer Art — treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.

(67) Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentliche Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden.

(68) Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten,

gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als ihrer Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist. Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen. Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden.

(69) Dürfen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt — die dem Verantwortlichen übertragen wurde, — oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sich aus ihrer besonderen Situation ergebenden personenbezogenen Daten einzulegen. Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.

(70) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so sollte die betroffene Person jederzeit unentgeltlich insoweit Widerspruch gegen eine solche — ursprüngliche oder spätere — Verarbeitung einschließlich des Profilings einlegen können, als sie mit dieser Direktwerbung zusammenhängt. Die betroffene Person sollte ausdrücklich auf dieses Recht hingewiesen werden; dieser Hinweis sollte in einer verständlichen und von anderen Informationen getrennten Form erfolgen.

(71) Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling“, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich des

Profilings, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der Institutionen der Union oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung. Diese Maßnahme sollte kein Kind betreffen.
Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben. Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.

(72) Das Profiling unterliegt den Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten, wie etwa die Rechtsgrundlage für die Verarbeitung oder die Datenschutzgrundsätze. Der durch diese Verordnung eingerichtete Europäische Datenschutzausschuss (im Folgenden „Ausschuss“) sollte, diesbezüglich Leitlinien herausgeben können.

(73) Im Recht der Union oder der Mitgliedstaaten können Beschränkungen hinsichtlich bestimmter Grundsätze und hinsichtlich des Rechts auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, des Rechts auf Datenübertragbarkeit und Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person und bestimmten damit zusammenhängenden Pflichten der Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, die Verhütung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung — was auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt — oder die Verhütung, Aufdeckung und Verfolgung von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen, das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses sowie die Weiterverarbeitung von archivierten personenbezogenen Daten zur Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen gehört, und zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen soziale Sicherheit, öffentliche Gesundheit und humanitäre Hilfe, zu schützen.

Diese Beschränkungen sollten mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

(74) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

(76) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

(77) Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Ausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Ausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.

(78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in

Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

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

(80) Jeder Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf betroffene Personen beziehen, die sich in der Union aufhalten, und dazu dienen, diesen Personen in der Union Waren oder Dienstleistungen anzubieten — unabhängig davon, ob von der betroffenen Person eine Zahlung verlangt wird — oder deren Verhalten, soweit dieses innerhalb der Union erfolgt, zu beobachten, sollte einen Vertreter benennen müssen, es sei denn, die Verarbeitung erfolgt gelegentlich, schließt nicht die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ein und bringt unter Berücksichtigung ihrer Art, ihrer Umstände, ihres Umfangs und ihrer Zwecke wahrscheinlich kein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich oder bei dem Verantwortlichen handelt es sich um eine Behörde oder öffentliche Stelle. Der Vertreter sollte im Namen des Verantwortlichen oder des Auftragsverarbeiters tätig werden und den Aufsichtsbehörden als Anlaufstelle dienen. Der Verantwortliche oder der Auftragsverarbeiter sollte den Vertreter ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln. Die Benennung eines solchen Vertreters berührt nicht die Verantwortung oder Haftung des Verantwortlichen oder des Auftragsverarbeiters nach Maßgabe dieser Verordnung. Ein solcher Vertreter sollte seine Aufgaben entsprechend dem Mandat des Verantwortlichen oder Auftragsverarbeiters ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des Verantwortlichen oder Auftragsverarbeiters sollte der bestellte Vertreter Durchsetzungsverfahren unterworfen werden.

(81) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die — insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen — hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen — auch für die Sicherheit der Verarbeitung — getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung,

Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(82) Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

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

(84) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

(85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht

nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(86) Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

(87) Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.

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

(89) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen gehören insbesondere solche, bei denen neue Technologien eingesetzt werden oder die neuartig sind und bei denen der Verantwortliche noch keine Datenschutz-Folgenabschätzung durchgeführt hat bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine Datenschutz-Folgenabschätzung notwendig geworden ist.

(90) In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien

und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

(91) Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

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

(93) Anlässlich des Erlasses des Gesetzes des Mitgliedstaats, auf dessen Grundlage die Behörde oder öffentliche Stelle ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt, können die Mitgliedstaaten es für erforderlich erachten, solche Folgeabschätzungen vor den Verarbeitungsvorgängen durchzuführen.

(94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung

personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.

(95) Der Auftragsverarbeiter sollte erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.

(96) Eine Konsultation der Aufsichtsbehörde sollte auch während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften, in denen eine Verarbeitung personenbezogener Daten vorgesehen ist, erfolgen, um die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.

(97) In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

(98) Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Insbesondere könnten in diesen Verhaltensregeln — unter Berücksichtigung des mit der Verarbeitung wahrscheinlich einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen — die Pflichten der Verantwortlichen und der Auftragsverarbeiter bestimmt werden.

(99) Bei der Ausarbeitung oder bei der Änderung oder Erweiterung solcher Verhaltensregeln sollten Verbände und oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, die maßgeblichen Interessenträger, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.

