



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

5455/16

---

**Interinstitutionelles Dossier:**  
2012/0011 (COD)

---

**DATAPROTECT 3**  
**JAI 44**  
**MI 27**  
**DIGIT 2**  
**DAPIX 13**  
**FREMP 5**  
**COMIX 39**  
**CODEC 55**

### **I/A-PUNKT-VERMERK**

---

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Vordok.:	15321/15
Betr.:	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) [erste Lesung] – Politische Einigung

---

### **EINLEITUNG**

1. Die Kommission hat am 25. Januar 2012 ein umfassendes Datenschutzpaket vorgeschlagen, das aus Folgendem besteht:
  - dem vorgenannten Vorschlag für eine Datenschutz-Grundverordnung, welche die Datenschutzrichtlinie von 1995 (ehemalige erste Säule) ersetzen soll;
  - einen Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, welche den Datenschutz-Rahmenbeschluss von 2008 (ehemalige dritte Säule) ersetzen soll.

2. Ziel der Datenschutz-Grundverordnung ist es, die Datenschutzrechte natürlicher Personen zu stärken und den freien Verkehr personenbezogener Daten im digitalen Binnenmarkt, auch durch eine Reduzierung des Verwaltungsaufwands, zu erleichtern.
3. Das Europäische Parlament hat seinen Standpunkt in erster Lesung zu der vorgeschlagenen Datenschutz-Grundverordnung am 12. März 2014 festgelegt (Dok. 7427/14).
4. Der Rat hat am 15. Juni 2015 eine allgemeine Ausrichtung (Dok. 9565/15) zu der Datenschutz-Grundverordnung festgelegt und damit dem Vorsitz ein Verhandlungsmandat zur Aufnahme von Trilog mit dem Europäischen Parlament erteilt.
5. Nach zehn Trilog, die von Juni 2015 an stattfanden, haben der Vorsitz und die Vertreter des Europäischen Parlaments, die von der Kommission unterstützt wurden, Einvernehmen über einen Gesamtkompromisstext erzielt.
6. Der Ausschuss der Ständigen Vertreter hat auf seiner Tagung vom 16. Dezember 2015 den aus dem Trilog vom 15. Dezember 2015 hervorgegangenen Text gebilligt.
7. Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments hat am 17. Dezember 2015 in einer außerordentlichen Sitzung über den im Trilog vereinbarten Text abgestimmt. Am selben Tag ist der Präsident des Ausschusses der Ständigen Vertreter mit einem Schreiben des Vorsitzenden des LIBE-Ausschusses (Dok. 15323/15) darüber unterrichtet worden, dass dieser dem LIBE-Ausschuss und anschließend dem Plenum empfehlen werde, die im Trilog erzielte Einigung, vorbehaltlich der Prüfung durch die Rechts- und Sprachsachverständigen, ohne Abänderungen zu billigen.
8. Der AStV hat den Text auf seiner Tagung vom 18. Dezember 2015 im Hinblick auf eine Einigung bestätigt (Dok. 15321/15).
9. Der Ausschuss der Ständigen Vertreter wird ersucht, dass er dem Rat empfiehlt, eine politische Einigung über den in der Anlage enthaltenen Text der Datenschutz-Grundverordnung zu erzielen.

**VERORDNUNG (EU) 2016/XXX  
DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

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

**(Text von Bedeutung für den EWR)**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –  
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf  
Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses<sup>1</sup>,

nach Stellungnahme des Ausschusses der Regionen<sup>2</sup>,

nach Stellungnahme des Europäischen Datenschutzbeauftragten<sup>3</sup>,

gemäß dem ordentlichen Gesetzgebungsverfahren<sup>4</sup>,

---

<sup>1</sup> [XXX]

<sup>2</sup> [XXX]

<sup>3</sup> [XXX]

<sup>4</sup> Standpunkt des Europäischen Parlaments vom 14. März 2014 und Beschluss des Rates vom  
[XXX].

in Erwägung nachstehender Gründe:

- (1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Die Datenverarbeitung sollte zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen der Menschen beitragen.
- (3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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.
- (3a) 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 Grundsätzen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere mit dem Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, dem Recht auf Schutz personenbezogener Daten, der Gedanken-, Gewissens- und Religionsfreiheit, der Freiheit der Meinungsäußerung und der Informationsfreiheit, der unternehmerischen Freiheit, dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren sowie mit der Achtung der Vielfalt der Kulturen, Religionen und Sprachen.

- (4) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs geführt. Der unionsweite Datenaustausch zwischen öffentlichen und privaten Akteuren einschließlich Einzelpersonen, 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.
- (5) Der rasche technologische Fortschritt und die Globalisierung stellen den Datenschutz vor neue Herausforderungen. Das Ausmaß von Datenaustausch und Datenerhebung hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass Privatwirtschaft und Staat im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend werden auch private Informationen öffentlich weltweit zugänglich gemacht. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Datenverkehr innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei gleichzeitig ein hohes Datenschutzniveau zu gewährleisten ist.
- (6) Diese Entwicklungen erfordern einen soliden, kohärenteren und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, um eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Jede Person sollte die Kontrolle über ihre eigenen Daten besitzen, und private Nutzer, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.
- (6a) Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Bestandteile der Verordnung in ihre jeweiligen nationalen Rechtsvorschriften aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.

- (7) 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 und in der Öffentlichkeit die Meinung weit verbreitet ist, dass speziell im Internet der Datenschutz nicht immer gewährleistet ist. Unterschiede beim Schutzniveau für die Rechte und Freiheiten von Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, kann den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.
- (8) Um ein gleichmäßiges und hohes Datenschutzniveau für den Einzelnen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit 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 für die Verarbeitung 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 darüber hinaus einen gewissen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung sensibler Daten. Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände spezifischer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

- (9) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine Stärkung und Präzisierung der Rechte der betroffenen Personen sowie eine Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, aber ebenso gleiche Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.
- (10) Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien **Verkehr** solcher Daten zu erlassen.
- (11) Damit in der Union ein gleichmäßiges Datenschutzniveau für den Einzelnen gewährleistet ist und Unterschiede, die den freien Datenverkehr im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die überall in der Union für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, den Einzelnen mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die für die Verarbeitung 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. Damit der Binnenmarkt reibungslos funktioniert, sollte der freie **Verkehr** personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten werden. Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine Reihe von Ausnahmen. 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 die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 maßgebend sein.

- (12) Der durch diese Verordnung gewährte Schutz betrifft die Verarbeitung personenbezogener Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts. Juristische Personen und insbesondere als juristische Person gegründete Unternehmen, deren Daten, zum Beispiel Name, Rechtsform oder Kontaktdaten, verarbeitet werden, sollten sich nicht auf diese Verordnung berufen können.
- (13) Der Schutz natürlicher Personen sollte technologieneutral sein und nicht von den verwendeten Verfahren abhängen, da andernfalls das Risiko einer Umgehung der Vorschriften groß wäre. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten vom Anwendungsbereich der Verordnung ausgenommen werden.
- (14) Diese Verordnung behandelt weder Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Datenverkehrs im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten, noch die von den Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchgeführte Verarbeitung personenbezogener Daten.

- (14a) Die Verordnung (EG) Nr. 45/2001 gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsinstrumente der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der 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.
- (15) Diese Verordnung sollte nicht für die Verarbeitung von personenbezogenen Daten gelten, 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 und familiäre Tätigkeiten könnten auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher persönlichen und familiären Tätigkeiten gelten. Für die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen, sollte die Verordnung jedoch gelten.

(16) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, sowie der freie Verkehr dieser Daten sind in einem eigenen EU-Rechtsinstrument geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung verwendet werden, dem spezifischeren EU-Instrument (Richtlinie XX/YYYY) unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie XX/YYY mit anderen Aufgaben betrauen, die nicht zwangsläufig zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt, als sie in den Geltungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, können die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen, um die Anwendung der Vorschriften der Datenschutz-Grundverordnung 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 Einrichtungen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen gesetzlich 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, Untersuchung, Aufdeckung, und Verfolgung von Straftaten oder die Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt, zählen. Dies ist beispielsweise für die Bekämpfung der Geldwäsche oder die Arbeit kriminaltechnischer Labors von Bedeutung.