(100) Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

(101) Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung

personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

(102) Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt. Die Mitgliedstaaten können völkerrechtliche Übereinkünfte schließen, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen beinhalten, sofern sich diese Übereinkünfte weder auf diese Verordnung noch auf andere Bestimmungen des Unionsrechts auswirken und ein angemessenes Schutzniveau für die Grundrechte der betroffenen Personen umfassen.

(103) Die Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, und auf diese Weise in Bezug auf das Drittland oder die internationale Organisation, das bzw. die für fähig gehalten wird, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Die Kommission kann, nach Abgabe einer ausführlichen Erklärung, in der dem Drittland oder der internationalen Organisation eine Begründung gegeben wird, auch entscheiden, eine solche Feststellung zu widerrufen.

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

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

Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Ausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.

(106) Die Kommission sollte die Wirkungsweise von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem bestimmten Sektor eines Drittlands oder einer internationalen Organisation überwachen; sie sollte auch die Wirkungsweise der Feststellungen, die auf der Grundlage des Artikels 25 Absatz 6 oder des Artikels 26 Absatz 4 der Richtlinie 95/46/EG erlassen werden, überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung von deren Wirkungsweise vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen. Für die Zwecke der Überwachung und der Durchführung der regelmäßigen Überprüfungen sollte die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments und des Rates sowie der anderen einschlägigen Stellen und Quellen berücksichtigen. Die Kommission sollte innerhalb einer angemessenen Frist die Wirkungsweise der letztgenannten Beschlüsse bewerten und dem durch diese Verordnung eingesetzten Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates (12) sowie dem Europäischen Parlament und dem Rat über alle maßgeblichen Feststellungen Bericht erstatten.

(107) Die Kommission kann feststellen, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Verordnung in Bezug auf die Datenübermittlung vorbehaltlich geeigneter Garantien, einschließlich verbindlicher interner Datenschutzvorschriften und auf Ausnahmen für bestimmte Fälle werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

(108) Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen. Datenübermittlungen dürfen auch von Behörden oder öffentlichen Stellen an Behörden oder öffentliche Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen — wie beispielsweise einer gemeinsamen Absichtserklärung –, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden, aufzunehmen sind. Die Genehmigung der zuständigen Aufsichtsbehörde sollte erlangt werden, wenn die Garantien in nicht rechtsverbindlichen Verwaltungsvereinbarungen vorgesehen sind.

(109) Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte

den Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.

(110) Jede Unternehmensgruppe oder jede Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sollte für ihre internationalen Datenübermittlungen aus der Union an Organisationen derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, genehmigte verbindliche interne Datenschutzvorschriften anwenden dürfen, sofern diese sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.

(111) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat, wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Verfahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist. Die Übermittlung sollte zudem möglich sein, wenn sie zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaats festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn sie aus einem durch Rechtsvorschriften vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In letzterem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.

(112) Diese Ausnahmen sollten insbesondere für Datenübermittlungen gelten, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. Die Übermittlung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein Interesse, das für die lebenswichtigen Interessen — einschließlich der körperlichen Unversehrtheit oder des Lebens — der betroffenen Person oder einer anderen Person wesentlich ist, zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben. Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten sollten solche Bestimmungen der Kommission mitteilen. Jede Übermittlung personenbezogener Daten einer betroffenen Person, die aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen, an eine internationale humanitäre Organisation, die erfolgt, um eine nach den Genfer Konventionen obliegende Aufgabe auszuführen oder um dem in bewaffneten Konflikten anwendbaren humanitären Völkerrecht nachzukommen, könnte als aus einem wichtigen Grund im öffentlichen Interesse notwendig oder als im lebenswichtigen Interesse der betroffenen Person liegend erachtet werden.

(113) Übermittlungen, die als nicht wiederholt erfolgend gelten können und nur eine begrenzte Zahl von betroffenen Personen betreffen, könnten auch zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der Verantwortliche sämtliche Umstände der Datenübermittlung geprüft hat. Der Verantwortliche sollte insbesondere die Art der personenbezogenen Daten, den Zweck und die Dauer der vorgesehenen Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland berücksichtigen und angemessene Garantien zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogener Daten vorsehen. Diese Übermittlungen sollten nur in den verbleibenden Fällen möglich sein, in denen keiner der anderen Gründe für die Übermittlung anwendbar ist. Bei wissenschaftlichen oder historischen Forschungszwecken oder bei statistischen Zwecken sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Der Verantwortliche sollte die Aufsichtsbehörde und die betroffene Person von der Übermittlung in Kenntnis setzen.

(114) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Datenschutzniveaus vorliegt, sollte der Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten in der Union nach der Übermittlung dieser Daten eingeräumt werden, damit sie weiterhin die Grundrechte und Garantien genießen können.

(115) Manche Drittländer erlassen Gesetze, Vorschriften und sonstige Rechtsakte, die vorgeben, die Verarbeitungstätigkeiten natürlicher und juristischer Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar zu regeln. Dies kann Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden in Drittländern umfassen, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird und die nicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets der betreffenden Drittländer kann gegen internationales Recht verstoßen und dem durch diese Verordnung in der Union gewährleisteten Schutz natürlicher Personen zuwiderlaufen. Datenübermittlungen sollten daher nur zulässig sein, wenn die Bedingungen dieser Verordnung für Datenübermittlungen an Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Offenlegung aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt ist.

(116) Wenn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, besteht eine erhöhte Gefahr, dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können und sich insbesondere gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, widersprüchliche Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. Um Mechanismen der internationalen Zusammenarbeit zu entwickeln, die die internationale Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtern und sicherstellen, sollten die Kommission und die Aufsichtsbehörden Informationen austauschen und bei Tätigkeiten, die mit der Ausübung ihrer Befugnisse in Zusammenhang stehen, mit den zuständigen Behörden der Drittländer nach dem Grundsatz der Gegenseitigkeit und gemäß dieser Verordnung zusammenarbeiten.

(117) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die befugt sind, ihre Aufgaben und Befugnisse völlig unabhängig wahrzunehmen, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde errichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.

(118) Die Tatsache, dass die Aufsichtsbehörden unabhängig sind, sollte nicht bedeuten, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden bzw. sie keiner gerichtlichen Überprüfung unterzogen werden können.

(119) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er mittels Rechtsvorschriften sicherstellen, dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Ausschuss und der Kommission gewährleistet.

(120) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, einschließlich derer im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über einen eigenen, öffentlichen, jährlichen Haushaltsplan verfügen, der Teil des gesamten Staatshaushalts oder nationalen Haushalts sein kann.

(121) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Rechtsvorschriften von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder im Wege eines transparenten Verfahrens entweder — auf Vorschlag der Regierung, eines Mitglieds der Regierung, des Parlaments oder einer Parlamentskammer — vom Parlament, der Regierung oder dem Staatsoberhaupt des Mitgliedstaats oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder ihr Amt integer ausüben, von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben. Die Aufsichtsbehörde sollte über eigenes Personal verfügen, das sie selbst oder eine nach dem Recht des Mitgliedstaats eingerichtete unabhängige Stelle auswählt und das ausschließlich der Leitung des Mitglieds oder der Mitglieder der Aufsichtsbehörde unterstehen sollte.

(122) Jede Aufsichtsbehörde sollte dafür zuständig sein, im Hoheitsgebiet ihres Mitgliedstaats die Befugnisse auszuüben und die Aufgaben zu erfüllen, die ihr mit dieser Verordnung übertragen wurden. Dies sollte insbesondere für Folgendes gelten: die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen oder Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats, die Verarbeitung personenbezogener Daten durch Behörden oder private Stellen, die im öffentlichen Interesse handeln, Verarbeitungstätigkeiten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben, oder Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Union, sofern sie auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet sind. Dies sollte auch die Bearbeitung von Beschwerden einer betroffenen Person, die Durchführung von Untersuchungen über die Anwendung dieser Verordnung sowie die Förderung der Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließen.

(123) Die Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen im Hinblick auf die Verarbeitung ihrer Daten zu schützen und den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern. Zu diesem Zweck sollten die Aufsichtsbehörden untereinander und mit der Kommission zusammenarbeiten, ohne dass eine Vereinbarung zwischen den Mitgliedstaaten über die Leistung von Amtshilfe oder über eine derartige Zusammenarbeit erforderlich wäre.

(124) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte — im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung — insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.

(125) Die federführende Behörde sollte berechtigt sein, verbindliche Beschlüsse über Maßnahmen zu erlassen, mit denen die ihr gemäß dieser Verordnung übertragenen Befugnisse ausgeübt werden. In ihrer Eigenschaft als federführende Behörde sollte diese Aufsichtsbehörde für die enge Einbindung und Koordinierung der betroffenen Aufsichtsbehörden im Entscheidungsprozess sorgen. Wird beschlossen, die Beschwerde der betroffenen Person vollständig oder teilweise abzuweisen, so sollte dieser Beschluss von der Aufsichtsbehörde angenommen werden, bei der die Beschwerde eingelegt wurde.

(126) Der Beschluss sollte von der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden gemeinsam vereinbart werden und an die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters gerichtet sein und für den Verantwortlichen und den Auftragsverarbeiter verbindlich sein. Der Verantwortliche oder Auftragsverarbeiter sollte die erforderlichen Maßnahmen treffen, um die Einhaltung dieser Verordnung und die Umsetzung des Beschlusses zu gewährleisten, der der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters im Hinblick auf die Verarbeitungstätigkeiten in der Union von der federführenden Aufsichtsbehörde mitgeteilt wurde.