- (16a) Die Verordnung gilt zwar auch 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 in ihrer gerichtlichen Eigenschaft zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge können besondere Stellen im Justizsystem des Mitgliedstaats betraut werden, die insbesondere die Einhaltung der Vorschriften dieser Verordnung kontrollieren, die Sensibilisierung von Richtern und Staatsanwälten für ihre Pflichten aus dieser Verordnung fördern und Beschwerden in Bezug auf eine derartige Datenverarbeitung bearbeiten sollten.
- (17) Die vorliegende Verordnung sollte die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates und speziell die Vorschriften der Artikel 12 bis 15 zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste nicht berühren. Die genannte Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt.
- (18) (...)
- (19) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

- (20) Damit einer Person der gemäß dieser Verordnung gewährleistete Schutz nicht vorenthalten wird, sollte die Verarbeitung personenbezogener Daten von in der Union aufhältigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten. Um festzustellen, ob dieser für die Verarbeitung Verantwortliche oder Auftragsverarbeiter in der Union aufhältigen betroffenen Personen Waren oder Dienstleistungen anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten. Während die bloße Zugänglichkeit der Website des für die Verarbeitung Verantwortlichen oder eines Vermittlers in der Union oder einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der für die Verarbeitung 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, und/oder die Erwähnung von in der Union aufhältigen Kunden oder Nutzern darauf hindeuten, dass der für die Verarbeitung Verantwortliche beabsichtigt, diesen betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten.
- (21) Die Verarbeitung personenbezogener Daten von in der Union aufhältigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung 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 Europäischen 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 Datenverarbeitungstechniken, durch die von einer 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.
- (22) Ist nach internationalem Recht das innerstaatliche 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 für die Verarbeitung Verantwortlichen Anwendung finden.

- (23) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbar natürliche Person beziehen. Einer Pseudonymisierung unterzogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine bestimmbar natürliche Person betrachtet werden. Um festzustellen, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach genutzt werden, um die Person direkt oder indirekt zu identifizieren, wie beispielsweise das Herausgreifen. Bei Prüfung der Frage, ob Mittel nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei sowohl die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine bestimmte oder bestimmbar natürliche Person beziehen, oder 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 und für Forschungszwecke.
- (23aa) Diese Verordnung sollte nicht für die Daten Verstorbener gelten. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der Daten Verstorbener vorsehen.
- (23a) Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der "Pseudonymisierung" im verfügbaren Teil dieser Verordnung sollen somit andere Datenschutzmaßnahmen nicht ausgeschlossen werden.
- (23b) (...)
- (23c) Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse ermöglichen, bei demselben für die Verarbeitung 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. Als für die Verarbeitung Verantwortlicher, der die Daten verarbeitet, gelten auch befugte Personen bei demselben für die Verarbeitung Verantwortlichen.

- (24) Dem Nutzer 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 Personen zu erstellen und sie zu identifizieren.
- (24c neu) Behörden, an die Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags weitergegeben werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, gelten nicht als Empfänger, wenn sie Daten erhalten, die für die Durchführung – gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten – eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Weitergabe, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateien betreffen oder zur Verknüpfung von Dateien führen. Die Verarbeitung dieser Daten durch die genannten Behörden sollte im Einklang mit den gemäß den Zwecken der Verarbeitung geltenden Datenschutzvorschriften erfolgen.
- (25) Die Einwilligung sollte durch eine eindeutige Handlung erfolgen, mit der ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen, auch elektronischen, oder mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch jede sonstige Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigendes Einverständnis, standardmäßig 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 sämtliche 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, in dessen Bereitstellung eingewilligt wird, erfolgen.

- (25aa) Oftmals kann der Zweck der Datenverarbeitung für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Datenerhebung nicht vollständig angegeben werden. Daher sollten betroffene Personen ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung geben können, wenn die anerkannten ethischen Standards der wissenschaftlichen Forschung eingehalten werden. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.
- (25a) Als genetische Daten sollten personenbezogene Daten über die ererbten oder erworbenen genetischen Merkmale eines Menschen gelten, die aus der Analyse einer biologischen Probe des betreffenden Menschen, insbesondere durch DNA- oder RNA-Analyse oder Analyse eines anderen Elements, durch die entsprechende Informationen erlangt werden können, gewonnen werden.
- (26) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den bisherigen, derzeitigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen; dazu gehören auch Informationen über die Person, die im Zuge der Vormerkung zur Erbringung und der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU an die Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer bestimmten Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder einem In-Vitro-Diagnose-Test stammen.

(27) Die Hauptniederlassung des für die Verarbeitung 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 für die Verarbeitung Verantwortlichen in der Union getroffen werden. In diesem Fall sollte die letztgenannte als Hauptniederlassung gelten. Zur Bestimmung der Hauptniederlassung eines für die Verarbeitung Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke 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 solchen Niederlassung. 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 für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter betroffen, so sollte die Aufsichtsbehörde des Mitgliedstaats, in dem der für die Verarbeitung Verantwortliche seine Hauptniederlassung hat, die zuständige federführende Aufsichtsbehörde bleiben, doch sollte die Aufsichtsbehörde des Auftragsverarbeiters als betroffene Aufsichtsbehörde betrachtet werden und 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 für die Verarbeitung 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.

- (28) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund 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 zentrales Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, bildet zusammen mit diesen eine Einheit, die als "Unternehmensgruppe" behandelt werden kann.
- (29) Die personenbezogenen Daten von Kindern müssen besonderen Schutz genießen, da Kinder sich der Risiken, Folgen, Vorsichtsmaßnahmen und ihrer Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften. Dies betrifft insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

(30) Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für die betroffenen Personen sollte erkennbar sein, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die Daten verarbeitet werden und künftig noch verarbeitet werden sollen. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dies gilt insbesondere für die Informationen über die Identität des für die Verarbeitung Verantwortlichen und die Zwecke der Verarbeitung und für sonstige Informationen, die eine faire und transparente Verarbeitung gewährleisten, bei der die betroffenen Personen und ihr Recht, eine Bestätigung und Mitteilung darüber zu erhalten, dass sie betreffende personenbezogene Daten verarbeitet werden, geachtet werden. Die betroffenen Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die besonderen Zwecke, zu denen die Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Datenerhebung feststehen. Die Daten sollten dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Maß beschränkt sein; dies heißt insbesondere, dass die Speicherfrist 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 Daten nicht länger als nötig gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unzutreffende oder unvollständige 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.

- (31) Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen, erforderlich ist.
- (31a) Wann immer sich diese Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme bezieht, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats; die entsprechenden Rechtsgrundlagen oder Gesetzgebungsmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte gefordert.
- (32) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der für die Verarbeitung Verantwortliche beweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderem Zusammenhang sollten Vorkehrungen getroffen werden, die sicherstellen, dass die betroffene Person weiß, dass und wozu sie ihre Einwilligung erteilt. Im Einklang mit der Richtlinie 93/13/EWG des Rates<sup>1</sup> sollte eine vom für die Verarbeitung 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 für die Verarbeitung Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen; es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung ohne Zwang gegeben hat, wenn sie eine echte Wahlfreiheit hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden.
- (33) (...)

- (34) Um sicherzustellen, dass die Einwilligung ohne Zwang erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung ohne Zwang gegeben wurde, keine rechtliche Handhabe liefern. Die Einwilligung gilt nicht als ohne Zwang erteilt, wenn zu verschiedenen Datenverarbeitungsvorgängen 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 gemacht wird, obwohl dies für diese Erfüllung nicht erforderlich ist.
- (35) Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.
- (35a) (...)
- (36) Erfolgt die Verarbeitung durch den für die Verarbeitung 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 nationalen Recht eines Mitgliedstaats bestehen. Mit dieser Verordnung wird nicht verlangt, dass für jede einzelne Verarbeitung ein spezifisches Gesetz erforderlich ist. Ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge kann ausreichend sein, wenn die Verarbeitung aufgrund einer dem für die Verarbeitung 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 dieser Rechtsgrundlage die allgemeinen Bedingungen der Verordnung zur Regelung der Rechtmäßigkeit der Datenverarbeitung präzisiert und könnte darin festgelegt werden, wie der für die Verarbeitung Verantwortliche zu bestimmen ist, welche Art von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen die Daten weitergegeben, 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 für die Verarbeitung 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 eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln soll, sofern dies durch ein öffentliches Interesse gerechtfertigt ist, etwa weil es um gesundheitliche Belange, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, geht.