(127) Jede Aufsichtsbehörde, die nicht als federführende Aufsichtsbehörde fungiert, sollte in örtlichen Fällen zuständig sein, wenn der Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, der Gegenstand der spezifischen Verarbeitung aber nur die Verarbeitungstätigkeiten in einem einzigen Mitgliedstaat und nur betroffene Personen in diesem einen Mitgliedstaat betrifft, beispielsweise wenn es um die Verarbeitung von personenbezogenen Daten von Arbeitnehmern im spezifischen Beschäftigungskontext eines Mitgliedstaats geht. In solchen Fällen sollte die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit unterrichten. Nach ihrer Unterrichtung sollte die federführende Aufsichtsbehörde entscheiden, ob sie den Fall nach den Bestimmungen zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden gemäß der Vorschrift zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden (im Folgenden „Verfahren der Zusammenarbeit und Kohärenz“) regelt oder ob die Aufsichtsbehörde, die sie unterrichtet hat, den Fall auf örtlicher Ebene regeln sollte. Dabei sollte die federführende Aufsichtsbehörde berücksichtigen, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat, damit Beschlüsse gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter wirksam durchgesetzt werden. Entscheidet die federführende Aufsichtsbehörde, den Fall selbst zu regeln, sollte die

Aufsichtsbehörde, die sie unterrichtet hat, die Möglichkeit haben, einen Beschlussentwurf vorzulegen, dem die federführende Aufsichtsbehörde bei der Ausarbeitung ihres Beschlussentwurfs im Rahmen dieses Verfahrens der Zusammenarbeit und Kohärenz weitestgehend Rechnung tragen sollte.

(128) Die Vorschriften über die federführende Behörde und das Verfahren der Zusammenarbeit und Kohärenz sollten keine Anwendung finden, wenn die Verarbeitung durch Behörden oder private Stellen im öffentlichen Interesse erfolgt. In diesen Fällen sollte die Aufsichtsbehörde des Mitgliedstaats, in dem die Behörde oder private Einrichtung ihren Sitz hat, die einzige Aufsichtsbehörde sein, die dafür zuständig ist, die Befugnisse auszuüben, die ihr mit dieser Verordnung übertragen wurden.

(129) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter, insbesondere im Fall von Beschwerden natürlicher Personen, Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse und Genehmigungsbefugnisse und beratende Befugnisse, sowie — unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten — die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Gerichtsverfahren anzustrengen. Dazu sollte auch die Befugnis zählen, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Die Mitgliedstaaten können andere Aufgaben im Zusammenhang mit dem Schutz personenbezogener Daten im Rahmen dieser Verordnung festlegen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Verordnung geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Verfahrensrecht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Jede rechtsverbindliche Maßnahme der Aufsichtsbehörde sollte schriftlich erlassen werden und sie sollte klar und eindeutig sein; die Aufsichtsbehörde, die die Maßnahme erlassen hat, und das Datum, an dem die Maßnahme erlassen wurde, sollten angegeben werden und die Maßnahme sollte vom Leiter oder von einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein und eine Begründung für die Maßnahme sowie einen Hinweis auf das Recht auf einen wirksamen Rechtsbehelf enthalten. Dies sollte zusätzliche Anforderungen nach dem Verfahrensrecht der Mitgliedstaaten nicht ausschließen. Der Erlass eines rechtsverbindlichen Beschlusses setzt voraus, dass er in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, gerichtlich überprüft werden kann.

(130) Ist die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, nicht die federführende Aufsichtsbehörde, so sollte die federführende Aufsichtsbehörde gemäß den Bestimmungen dieser Verordnung über Zusammenarbeit und Kohärenz eng mit der Aufsichtsbehörde zusammenarbeiten, bei der die Beschwerde eingereicht wurde. In solchen Fällen sollte die federführende Aufsichtsbehörde bei Maßnahmen, die rechtliche Wirkungen entfalten sollen, unter anderem bei der Verhängung von Geldbußen, den Standpunkt der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde und die weiterhin befugt sein sollte, in Abstimmung mit der zuständigen Aufsichtsbehörde Untersuchungen im Hoheitsgebiet ihres eigenen Mitgliedstaats durchzuführen, weitestgehend berücksichtigen.

(131) Wenn eine andere Aufsichtsbehörde als federführende Aufsichtsbehörde für die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters fungieren sollte, der konkrete Gegenstand einer Beschwerde oder der mögliche Verstoß jedoch nur die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters in dem Mitgliedstaat betrifft, in dem die Beschwerde eingereicht wurde oder der

mögliche Verstoß aufgedeckt wurde, und die Angelegenheit keine erheblichen Auswirkungen auf betroffene Personen in anderen Mitgliedstaaten hat oder haben dürfte, sollte die Aufsichtsbehörde, bei der eine Beschwerde eingereicht wurde oder die Situationen, die mögliche Verstöße gegen diese Verordnung darstellen, aufgedeckt hat bzw. auf andere Weise darüber informiert wurde, versuchen, eine gütliche Einigung mit dem Verantwortlichen zu erzielen; falls sich dies als nicht erfolgreich erweist, sollte sie die gesamte Bandbreite ihrer Befugnisse wahrnehmen. Dies sollte auch Folgendes umfassen: die spezifische Verarbeitung im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde oder im Hinblick auf betroffene Personen im Hoheitsgebiet dieses Mitgliedstaats; die Verarbeitung im Rahmen eines Angebots von Waren oder Dienstleistungen, das speziell auf betroffene Personen im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde ausgerichtet ist; oder eine Verarbeitung, die unter Berücksichtigung der einschlägigen rechtlichen Verpflichtungen nach dem Recht der Mitgliedstaaten bewertet werden muss.

(132) Auf die Öffentlichkeit ausgerichtete Sensibilisierungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, und an natürliche Personen, insbesondere im Bildungsbereich, richten.

(133) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist. Eine Aufsichtsbehörde, die um Amtshilfe ersucht hat, kann eine einstweilige Maßnahme erlassen, wenn sie nicht binnen eines Monats nach Eingang des Amtshilfeersuchens bei der ersuchten Aufsichtsbehörde eine Antwort von dieser erhalten hat.

(134) Jede Aufsichtsbehörde sollte gegebenenfalls an gemeinsamen Maßnahmen von anderen Aufsichtsbehörden teilnehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer bestimmten Frist antworten müssen.

(135) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) für die Zusammenarbeit zwischen den Aufsichtsbehörden eingeführt werden. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme zu erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragt, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Dieses Verfahren sollte andere Maßnahmen, die die Kommission möglicherweise in Ausübung ihrer Befugnisse nach den Verträgen trifft, unberührt lassen.

(136) Bei Anwendung des Kohärenzverfahrens sollte der Ausschuss, falls von der Mehrheit seiner Mitglieder so entschieden wird oder falls eine andere betroffene Aufsichtsbehörde oder die Kommission darum ersuchen, binnen einer festgelegten Frist eine Stellungnahme abgeben. Dem Ausschuss sollte auch die Befugnis übertragen werden, bei Streitigkeiten zwischen Aufsichtsbehörden rechtsverbindliche Beschlüsse zu erlassen. Zu diesem Zweck sollte er in klar bestimmten Fällen, in denen die Aufsichtsbehörden insbesondere im Rahmen des Verfahrens der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden widersprüchliche Standpunkte zu dem Sachverhalt, vor allem in der Frage, ob ein Verstoß gegen diese Verordnung vorliegt, vertreten, grundsätzlich mit einer Mehrheit von zwei Dritteln seiner Mitglieder rechtsverbindliche Beschlüsse erlassen.

(137) Es kann dringender Handlungsbedarf zum Schutz der Rechte und Freiheiten von betroffenen Personen bestehen, insbesondere wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht. Eine Aufsichtsbehörde sollte daher hinreichend begründete einstweilige Maßnahmen in ihrem Hoheitsgebiet mit einer festgelegten Geltungsdauer von höchstens drei Monaten erlassen können.

(138) Die Anwendung dieses Verfahrens sollte in den Fällen, in denen sie verbindlich vorgeschrieben ist, eine Bedingung für die Rechtmäßigkeit einer Maßnahme einer Aufsichtsbehörde sein, die rechtliche Wirkungen entfalten soll. In anderen Fällen von grenzüberschreitender Relevanz sollte das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden zur Anwendung gelangen, und die betroffenen Aufsichtsbehörden können auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen, ohne auf das Kohärenzverfahren zurückzugreifen.

(139) Zur Förderung der einheitlichen Anwendung dieser Verordnung sollte der Ausschuss als unabhängige Einrichtung der Union eingesetzt werden. Damit der Ausschuss seine Ziele erreichen kann, sollte er Rechtspersönlichkeit besitzen. Der Ausschuss sollte von seinem Vorsitz vertreten werden. Er sollte die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten ersetzen. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder deren jeweiligen Vertretern gebildet werden. An den Beratungen des Ausschusses sollte die Kommission ohne Stimmrecht teilnehmen und der Europäische Datenschutzbeauftragte sollte spezifische Stimmrechte haben. Der Ausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission insbesondere im Hinblick auf das Schutzniveau in Drittländern oder internationalen Organisationen beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Ausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.

(140) Der Ausschusssollte von einem Sekretariat unterstützt werden, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird. Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, sollte diese Aufgaben ausschließlich gemäß den Anweisungen des Vorsitzes des Ausschusses durchführen und diesem Bericht erstatten.