- (37) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen 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 Datenverarbeitung 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.
- (38) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines für die Verarbeitung Verantwortlichen, auch eines für die Verarbeitung Verantwortlichen, an den die Daten weitergegeben 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 ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn ein relevantes und angemessenes Verhältnis zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des für die Verarbeitung 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 Datenerhebung 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 für die Verarbeitung Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Gesetz die Rechtsgrundlage für die Verarbeitung von Daten durch Behörden zu schaffen, sollte dieser Rechtfertigungsgrund nicht bei Verarbeitungen durch Behörden greifen, 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 für die Verarbeitung Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

- (38a) Für die Verarbeitung Verantwortliche, die Teil einer Unternehmensgruppe oder einer Einrichtung sind, die einer zentralen Stelle zugeordnet ist, 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.
- (39) Die Verarbeitung von Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern ("Denial of access"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

(40) Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Datenerhebung. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung 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 oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke sollte als konformer 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 sich zu vergewissern, dass ein Zweck der Weiterverarbeitung mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbar ist, sollte der für die Verarbeitung Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die 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 ihrem Verhältnis zu dem für die Verarbeitung 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 einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der für die Verarbeitung Verantwortliche die 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. Der Hinweis des für die Verarbeitung Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der relevanten 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 für die Verarbeitung Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des für die Verarbeitung Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

(41) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, bedürfen eines besonderen Schutzes, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese Daten sollten auch personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Tatsache, dass in dieser Verordnung der Begriff "rassische Herkunft" verwendet wird, nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern wird nicht systematisch eine Verarbeitung sensibler Daten darstellen, 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 Person ermöglichen. Derartige 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 hoheitlicher Gewalt, die dem für die Verarbeitung Verantwortlichen übertragen wurde, möglich ist. Außer 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 unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder im Bedarfsfall ausdrücklich vorgesehen werden, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.

(42) Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien sollten auch erlaubt sein, wenn sie im Recht der Union oder der Mitgliedstaaten vorgesehen sind, und – vorbehaltlich angemessener Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte – wenn dies durch ein öffentliches Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von Daten auf dem Gebiet des Arbeitsrechts und des Rechts des Sozialschutzes einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Dies kann wegen gesundheitlicher Belange geschehen, wie die Gewährleistung der öffentlichen Gesundheit und die Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sichergestellt werden soll, oder wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken oder wissenschaftlichen und historischen Forschungszwecken oder statistischen Zwecken dient. Die Verarbeitung solcher Daten sollte zudem ausnahmsweise erlaubt sein, wenn sie erforderlich ist, um rechtliche Ansprüche, sei es in einem Gerichtsverfahren oder sei es in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, zu begründen, geltend zu machen oder zu verteidigen.

(42a) Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes bedürfen, dürfen nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse des Einzelnen wie der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, 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 Versorgung oder Behandlung im Gesundheits- oder Sozialbereich und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen und 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 die 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 nach dem einzelstaatlichen Recht dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und geeignete 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 Datenverkehr innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten.

- (42b) 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 unterliegt geeigneten und besonderen Maßnahmen zum Schutz der persönlichen Rechte und Freiheiten. In diesem Zusammenhang sollte der Begriff "öffentliche Gesundheit" im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie 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 personenbezogener Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.
- (43) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im internationalen Recht verankerte Ziele von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.
- (44) Wenn es in einem Mitgliedstaat zum Funktionieren des demokratischen Systems gehört, dass die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.
- (45) Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen. 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 für die Verarbeitung Verantwortlichen bereitgestellten Online-Dienst anzumelden – einschließen.

- (46) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich 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 bestimmte Situationen wie etwa Werbung im Internet, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer kindgerechten Sprache erfolgen.
- (47) Es gilt, die Modalitäten festzulegen, die es einer betroffenen Person ermöglichen, die ihr nach dieser Verordnung zustehenden Rechte wahrzunehmen, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere den Zugang zu Daten oder deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der für die Verarbeitung Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, insbesondere wenn die personenbezogenen Daten elektronisch verarbeitet werden. Der für die Verarbeitung Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu beantworten und gegebenenfalls zu begründen, warum er ihn ablehnt.
- (48) 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 für die Verarbeitung 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 ein Profil erstellt wird und welche Folgen dies hat. Werden die Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die 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.

- (49) 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 Daten rechtmäßig an einen anderen Empfänger weitergegeben werden dürfen, sollte die betroffene Person bei der erstmaligen Weitergabe der Daten an diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der für die Verarbeitung Verantwortliche, die 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 Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.
- (50) Diese Pflicht erübrigt sich jedoch, wenn die betroffene Person bereits informiert ist oder wenn die Speicherung oder Weitergabe ausdrücklich gesetzlich geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist. Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke oder zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein; als Anhaltspunkt können dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige angemessene Garantien dienen.

- (51) Eine natürliche Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich von der Rechtmäßigkeit der Verarbeitung überzeugen zu können. Dies schließt das Recht natürlicher Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der Daten sind, nach welcher Logik die automatische Datenverarbeitung erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit kann der für die Verarbeitung Verantwortliche den Fernzugang zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dabei dürfen die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigt werden. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der für die Verarbeitung Verantwortliche eine große Menge von Informationen über die betroffene Person, so kann er verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.
- (52) Der für die Verarbeitung Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Ein für die Verarbeitung Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.

- (53) Eine natürliche 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 Recht der Union oder der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn sich die Zwecke, für die die Daten erhoben wurden, erübrigt haben, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist besonders wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die 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 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 für die Verarbeitung Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken oder zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist.
- (54) Um dem "Recht auf Vergessenwerden" im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung so weit gehen, dass ein für die Verarbeitung Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, die Pflicht hat, den für die Verarbeitung Verantwortlichen, die diese Daten verarbeiten, mitzuteilen, dass alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen dieser Daten zu löschen sind. Der für die Verarbeitung Verantwortliche sollte unter Berücksichtigung der verfügbaren Technologie und der ihm zur Verfügung stehenden Mittel angemessene Maßnahmen, auch technischer Art, treffen, um die für die Verarbeitung Verantwortlichen, die die Daten verarbeiten, über den Antrag der betroffenen Person zu unterrichten, damit die vorgenannte Mitteilung sichergestellt ist.

- (54a) Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden oder dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateien sollte die Beschränkung der Verarbeitung personenbezogener Daten grundsätzlich durch technische Mittel so erfolgen, dass die Daten in keiner Weise weiterverarbeitet werden und nicht mehr verändert werden können, wobei in dem System unmissverständlich darauf hingewiesen werden sollte, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde.
- (55) 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 für die Verarbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen für die Verarbeitung Verantwortlichen zu übermitteln. Die für die Verarbeitung Verantwortlichen sollten dazu angehalten werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer ausdrücklichen 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 ausdrücklichen Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen für die Verarbeitung Verantwortliche ausgeübt werden, die Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher insbesondere nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung 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, begründet für den für die Verarbeitung Verantwortlichen nicht die Pflicht, 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 Rechte 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, sofern und solange diese Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die Daten direkt von einem für die Verarbeitung Verantwortlichen einem anderen für die Verarbeitung Verantwortlichen übermittelt werden.

- (56) In Fällen, in denen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden dürfen, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt – die dem für die Verarbeitung Verantwortlichen übertragen wurde, – oder aufgrund des berechtigten Interesses des für die Verarbeitung 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 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.
- (57) 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 muss ausdrücklich auf dieses Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(58) Die betroffene Person sollte das Recht haben, keiner Entscheidung – die 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-Kreditanspruchs oder Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das "Profiling" in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung persönlicher Aspekte in Bezug auf die betroffene Person, insbesondere zwecks Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich Profiling, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Recht der Union oder der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der EU-Institutionen oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem für die Verarbeitung Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem für die Verarbeitung 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 sowie darauf, dass diese Maßnahme kein Kind betreffen darf, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung. 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 unzutreffenden 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 Menschen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Ausrichtung 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.

- (58a) Profiling an sich unterliegt den Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten, wie etwa die Rechtsgrundlage für die Verarbeitung oder die Datenschutzgrundsätze. Der Europäische Datenschutzausschuss sollte die Möglichkeit haben, Leitlinien diesbezüglich herauszugeben.
- (59) Im Recht der Union oder der Mitgliedstaaten können Beschränkungen bestimmter Grundsätze sowie des Rechts auf Unterrichtung, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch, von Entscheidungen, die auf der Erstellung von Profilen beruhen, und von Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person sowie von bestimmten damit zusammenhängenden Pflichten der für die Verarbeitung Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, 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 um sonstige öffentliche Interessen der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen Sozialschutz, öffentliche Gesundheit und humanitäre Hilfe, zu schützen. Diese Beschränkungen müssen mit der Charta der Grundrechte der Europäischen Union und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.
- (60) Die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der für die Verarbeitung Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser 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 persönlichen Rechte und Freiheiten berücksichtigen.