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

(142) Betroffene Personen, die sich in ihren Rechten gemäß dieser Verordnung verletzt sehen, sollten das Recht haben, nach dem Recht eines Mitgliedstaats gegründete Einrichtungen, Organisationen oder Verbände ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes personenbezogener Daten tätig sind, zu beauftragen, in ihrem Namen Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder das Recht auf Schadensersatz in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. Die Mitgliedstaaten können vorsehen, dass diese Einrichtungen, Organisationen oder Verbände das Recht haben, unabhängig vom Auftrag einer betroffenen Person in dem betreffenden Mitgliedstaat eine eigene Beschwerde einzulegen, und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf haben sollten, wenn sie Grund zu der Annahme haben, dass die Rechte der betroffenen Person infolge einer nicht im Einklang mit dieser Verordnung stehenden

Verarbeitung verletzt worden sind. Diesen Einrichtungen, Organisationen oder Verbänden kann unabhängig vom Auftrag einer betroffenen Person nicht gestattet werden, im Namen einer betroffenen Person Schadenersatz zu verlangen.

(143) Jede natürliche oder juristische Person hat das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof eine Klage auf Nichtigerklärung eines Beschlusses des Ausschusses zu erheben. Als Adressaten solcher Beschlüsse müssen die betroffenen Aufsichtsbehörden, die diese Beschlüsse anfechten möchten, binnen zwei Monaten nach deren Übermittlung gemäß Artikel 263 AEUV Klage erheben. Sofern Beschlüsse des Ausschusses einen Verantwortlichen, einen Auftragsverarbeiter oder den Beschwerdeführer unmittelbar und individuell betreffen, so können diese Personen binnen zwei Monaten nach Veröffentlichung der betreffenden Beschlüsse auf der Website des Ausschusses im Einklang mit Artikel 263 AEUV eine Klage auf Nichtigerklärung erheben. Unbeschadet dieses Rechts nach Artikel 263 AEUV sollte jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Das Recht auf einen wirksamen gerichtlichen Rechtsbehelf umfasst jedoch nicht rechtlich nicht bindende Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Verfahrensrecht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den bei ihnen anhängigen Rechtsstreit maßgebliche Sach- und Rechtsfragen zu prüfen, einschließt. Wurde eine Beschwerde von einer Aufsichtsbehörde abgelehnt oder abgewiesen, kann der Beschwerdeführer Klage bei den Gerichten desselben Mitgliedstaats erheben.
Im Zusammenhang mit gerichtlichen Rechtsbehelfen in Bezug auf die Anwendung dieser Verordnung können einzelstaatliche Gerichte, die eine Entscheidung über diese Frage für erforderlich halten, um ihr Urteil erlassen zu können, bzw. müssen einzelstaatliche Gerichte in den Fällen nach Artikel 267 AEUV den Gerichtshof um eine Vorabentscheidung zur Auslegung des Unionsrechts — das auch diese Verordnung einschließt — ersuchen. Wird darüber hinaus der Beschluss einer Aufsichtsbehörde zur Umsetzung eines Beschlusses des Ausschusses vor einem einzelstaatlichen Gericht angefochten und wird die Gültigkeit des Beschlusses des Ausschusses in Frage gestellt, so hat dieses einzelstaatliche Gericht nicht die Befugnis, den Beschluss des Ausschusses für nichtig zu erklären, sondern es muss im Einklang mit Artikel 267 AEUV in der Auslegung des Gerichtshofs den Gerichtshof mit der Frage der Gültigkeit befassen, wenn es den Beschluss für nichtig hält. Allerdings darf ein einzelstaatliches Gericht den Gerichtshof nicht auf Anfrage einer natürlichen oder juristischen Person mit Fragen der Gültigkeit des Beschlusses des Ausschusses befassen, wenn diese Person Gelegenheit hatte, eine Klage auf Nichtigerklärung dieses Beschlusses zu erheben — insbesondere wenn sie unmittelbar und individuell von dem Beschluss betroffen war –, diese Gelegenheit jedoch nicht innerhalb der Frist gemäß Artikel 263 AEUV genutzt hat.

(144) Hat ein mit einem Verfahren gegen die Entscheidung einer Aufsichtsbehörde befasstes Gericht Anlass zu der Vermutung, dass ein dieselbe Verarbeitung betreffendes Verfahren — etwa zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter oder wegen desselben Anspruchs — vor einem zuständigen Gericht in einem anderen Mitgliedstaat anhängig ist, so sollte es mit diesem Gericht Kontakt aufnehmen, um sich zu vergewissern, dass ein solches verwandtes Verfahren existiert. Sind verwandte Verfahren vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene Gericht das Verfahren aussetzen oder sich auf Anfrage einer Partei auch zugunsten des zuerst angerufenen Gerichts für unzuständig erklären, wenn dieses später angerufene Gericht für die

betreffenden Verfahren zuständig ist und die Verbindung von solchen verwandten Verfahren nach seinem Recht zulässig ist. Verfahren gelten als miteinander verwandt, wenn zwischen ihnen eine so enge Beziehung gegeben ist, dass eine gemeinsame Verhandlung und Entscheidung geboten erscheint, um zu vermeiden, dass in getrennten Verfahren einander widersprechende Entscheidungen ergehen.

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

(146) Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.

(147) Soweit in dieser Verordnung spezifische Vorschriften über die Gerichtsbarkeit — insbesondere in Bezug auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter — enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates (13) enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.

(148) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des

Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(149) Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, festlegen können. Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.

(150) Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.

(151) Nach den Rechtsordnungen Dänemarks und Estlands sind die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig. Die Vorschriften über die Geldbußen können so angewandt werden, dass die Geldbuße in Dänemark durch die zuständigen nationalen Gerichte als Strafe und in Estland durch die Aufsichtsbehörde im Rahmen eines Verfahrens bei Vergehen verhängt wird, sofern eine solche Anwendung der Vorschriften in diesen Mitgliedstaaten die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen hat. Daher sollten die zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen. In jeden Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.

(152) Soweit diese Verordnung verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen diese Verordnung — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht. Es sollte im Recht der Mitgliedstaaten geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.

(153) Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die

Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und Kohärenz und besondere Datenverarbeitungssituationen erlassen. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das Recht des Mitgliedstaats angewendet werden, dem der Verantwortliche unterliegt. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.

(154) Diese Verordnung ermöglicht es, dass bei ihrer Anwendung der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten berücksichtigt wird. Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden. Personenbezogene Daten in Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Stelle befinden, sollten von dieser Behörde oder Stelle öffentlich offengelegt werden können, sofern dies im Unionsrecht oder im Recht der Mitgliedstaaten, denen sie unterliegt, vorgesehen ist. Diese Rechtsvorschriften sollten den Zugang der Öffentlichkeit zu amtlichen Dokumenten und die Weiterverwendung von Informationen des öffentlichen Sektors mit dem Recht auf Schutz personenbezogener Daten in Einklang bringen und können daher die notwendige Übereinstimmung mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung regeln. Die Bezugnahme auf Behörden und öffentliche Stellen sollte in diesem Kontext sämtliche Behörden oder sonstigen Stellen beinhalten, die vom Recht des jeweiligen Mitgliedstaats über den Zugang der Öffentlichkeit zu Dokumenten erfasst werden. Die Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates (14) lässt das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des Rechts der Mitgliedstaaten unberührt und beeinträchtigt diesen in keiner Weise, und sie bewirkt insbesondere keine Änderung der in dieser Verordnung dargelegten Rechte und Pflichten. Insbesondere sollte die genannte Richtlinie nicht für Dokumente gelten, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nicht oder nur eingeschränkt zugänglich sind, oder für Teile von Dokumenten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, bei denen Rechtsvorschriften vorsehen, dass ihre Weiterverwendung nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist.

(155) Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

(156) Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken sollte geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung unterliegen. Mit diesen Garantien sollte sichergestellt werden, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere der Grundsatz der Datenminimierung gewährleistet wird. Die Weiterverarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder

historischen Forschungszwecken oder zu statistischen Zwecken erfolgt erst dann, wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen (wie z. B. die Pseudonymisierung von personenbezogenen Daten). Die Mitgliedstaaten sollten geeignete Garantien in Bezug auf die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorsehen. Es sollte den Mitgliedstaaten erlaubt sein, unter bestimmten Bedingungen und vorbehaltlich geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen in Bezug auf die Informationsanforderungen sowie der Rechte auf Berichtigung, Löschung, Vergessenwerden, zur Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie auf Widerspruch bei der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorzusehen. Im Rahmen der betreffenden Bedingungen und Garantien können spezifische Verfahren für die Ausübung dieser Rechte durch die betroffenen Personen vorgesehen sein — sofern dies angesichts der mit der spezifischen Verarbeitung verfolgten Zwecke angemessen ist — sowie technische und organisatorische Maßnahmen zur Minimierung der Verarbeitung personenbezogener Daten im Hinblick auf die Grundsätze der Verhältnismäßigkeit und der Notwendigkeit. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken sollte auch anderen einschlägigen Rechtsvorschriften, beispielsweise für klinische Prüfungen, genügen.

(157) Durch die Verknüpfung von Informationen aus Registern können Forscher neue Erkenntnisse von großem Wert in Bezug auf weit verbreiteten Krankheiten wie Herz-Kreislauferkrankungen, Krebs und Depression erhalten. Durch die Verwendung von Registern können bessere Forschungsergebnisse erzielt werden, da sie auf einen größeren Bevölkerungsanteil gestützt sind. Im Bereich der Sozialwissenschaften ermöglicht die Forschung anhand von Registern es den Forschern, entscheidende Erkenntnisse über den langfristigen Zusammenhang einer Reihe sozialer Umstände zu erlangen, wie Arbeitslosigkeit und Bildung mit anderen Lebensumständen. Durch Register erhaltene Forschungsergebnisse bieten solide, hochwertige Erkenntnisse, die die Basis für die Erarbeitung und Umsetzung wissensgestützter politischer Maßnahmen darstellen, die Lebensqualität zahlreicher Menschen verbessern und die Effizienz der Sozialdienste verbessern können. Zur Erleichterung der wissenschaftlichen Forschung können daher personenbezogene Daten zu wissenschaftlichen Forschungszwecken verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt sind.