- (60a) Solche Risiken – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Datenverarbeitung hervorgehen, die zu einer physischen, materiellen oder moralischen Schädigung führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden 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 oder Daten über Gesundheit oder Sexualleben oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen 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 ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.
- (60b) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.
- (60c) Anleitungen, wie der für die Verarbeitung 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 Europäischen Datenschutzausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Europäische Datenschutzausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.

- (61) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden persönlichen Rechte und Freiheiten ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und Maßnahmen treffen, die insbesondere dem Grundsatz 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 Datenverarbeitung zu überwachen, und der für die Verarbeitung Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Auslegung, 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 Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die für die Verarbeitung Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte bei öffentlichen Ausschreibungen Rechnung getragen werden.
- (62) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie zur Klärung der Verantwortung und Haftung der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, einschließlich der Fälle, in denen ein für die Verarbeitung Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen für die Verarbeitung Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführt wird.

(63) Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf in der Union aufhältige betroffene Personen beziehen 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 Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 9a ein und bringt unter Berücksichtigung ihrer Art, ihrer Umstände, ihres Umfangs und ihrer Zwecke wahrscheinlich kein Risiko für die persönlichen Rechte und Freiheiten mit sich oder bei dem für die Verarbeitung Verantwortlichen handelt es sich um eine Behörde oder öffentliche Stelle. Der Vertreter sollte im Namen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters tätig werden und den Aufsichtsbehörden als Ansprechpartner dienen. Der für die Verarbeitung 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 und Haftung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters nach Maßgabe dieser Verordnung. Der Vertreter sollte seine Aufgaben entsprechend dem Mandat des für die Verarbeitung Verantwortlichen ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des für die Verarbeitung Verantwortlichen sollte der bestellte Vertreter Durchsetzungsmaßnahmen unterworfen werden.

(63a) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des für die Verarbeitung Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein für die Verarbeitung 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 für die Verarbeitung 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 für die Verarbeitung 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 für die Verarbeitung 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 für die Verarbeitung Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des für die Verarbeitung Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der Daten besteht.

(64) (...)

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

(66) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa die Verschlüsselung, treffen. Diese Maßnahmen müssen 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 des Datensicherheitsrisikos sollten die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Weitergabe von beziehungsweise unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder moralischen Schaden führen könnte.

(66a) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen, besser eingehalten wird, sollte der für die Verarbeitung 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 für die Verarbeitung Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

(67) Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder moralischen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile. Deshalb sollte der für die Verarbeitung Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde ohne unangemessene Verzögerung und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, darüber unterrichten, es sei denn, der für die Verarbeitung 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 führt. Falls die Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(67a) (neu) Natürliche Personen sollten ohne unangemessene Verzögerung benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten führt, damit sie die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden (z. B. Strafverfolgungsbehörden) erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste sie sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen der Datensicherheit zu treffen.

(68) Es ist zu prüfen, ob alle geeigneten technischen und 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 ohne unangemessene Verzögerung 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.

(68a) (...)

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

(70) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat doch keineswegs in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese 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 persönlichen Rechte und Freiheiten mit sich bringen. Bei diesen Arten von Verarbeitungsvorgängen kann es sich um solche handeln, bei denen insbesondere neue Technologien eingesetzt werden oder die neuartig sind und bei denen der für die Verarbeitung Verantwortliche zuvor keine Datenschutz-Folgenabschätzung durchgeführt hat oder die in Anbetracht der seit der ursprünglichen Verarbeitung vergangenen Zeit notwendig geworden sind.

- (70a) In derartigen Fällen sollte der für die Verarbeitung 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 und die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.
- (71) 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 in den Fällen durchgeführt werden, in denen die Daten für das Treffen von Entscheidungen in Bezug auf Einzelpersonen 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 Sicherungsmaßnahmen verarbeitet werden. Gleichmaßen 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 hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, Angehörigen der Gesundheitsberufe oder Anwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

- (72) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht 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 für die Verarbeitung Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.
- (73) Anlässlich des Erlasses des nationalen Gesetzes, 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.
- (74) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen geplanter Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen würde, und ist der für die Verarbeitung 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 von Datenverarbeitungen und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für die betroffenen Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungersuchen 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 Datenverarbeitung gemäß Artikel 33 durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die persönlichen Rechte und Freiheiten geplanten Maßnahmen.

- (74a) Der Auftragsverarbeiter sollte erforderlichenfalls den für die Verarbeitung 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.
- (74b) 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.
- (75) In Fällen, in denen die Verarbeitung durch eine Behörde – mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die in ihrer gerichtlichen Eigenschaft handeln – oder im privaten Sektor durch einen für die Verarbeitung Verantwortlichen erfolgt, dessen Kern-tätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Über-wachung der betroffenen Personen erfordern, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet der Datenschutzvorschriften und -verfahren verfügt, unterstützt werden. Im privaten Sektor bezieht sich die Kerntätigkeit eines für die Verarbeitung Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach der Art der durch-geführten Datenverarbeitungsvorgänge und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personen-bezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des für die Verarbeitung Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.
- (76) Verbände oder andere Vereinigungen, die bestimmte Kategorien von für die Verarbeitung 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 persönlichen Rechte und Freiheiten – die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter bestimmt werden.

- (76a) Bei der Ausarbeitung oder bei der Änderung oder Erweiterung solcher Verhaltensregeln sollten Verbände und oder andere Vereinigungen, die bestimmte Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, die einschlägigen interessierten Kreise, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.
- (77) 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.
- (78) Der grenzüberschreitende 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 garantierte Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an für die Verarbeitung Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn ein Drittland oder eine internationale Organisation ihm bzw. ihr übermittelte personenbezogene Daten an für die Verarbeitung Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weitergibt. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Sie dürfen nur stattfinden, wenn die in Kapitel V festgelegten Bedingungen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.
- (79) Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt. Die Mitgliedstaaten dürfen internationale 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.

- (80) Die Kommission darf mit Wirkung für die gesamte Union feststellen, dass bestimmte Drittländer oder ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an diese Länder übermittelt werden. Die Kommission kann sich – nach Übermittlung einer entsprechenden Benachrichtigung und einer vollständigen Begründung an das Drittland – auch für den Widerruf einer solchen Feststellung entscheiden.
- (81) 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 Zugang zur Justiz 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 bestimmten Verarbeitungsvorgängen und des Geltungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das im Wesentlichen dem innerhalb der Union gewährleisteten Schutzniveau gleichwertig ist, insbesondere in Fällen, in denen Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den europäischen Datenschutzbehörden vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden.

- (81a) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des 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 Europäischen Datenschutzausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.
- (81b) Die Kommission sollte die Wirkungsweise von Feststellungen betreffend das Schutzniveau in einem Drittland oder einem Gebiet oder einem bestimmten Sektor eines Drittlands oder einer internationalen Organisation überwachen; dies gilt auch für Feststellungen, die auf der Grundlage des Artikels 25 Absatz 6 oder des Artikels 26 Absatz 4 der Richtlinie 95/46/EG erlassen werden. 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 relevanten 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 sowie dem Europäischen Parlament und dem Rat über alle relevanten Feststellungen Bericht erstatten.

- (82) Die Kommission kann feststellen, dass ein Drittland oder 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 der Artikel 42 bis 44 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.
- (83) Bei Fehlen eines Angemessenheitsbeschlusses sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese Garantien können darin bestehen, dass auf verbindliche unternehmensinterne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Schutzklauseln sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der EU 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 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.

- (84) Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter keinesfalls daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, einschließlich Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden oder 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 für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.
- (85) 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 genehmigte verbindliche unternehmensinterne Datenschutzvorschriften anwenden dürfen, sofern diese sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.
- (86) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre 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 gesetzlich vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In diesem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.

- (87) Diese 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 einzelstaatlichen Recht 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 Zustimmung zu erteilen, an eine internationale humanitäre Organisation, die erfolgt, um eine nach den Genfer Konventionen obliegende Aufgabe auszuführen und/oder um im Geiste einer getreuen Anwendung des in bewaffneten Konflikten anwendbaren humanitären Völkerrechts tätig zu werden, könnte als aus einem wichtigen Grund im öffentlichen Interesse notwendig oder als im lebenswichtigen Interesse der betroffenen Person liegend erachtet werden.
- (88) 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 für die Verarbeitung Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der für die Verarbeitung Verantwortliche sämtliche Umstände der Datenübermittlung geprüft hat. Der für die Verarbeitung Verantwortliche sollte insbesondere die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland sowie vorgesehene geeignete Garantien zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogener Daten berücksichtigen. Diese Übermittlungen sollten nur in den verbleibenden Fällen möglich sein, in denen keiner der anderen Gründe für die Übermittlung anwendbar ist. Bei wissenschaftlichen und historischen Forschungszwecken oder bei statistischen Zwecken sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Der für die Verarbeitung Verantwortliche sollte die Aufsichtsbehörde und die betroffene Person von der Übermittlung in Kenntnis setzen.

- (89) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Datenschutzniveaus vorliegt, sollte der für die Verarbeitung 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.
- (90) Manche Drittländer erlassen Gesetze, Vorschriften und sonstige Rechtsakte, durch die die Datenverarbeitungstätigkeiten natürlicher und juristischer Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar geregelt werden. Dies kann Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden in Drittländern umfassen, mit denen von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Weitergabe 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 Weitergabe aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist.

- (91) Bei der grenzüberschreitenden Übermittlung personenbezogener Daten außerhalb der Union ist der Einzelne womöglich weniger in der Lage, seine Datenschutzrechte wahrzunehmen und sich insbesondere gegen die unrechtmäßige Nutzung oder Weitergabe dieser Informationen zu schützen. Zugleich können die Aufsichtsbehörden unter Umständen nicht in der Lage sein, Beschwerden nachzugehen oder Untersuchungen in Bezug auf Tätigkeiten im Ausland durchzuführen. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, nicht übereinstimmende Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Daher bedarf es der Förderung einer engeren Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. 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 unter Einhaltung der Bestimmungen dieser Verordnung, einschließlich der Bestimmungen des Kapitels V, zusammenarbeiten.
- (92) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die befugt sind, ihre Aufgaben und Befugnisse völlig unabhängig wahrzunehmen, ist ein wesentliches Element des Schutzes des Einzelnen im Hinblick auf die Verarbeitung personenbezogener Daten. Die Mitgliedstaaten können mehr als eine Aufsichtsbehörde errichten, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.
- (92a) Die Tatsache, dass die Aufsichtsbehörden unabhängig sind, sollte nicht bedeuten, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden können. Sie bedeutet auch nicht, dass die Aufsichtsbehörden keiner gerichtlichen Überprüfung unterzogen werden können.

- (93) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er durch ein Rechtsinstrument sicherstellen, dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Kontaktstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Kommission gewährleistet.
- (94) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über einen eigenen, öffentlichen, jährlichen Haushaltsplan verfügen, der Teil des gesamten Staatshaushalts oder nationalen Haushalts sein kann.
- (95) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten gesetzlich von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder – auf Vorschlag der Regierung, eines Mitglieds der Regierung, des Parlaments oder einer Parlamentskammer – vom Parlament und/oder von der Regierung oder dem Staatsoberhaupt des Mitgliedstaats oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder ihr Amt integer ausüben, von allen mit den Aufgaben ihres Amtes 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 untersteht.

- (95a) 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 für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats, die Verarbeitung personenbezogener Daten durch Behörden oder private Einrichtungen, die im öffentlichen Interesse handeln, Verarbeitungstätigkeiten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben, oder Verarbeitungstätigkeiten eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Europäischen 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 der Verordnung sowie die Förderung der Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließen.
- (96) Die Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen im Hinblick auf die Verarbeitung ihrer Daten zu schützen und den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern. Zu diesem Zweck 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.

- (97) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines für die Verarbeitung 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 für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der für die Verarbeitung 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 Europäische Datenschutzausschuss kann – 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 ausarbeiten, 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 relevanten und begründeten Einspruch darstellt.
- (97a) 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.
- (97b) Der Beschluss sollte von der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden gemeinsam vereinbart werden und an die Hauptniederlassung oder die einzige Niederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters gerichtet sein und für den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter verbindlich sein. Der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter sollte die erforderlichen Maßnahmen treffen, um die Einhaltung dieser Verordnung und die Umsetzung des Beschlusses zu gewährleisten, der der Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters im Hinblick auf die Verarbeitungstätigkeiten in der Union von der federführenden Aufsichtsbehörde mitgeteilt wurde.

- (97c) Jede Aufsichtsbehörde, die nicht als federführende Aufsichtsbehörde fungiert, sollte in örtlichen Fällen zuständig sein, wenn der für die Verarbeitung 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 Arbeitnehmerdaten 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 dem Prinzip der zentralen Kontaktstelle gemäß Artikel 54a regelt oder ob die Aufsichtsbehörde, die sie unterrichtet hat, den Fall auf örtlicher Ebene regeln sollte. Dabei sollte die federführende Aufsichtsbehörde berücksichtigen, ob der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat, damit Beschlüsse gegenüber dem für die Verarbeitung 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 nach dem Prinzip der zentralen Kontaktstelle gemäß Artikel 54a weitestgehend Rechnung tragen sollte.
- (98) Die Vorschriften über die federführende Behörde und das Prinzip der zentralen Kontaktstelle gemäß Artikel 54a sollten keine Anwendung finden, wenn die Verarbeitung durch Behörden oder private Einrichtungen 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.
- (99) (...)

(100) 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 Einzelner, Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse und Genehmigungsbefugnisse und beratende Befugnisse, sowie – unbeschadet der Befugnisse der Strafverfolgungsbehörden nach nationalem Recht – die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und/oder 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 Unionsrecht und nationalem Recht 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 nationalen Verfahrensrecht 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 nationalem Verfahrensrecht nicht ausschließen. Der Erlass eines solchen rechtsverbindlichen Beschlusses setzt voraus, dass er in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, gerichtlich überprüft werden kann.

(101) (...)

(101a) Ist die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, nicht die federführende Aufsichtsbehörde, so sollte die federführende Aufsichtsbehörde im Einklang mit 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.

(101b) Wenn eine andere Aufsichtsbehörde als federführende Aufsichtsbehörde für die Verarbeitungstätigkeiten des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters fungieren sollte, der konkrete Gegenstand einer Beschwerde oder der mögliche Verstoß jedoch nur die Verarbeitungstätigkeiten des für die Verarbeitung 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 die Verordnung darstellen, aufgedeckt hat bzw. auf andere Weise darüber informiert wurde, versuchen, eine gütliche Einigung mit dem für die Verarbeitung 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; oder 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 nationalem Recht bewertet werden muss.

(102) Die Aufklärungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, und an Einzelpersonen, insbesondere im Bildungsbereich, richten.

- (103) 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 binnen eines Monats nach Eingang des Ersuchens bei der ersuchten Aufsichtsbehörde keine Antwort von dieser erhalten hat.
- (104) Jede Aufsichtsbehörde sollte gegebenenfalls an gemeinsamen Maßnahmen von Aufsichtsbehörden teilnehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer festgelegten Frist antworten müssen.
- (105) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) 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.
- (106) Bei Anwendung des Kohärenzverfahrens sollte der Europäische Datenschutzausschuss, 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 Europäischen Datenschutzausschuss sollte auch die Befugnis übertragen werden, im Falle von Streitigkeiten zwischen Aufsichtsbehörden rechtsverbindliche Beschlüsse zu erlassen. Zu diesem Zweck sollte er in klar definierten 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 oder nicht, vertreten, grundsätzlich mit einer Mehrheit von zwei Dritteln seiner Mitglieder rechtsverbindliche Beschlüsse erlassen.

(107) (...)

(108) 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. Daher kann eine Aufsichtsbehörde hinreichend begründete einstweilige Maßnahmen in ihrem Hoheitsgebiet mit einer festgelegten Geltungsdauer von höchstens drei Monaten erlassen.

(109) 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.

(110) Zur Förderung der einheitlichen Anwendung dieser Verordnung sollte der Europäische Datenschutzausschuss als unabhängige Einrichtung der Union eingesetzt werden. Damit der Europäische Datenschutzausschuss seine Ziele erreichen kann, sollte er Rechtspersönlichkeit besitzen. Der Europäische Datenschutzausschuss 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 seinen Beratungen sollte die Kommission ohne Stimmrecht und der Europäische Datenschutzbeauftragte mit spezifischen Stimmrechten teilnehmen. Der Europäische Datenschutzausschuss 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 Europäische Datenschutzausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.

(110a) Der Europäische Datenschutzausschuss sollte von einem Sekretariat unterstützt werden, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird. Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Europäischen Datenschutzausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, sollte diese Aufgaben ausschließlich gemäß den Anweisungen des Vorsitzes des Europäischen Datenschutzausschusses durchführen und diesem Bericht erstatten.

(111) 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 Grundrechtecharta 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 vonnöten sein, sollte die betroffene Person auch hierüber 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.

(112) Betroffene Personen, die sich in ihren Rechten gemäß dieser Verordnung verletzt sehen, sollten das Recht haben, Einrichtungen, Organisationen oder Verbände, die die keinen Erwerbszweck verfolgen, deren satzungsmäßige Ziele von öffentlichem Interesse sind, die im Bereich des Schutzes personenbezogener Daten tätig sind und die nach dem Recht eines Mitgliedstaats gegründet 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 sollten, unabhängig vom Auftrag einer betroffenen Person in dem betreffenden Mitgliedstaat eine eigene Beschwerde einzulegen, und/oder 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 Schadensersatz zu verlangen.

(113) Jede natürliche oder juristische Person hat das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof der Europäischen Union (im Folgenden "Gerichtshof") eine Klage auf Nichtigerklärung eines Beschlusses des Europäischen Datenschutzausschusses 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 Europäischen Datenschutzausschusses einen für die Verarbeitung 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 Europäischen Datenschutzausschusses 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. Dieses Recht umfasst jedoch nicht andere – rechtlich nicht bindende – Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem nationalen Verfahrensrecht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit relevanten Sach- und Rechtsfragen zu prüfen, einschließt. 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 Europäischen Datenschutzausschusses vor einem einzelstaatlichen Gericht angefochten und wird die Gültigkeit des Beschlusses des Europäischen Datenschutzausschusses in Frage gestellt, so hat dieses einzelstaatliche Gericht nicht die Befugnis, den Beschluss des Europäischen Datenschutzausschusses 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 Antrag einer natürlichen oder juristischen Person mit Fragen der Gültigkeit des Beschlusses des Europäischen Datenschutzausschusses 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.

(113a) 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 für die Verarbeitung 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 Verfahren verbundenes Verfahren existiert. Sind miteinander verbundene Verfahren vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene Gericht das Verfahren aussetzen oder sich auf Antrag einer Partei auch zugunsten des zuerst angerufenen Gerichts für unzuständig erklären, wenn dieses für die betreffenden Verfahren zuständig ist und die Verbindung von miteinander verbundenen Verfahren nach seinem Recht zulässig ist. Verfahren gelten als miteinander im Zusammenhang stehend, 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.

(114) (...)

(115) (...)

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

(117) (...)

(118) Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, sollten von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter ersetzt werden, der von seiner Haftung befreit werden sollte, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Europäischen 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. Wird auf eine Verarbeitung Bezug genommen, die mit der vorliegenden Verordnung nicht im Einklang steht, so gilt dies auch für Verarbeitungen, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und nationalen Rechtsvorschriften zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang stehen. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind für die Verarbeitung Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des nationalen Rechts zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder für die Verarbeitung 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 für die Verarbeitung Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte für die Verarbeitung Verantwortliche oder Auftragsverarbeiter anstrengen.

(118a) Soweit in dieser Verordnung spezifische Vorschriften über die Gerichtsbarkeit – insbesondere in Bezug auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter – enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.

(118b) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen und Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls die 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 für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen und Geldbußen sollte es angemessenen Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Grundrechtecharta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(119) Die Mitgliedstaaten können die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, regeln. 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.

(120) 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 Vergehen, 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 der Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden die Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff "Unternehmen" im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden die 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.

(120a) (neu) 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 strafrechtliche Sanktion 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.

- (120a) Soweit diese Verordnung Geldbußen 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. Die Art dieser Sanktionen (strafrechtliche oder verwaltungsrechtliche Sanktionen) sollte im nationalen Recht geregelt werden.
- (121) 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 der Grundrechte der Europäischen Union garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die Mitgliedstaaten sollten deshalb 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 für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit, die Kohärenz und besondere Datenverarbeitungssituationen regeln. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das nationale Recht des Mitgliedstaats angewendet werden, dem der für die Verarbeitung 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.

(121a) Diese Verordnung ermöglicht es, dass bei der Anwendung ihrer Vorschriften 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 freigegeben werden können, sofern dies in den Rechtsvorschriften der Union oder des Mitgliedstaats, 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 vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors lässt das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des nationalen Rechts 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, deren Weiterverwendung gesetzlich nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist.

(122) (...)

(123) (...)

- (124) 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 gesetzlich oder tarifvertraglich 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.
- (125) Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken sollte angemessenen 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 und historischen Forschungszwecken oder zu statistischen Zwecken erfolgt erst dann, wenn der für die Verarbeitung Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von Daten, bei der die Bestimmung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern angemessene Garantien bestehen (wie z. B. die Pseudonymisierung von Daten). Die Mitgliedstaaten sollten angemessene Garantien in Bezug auf die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken vorsehen. Es sollte den Mitgliedstaaten erlaubt sein, unter bestimmten Bedingungen und bei Bestehen geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen zu den Informationsanforderungen, zur Berichtigung, zur Löschung, zu dem Vergessenwerden, zur Einschränkung der Verarbeitung und zu dem Recht auf Datenübertragbarkeit sowie zu dem Recht auf Widerspruch bei der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen und 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 Versuche, genügen.

(125a)(...)

(125aa) Durch die Verknüpfung von Informationen aus Registern können Forscher neue Erkenntnisse von großem Wert beispielsweise zu weit verbreiteten Krankheiten wie Herz-Kreislaufkrankungen, Krebs, Depression usw. 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 langfristige Auswirkungen einer Reihe sozialer Umstände zu erlangen, wie z. B. Arbeitslosigkeit und Bildung; ferner können diese Informationen mit anderen Lebensumständen verknüpft werden. Auf der Grundlage von Registern erhaltene Forschungsergebnisse bieten solide, hochwertige Erkenntnisse, die die Basis für die Erarbeitung und Umsetzung wissenschaftsgestützter politischer Maßnahmen darstellen, die Lebensqualität zahlreicher Menschen verbessern und die Effizienz der Sozialdienste verbessern können usw. Zur Erleichterung der wissenschaftlichen Forschung können daher personenbezogene Daten zu wissenschaftlichen Forschungszwecken verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Recht der Mitgliedstaaten oder im Unionsrecht festgelegt sind.

(125b) Diese Verordnung sollte daher 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 Einrichtungen, die Aufzeichnungen von öffentlichem Interesse führen, sollten Dienststellen sein, die gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sind, 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 Zwecken der Archivierung 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.

(126) 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 und darüber hinaus dem in Artikel 179 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die 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.

(126a) 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.

(126b) Für die Zwecke der Einwilligung in die Teilnahme an wissenschaftlichen Forschungstätigkeiten im Rahmen klinischer Versuche sollten die einschlägigen Bestimmungen der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates gelten.

(126c) 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 angemessene Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Garantie 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 Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.

(126d) 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 des Vertrags über die Arbeitsweise der Europäischen Union dargelegten statistischen Grundsätzen entwickelt, erstellt und verbreitet werden, wobei die nationalen Statistiken auch mit dem einzelstaatlichen Recht übereinstimmen müssen. Die Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften enthält genauere Bestimmungen zur Vertraulichkeit statistischer Informationen.

- (127) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten gesetzlich regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen. Dies berührt nicht die bestehenden Verpflichtungen der Mitgliedstaaten zum Erlass von Vorschriften über das Berufsgeheimnis, wenn dies aufgrund des Unionsrechts erforderlich ist.
- (128) Im Einklang mit Artikel 17 des Vertrags über die Arbeitsweise der Europäischen Union achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.
- (129) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 2090 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.

(130) Um einheitliche Bedingungen für die Anwendung dieser Verordnung sicherzustellen, 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 vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren<sup>5</sup>, ausgeübt werden. Die Kommission sollte besondere Maßnahmen für Kleinunternehmen sowie kleine und mittlere Unternehmen erwägen.

(131) Für den Erlass von Durchführungsrechtsakten bezüglich Standardvertragsklauseln für Verträge zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern sowie zwischen Auftragsverarbeitern; Verhaltensregeln; technische Standards und Verfahren für die Zertifizierung; Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder Verarbeitungssektor dieses Drittlands oder in einer internationalen Organisation; Standardschutzklauseln; Formate und Verfahren für den Informationsaustausch zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden im Hinblick auf verbindliche unternehmensinterne Datenschutzvorschriften; Amtshilfe; Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss sollte das Prüfverfahren angewandt werden, da es sich um Durchführungsrechtsakte von allgemeiner Tragweite handelt.

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

---

<sup>5</sup> Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ABl. L 55 vom 28.2.2011, S. 13.

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

(134) 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 für die Verarbeitung Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen/Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

(135) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG festgelegten spezifischen Pflichten, die dasselbe Ziel verfolgen, unterliegen einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Um das Verhältnis zwischen dieser Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen worden ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit der Verordnung zu gewährleisten –

(136) (...)

(137) (...)

(138) (...)

(139) (...)

# KAPITEL I

## ALLGEMEINE BESTIMMUNGEN

### *Artikel 1*

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

1. Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
2. Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
  - 2a. (...)
3. Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

### *Artikel 2*

#### ***Sachlicher Anwendungsbereich***

1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.
2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird
  - (a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt,
  - (b) (...)
  - (c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union fallen,
  - (d) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

- (e) durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt.
- 2a. Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsinstrumente der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 90a an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.
3. Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

### *Artikel 3*

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

1. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
2. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union aufhältigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung
  - (a) dazu dient, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
  - (b) der Beobachtung ihres Verhaltens dient, soweit ihr Verhalten in der Europäischen Union erfolgt.
3. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der völkerrechtlich dem nationalen Recht eines Mitgliedstaats unterliegt.

## Artikel 4

### **Begriffsbestimmungen**

Im Sinne dieser Verordnung bezeichnet der Ausdruck

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

- (4) "Datei" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
- (5) "für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten bestimmt werden;
- (6) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- (7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden hat im Einklang mit den gemäß den Zwecken der Verarbeitung geltenden Datenschutzvorschriften zu erfolgen;
- (7a) "Dritter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;
- (8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
- (9) "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob zufällig oder unrechtmäßig, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

- (10) "genetische Daten" personenbezogene Daten jedweder Art zu den ererbten oder erworbenen genetischen Merkmalen eines Menschen, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden;
- (11) "biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die die eindeutige Identifizierung dieses Menschen ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
- (12) "Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
- (12a) (...)
- (13) "Hauptniederlassung"
- (a) im Falle eines für die Verarbeitung Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des für die Verarbeitung Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;
- (b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union und, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;
- (14) "Vertreter" jede in der Union niedergelassene natürliche oder juristische Person, die von dem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 25 bestellt wurde und den für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

- (15) "Unternehmen" jede natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
- (16) "Unternehmensgruppe" eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
- (17) "verbindliche unternehmensinterne Datenschutzvorschriften" Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats der Union niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern verpflichtet;
- (18) (...)
- (19) "Aufsichtsbehörde" eine von einem Mitgliedstaat gemäß Artikel 46 eingerichtete unabhängige staatliche Stelle;
- (19a) "betroffene Aufsichtsbehörde" eine Aufsichtsbehörde, die von der Verarbeitung betroffen ist, weil
- (a) der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
  - (b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in diesem Mitgliedstaat hat oder haben kann oder
  - (c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;
- (19b) "grenzüberschreitende Verarbeitung personenbezogener Daten" entweder
- (a) eine Verarbeitung, die im Rahmen der Tätigkeiten von Niederlassungen eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

- (b) eine Verarbeitung, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

(19c) "relevanter und begründeter Einspruch"

einen Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob gegebenenfalls die beabsichtigte Maßnahme gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht. Aus dem Einspruch muss die Tragweite der Risiken, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen, klar hervorgehen;

- (20) "Dienst der Informationsgesellschaft" eine Dienstleistung im Sinne des Artikels 1 Nummer 2 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft;

- (21) "internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

## KAPITEL II

### GRUNDSÄTZE

#### *Artikel 5*

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

1. Personenbezogene Daten müssen
  - (a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");
  - (b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 83 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("Zweckbindung");
  - (c) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("Datenminimierung");
  - (d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden ("Richtigkeit");
  - (e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten vorbehaltlich der Durchführung angemessener technischer und organisatorischer Maßnahmen, die von der Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 83 Absatz 1 verarbeitet werden ("Speicherbegrenzung");

- (eb) in einer Weise verarbeitet werden, die einen angemessenen Schutz der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");
  - (ee) (...)
  - (f) (...)
2. Der für die Verarbeitung Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht").

#### *Artikel 6*

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

1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
- (a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere festgelegte Zwecke gegeben;
  - (b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;
  - (c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
  - (d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
  - (e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

- (f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dies gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

2. (...)

2a. (neu) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung personenbezogener Daten zur Erfüllung von Artikel 6 Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

3. Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e muss festgelegt werden durch

- (a) Rechtsvorschriften der Union oder
- (b) Rechtsvorschriften der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Datenverarbeitung durch den für die Verarbeitung Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die Daten weitergegeben werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, unter anderem für sonstige spezifische Verarbeitungssituationen gemäß Kapitel IX. Die Rechtsvorschriften der Union oder die Rechtsvorschriften der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

- 3a. Beruht die Verarbeitung für einen anderen Zweck als den, zu dem die Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 21 Absatz 1 Buchstaben aa bis g genannten Ziele darstellt, so berücksichtigt der für die Verarbeitung Verantwortliche – um sich zu vergewissern, ob die Verarbeitung für einen anderen Zweck mit dem Zweck, zu dem die Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem
- (a) jede Verbindung zwischen den Zwecken, für die die Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
  - (b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem für die Verarbeitung Verantwortlichen,
  - (c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a verarbeitet werden,
  - (d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
  - (e) das Vorhandensein angemessener Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.
4. (...)
5. (...)

#### *Artikel 7*

#### ***Bedingungen für die Einwilligung***

1. Beruht die Verarbeitung auf einer Einwilligung, muss der für die Verarbeitung Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu der Verarbeitung ihrer personenbezogenen Daten erteilt hat.
- 1a. (...)

2. Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung, mit der die betroffene Person ihre Einwilligung erteilt hat, sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.
3. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
4. Bei der Beurteilung, ob die Einwilligung ohne Zwang erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zur Verarbeitung von Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich ist.

#### *Artikel 8*

#### ***Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft***

1. In den Fällen, in denen Artikel 6 Absatz 1 Buchstabe a zur Anwendung kommt, ist die Verarbeitung personenbezogener Daten eines Kindes, dem direkt Dienste der Informationsgesellschaft angeboten werden, bis zum vollendeten sechzehnten Lebensjahr oder, sofern im Recht eines Mitgliedstaats vorgesehen, bis zu einer niedrigeren Altersgrenze, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf, nur rechtmäßig, wenn und insoweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.
  - 1a. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um in solchen Fällen nachzuprüfen, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

2. Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.
3. (...)
4. (...).

#### *Artikel 9*

#### ***Verarbeitung besonderer Kategorien personenbezogener Daten***

1. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer Person oder Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung ist untersagt.
2. Absatz 1 gilt nicht in folgenden Fällen:
  - (a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach den Rechtsvorschriften der Union oder eines Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, oder
  - (b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht eines Mitgliedstaats, das angemessene Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist, oder
  - (c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich und die betroffene Person ist aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder

- (d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Erwerbszweck im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder
- (e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder
- (f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte in ihrer gerichtlichen Eigenschaft erforderlich, oder
- (g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und geeignete und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines wichtigen öffentlichen Interesses erforderlich, oder
- (h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 4 genannten Bedingungen und Garantien erforderlich, oder
- (hb) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das geeignete und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

- (i) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und geeignete und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 83 Absatz 1 erforderlich.
  - (j) (...)
3. (...)
4. Die in Absatz 1 genannten personenbezogenen Daten können zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.
5. Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder gesundheitlichen Daten betroffen ist.

#### *Artikel 9a*

#### ***Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten***

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

## *Artikel 10*

### ***Verarbeitung, für die eine Bestimmung der betroffenen Person nicht erforderlich ist***

1. Ist für die Zwecke, für die ein für die Verarbeitung Verantwortlicher personenbezogene Daten verarbeitet, die Bestimmung der betroffenen Person durch den für die Verarbeitung Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu bestimmen.
2. Kann der für die Verarbeitung Verantwortliche in derartigen Fällen nachweisen, dass er nicht in der Lage ist, die betroffene Person zu bestimmen, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 18 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Bestimmung ermöglichen.

# KAPITEL III

## RECHTE DER BETROFFENEN PERSON

### ABSCHNITT 1

#### TRANSPARENZ UND MODALITÄTEN

##### *Artikel 11*

##### *Transparente Information und Kommunikation*

1. (...)
2. (...)

##### *Artikel 12*

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

1. Der für die Verarbeitung Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 14 und 14a und alle Mitteilungen gemäß den Artikeln 15 bis 20 und Artikel 32, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls in elektronischer Form. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.
- 1a. Der für die Verarbeitung Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 20. In den in Artikel 10 Absatz 2 genannten Fällen darf sich der für die Verarbeitung Verantwortliche sich nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 20 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu bestimmen.

2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 20 ergriffenen Maßnahmen ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um höchstens weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität des Antrags und der Anzahl von Anträgen erforderlich ist. Kommt es zu einer Fristverlängerung, so wird die betroffene Person innerhalb eines Monats nach Eingang des Antrags über die Gründe für die Verzögerung unterrichtet. Stellt die betroffene Person den Antrag in elektronischer Form, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.
3. Wird der für die Verarbeitung Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.
4. Informationen gemäß den Artikeln 14 und 14a sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 20 und Artikel 32 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall ihrer Häufung – unverhältnismäßigen Anträgen einer betroffenen Person kann der für die Verarbeitung Verantwortliche ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder er kann sich weigern, aufgrund des Antrags tätig zu werden. In diesen Fällen hat der für die Verarbeitung Verantwortliche den Nachweis für den offenkundig unbegründeten oder unverhältnismäßigen Charakter des Antrags zu erbringen.
  - 4a. Hat der für die Verarbeitung Verantwortliche begründete Zweifel an der Identität der Person, die den Antrag gemäß den Artikeln 15 bis 19 stellt, so kann er unbeschadet des Artikels 10 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.
  - 4b. Die Informationen, die den betroffenen Personen gemäß den Artikeln 14 und 14a bereitzustellen sind, 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, müssen sie maschinenlesbar sein.

- 4c. Der Kommission wird die Befugnis übertragen, gemäß Artikel 86 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.
5. (...)
6. (...).

*Artikel 13*

***Rechte gegenüber Empfängern***

(...)

**ABSCHNITT 2**

**INFORMATIONSPFLICHT UND AUSKUNFTSRECHT**

*Artikel 14*

***Informationspflicht bei Erhebung der Daten bei der betroffenen Person***

1. Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
  - (a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters; zusätzlich werden, falls vorhanden, auch die Kontaktdaten des Datenschutzbeauftragten angegeben;
  - (b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung;
  - (c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt werden;

- (d) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
  - (e) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle der in Artikel 42 oder Artikel 43 oder Artikel 44 Absatz 1 Buchstabe h erwähnten Übermittlungen einen Verweis auf die entsprechenden oder geeigneten Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.
- 1a. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:
- (a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
  - (b) ...
  - (c) ...
  - (d) ...
  - (e) das Bestehen eines Rechts auf Auskunft seitens des für die Verarbeitung Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung dieser Daten oder eines Widerspruchsrechts gegen die Verarbeitung dieser Daten sowie des Rechts auf Datenübertragbarkeit;
  - (ea) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
  - (f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- (g) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte;
  - (h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und – zumindest in diesen Fällen – aussagekräftige Informationen über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
- 1b. Beabsichtigt der für die Verarbeitung Verantwortliche, die Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen relevanten Informationen gemäß Absatz 1a zur Verfügung.
2. (...)
3. (...)
4. (...)
5. Die Absätze 1, 1a und 1b finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.
6. (...)
7. (...)
8. (...).

*Artikel 14a*

***Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden***

1. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen Person Folgendes mit:
  - (a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters; zusätzlich werden, falls vorhanden, auch die Kontaktdaten des Datenschutzbeauftragten angegeben;
  - (b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung;
  - (ba) die Kategorien personenbezogener Daten, die verarbeitet werden;
  - (c) (...)
  - (d) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
  - (da) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle der in Artikel 42 oder Artikel 43 oder Artikel 44 Absatz 1 Buchstabe h genannten Übermittlungen einen Verweis auf die entsprechenden oder geeigneten Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.
2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:
  - (b) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
  - (ba) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt werden;

- (c) (...)
  - (e) das Bestehen eines Rechts auf Auskunft seitens des für die Verarbeitung Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung dieser Daten und eines Widerspruchsrechts gegen die Verarbeitung dieser Daten sowie des Rechts auf Datenübertragbarkeit;
  - (ea) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
  - (f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
  - (g) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
  - (h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und – zumindest in diesen Fällen – aussagekräftige Informationen über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
3. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2
- (a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der Daten innerhalb einer angemessenen Frist nach Erlangung der Daten, längstens jedoch innerhalb eines Monats, oder,
  - (b) falls die Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
  - (c) falls die Weitergabe an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.
- 3a. Beabsichtigt der für die Verarbeitung Verantwortliche, die Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen relevanten Informationen gemäß Absatz 2 zur Verfügung.

4. Die Absätze 1 bis 3a finden keine Anwendung, wenn und soweit
- (a) die betroffene Person bereits über die Informationen verfügt oder
  - (b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 83 Absatz 1 genannten Bedingungen und Garantien oder soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele der im öffentlichen Interesse liegenden Archivzwecke oder der wissenschaftlichen und historischen Forschungszwecke oder der statistischen Zwecke unmöglich macht oder ernsthaft beeinträchtigt; in diesen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit, oder
  - (c) die Erlangung oder Weitergabe durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder
  - (d) die Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

#### *Artikel 15*

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

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese Daten und auf folgende Informationen:
- (a) die Verarbeitungszwecke;
  - (b) die Kategorien personenbezogener Daten, die verarbeitet werden;

- (c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern oder bei internationalen Organisationen;
  - (d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
  - (e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung dieser Daten durch den für die Verarbeitung Verantwortlichen oder eines Widerspruchsrechts gegen die Verarbeitung dieser Daten;
  - (f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
  - (g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
  - (h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und – zumindest in diesen Fällen – aussagekräftige Informationen über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
- 1a. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 42 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

- 1b. Der für die Verarbeitung Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der für die Verarbeitung Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag in elektronischer Form, so ist sie auf gängigem elektronischem Wege zu unterrichten, sofern sie nichts anderes angibt.
2. (...)
- 2a. Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.
3. (...)
4. (...).

### **ABSCHNITT 3**

## **BERICHTIGUNG UND LÖSCHUNG**

### *Artikel 16*

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

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung sie betreffender unzutreffender personenbezogener Daten ohne unangemessene Verzögerung zu verlangen. Im Hinblick auf die Zwecke, für die die Daten verarbeitet wurden, hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

## Artikel 17

### **Recht auf Löschung ("Recht auf "Vergessenwerden")**

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten ohne unangemessene Verzögerung gelöscht werden, und der für die Verarbeitung Verantwortliche ist verpflichtet, personenbezogene Daten ohne unangemessene Verzögerung zu löschen, sofern einer der folgenden Gründe zutrifft:
  - (a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
  - (b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.
  - (c) Die betroffene Person legt gemäß Artikel 19 Absatz 1 Widerspruch gegen die Verarbeitung personenbezogener Daten ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 19 Absatz 2 Widerspruch gegen die Verarbeitung ein.
  - (d) Die Daten wurden unrechtmäßig verarbeitet.
  - (e) Die Löschung der Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Recht der Union oder der Mitgliedstaaten erforderlich, dem der für die Verarbeitung Verantwortliche unterliegt.
  - (f) Die Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.
- 1a. (...)
2. (...)

- 2a. Hat der für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.
3. Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung der personenbezogenen Daten erforderlich ist
- (a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
  - (b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung personenbezogener Daten nach dem Recht der Union oder der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;
  - (c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und hb sowie Artikel 9 Absatz 4;
  - (d) für im öffentlichen Interesse liegende Archivzwecke oder wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 83 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele der im öffentlichen Interesse liegenden Archivzwecke oder der wissenschaftlichen und historischen Forschungszwecke oder der statistischen Zwecke unmöglich macht oder ernstlich beeinträchtigt.
  - (e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
4. (...)
5. (...)
6. (...)
7. (...)
8. (...)
9. (...)

*Artikel 17a*

***Recht auf Einschränkung der Verarbeitung***

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, wenn
  - (a) die Richtigkeit der Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen,
  - (ab) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der Daten ablehnt und stattdessen die Einschränkung der Nutzung der Daten beantragt;
  - (b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
  - (c) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 19 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des für die Verarbeitung Verantwortlichen gegenüber denen der betroffenen Person überwiegen.
  
2. Wurde die Verarbeitung personenbezogener Daten gemäß Absatz 1 eingeschränkt, so dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.
  
3. Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem für die Verarbeitung Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

## *Artikel 17b*

### ***Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung***

Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 17a mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

## *Artikel 18*

### ***Recht auf Datenübertragbarkeit***

1. (...)
2. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen ohne Behinderung durch den für die Verarbeitung Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln, sofern
  - (a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
  - (b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.
- 2a. (neu) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die Daten direkt von einem für die Verarbeitung Verantwortlichen einem anderen für die Verarbeitung Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.
- 2a. Die Ausübung dieses Rechts lässt Artikel 17 unberührt. Das Recht gemäß Absatz 2 gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde.

2aa. Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

3. (...)