(158) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu Archivzwecken gelten, wobei darauf hinzuweisen ist, dass die Verordnung nicht für verstorbene Personen gelten sollte. Behörden oder öffentliche oder private Stellen, die Aufzeichnungen von öffentlichem Interesse führen, sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sein, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen. Es sollte den Mitgliedstaaten ferner erlaubt sein vorzusehen, dass personenbezogene Daten zu Archivzwecken weiterverarbeitet werden, beispielsweise im Hinblick auf die Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen, Völkermord, Verbrechen gegen die Menschlichkeit, insbesondere dem Holocaust, und Kriegsverbrechen.

(159) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gelten. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Darüber hinaus sollte sie dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im

öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken zu genügen, sollten spezifische Bedingungen insbesondere hinsichtlich der Veröffentlichung oder sonstigen Offenlegung personenbezogener Daten im Kontext wissenschaftlicher Zwecke gelten. Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten.

(160) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu historischen Forschungszwecken gelten. Dazu sollte auch historische Forschung und Forschung im Bereich der Genealogie zählen, wobei darauf hinzuweisen ist, dass diese Verordnung nicht für verstorbene Personen gelten sollte.

(161) Für die Zwecke der Einwilligung in die Teilnahme an wissenschaftlichen Forschungstätigkeiten im Rahmen klinischer Prüfungen sollten die einschlägigen Bestimmungen der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates (15) gelten.

(162) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu statistischen Zwecken gelten. Das Unionsrecht oder das Recht der Mitgliedstaaten sollte in den Grenzen dieser Verordnung den statistischen Inhalt, die Zugangskontrolle, die Spezifikationen für die Verarbeitung personenbezogener Daten zu statistischen Zwecken und geeignete Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Sicherstellung der statistischen Geheimhaltung bestimmen. Unter dem Begriff „statistische Zwecke“ ist jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen. Diese statistischen Ergebnisse können für verschiedene Zwecke, so auch für wissenschaftliche Forschungszwecke, weiterverwendet werden. Im Zusammenhang mit den statistischen Zwecken wird vorausgesetzt, dass die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.

(163) Die vertraulichen Informationen, die die statistischen Behörden der Union und der Mitgliedstaaten zur Erstellung der amtlichen europäischen und der amtlichen nationalen Statistiken erheben, sollten geschützt werden. Die europäischen Statistiken sollten im Einklang mit den in Artikel 338 Absatz 2 AEUV dargelegten statistischen Grundsätzen entwickelt, erstellt und verbreitet werden, wobei die nationalen Statistiken auch mit dem Recht der Mitgliedstaaten übereinstimmen müssen. Die Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates (16) enthält genauere Bestimmungen zur Vertraulichkeit europäischer Statistiken.

(164) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten durch Rechtsvorschriften regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen. Dies berührt nicht die bestehenden Verpflichtungen der Mitgliedstaaten zum Erlass von Vorschriften über das Berufsgeheimnis, wenn dies aufgrund des Unionsrechts erforderlich ist.

(165) Im Einklang mit Artikel 17 AEUV achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.

(166) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen. Delegierte Rechtsakte sollten insbesondere in Bezug auf die für Zertifizierungsverfahren geltenden Kriterien und Anforderungen, die durch

standardisierte Bildsymbole darzustellenden Informationen und die Verfahren für die Bereitstellung dieser Bildsymbole erlassen werden. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt. Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission gewährleisten, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat gleichzeitig, rechtzeitig und auf angemessene Weise übermittelt werden.

(167) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden. In diesem Zusammenhang sollte die Kommission besondere Maßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen erwägen.

(168) Für den Erlass von Durchführungsrechtsakten bezüglich Standardvertragsklauseln für Verträge zwischen Verantwortlichen und Auftragsverarbeitern sowie zwischen Auftragsverarbeitern; Verhaltensregeln; technische Standards und Verfahren für die Zertifizierung; Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland, einem Gebiet oder bestimmten Sektor dieses Drittlands oder in einer internationalen Organisation; Standardschutzklauseln; Formate und Verfahren für den Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden im Hinblick auf verbindliche interne Datenschutzvorschriften; Amtshilfe; sowie Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollte das Prüfverfahren angewandt werden.

(169) Die Kommission sollte sofort geltende Durchführungsrechtsakte erlassen, wenn anhand vorliegender Beweise festgestellt wird, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau gewährleistet, und dies aus Gründen äußerster Dringlichkeit erforderlich ist.

(170) Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines gleichwertigen Datenschutzniveaus für natürliche Personen und des freien Verkehrs personenbezogener Daten in der Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(171) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

(172) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 7. März 2012 (17) eine Stellungnahme abgegeben.

(173) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (18) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie

entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten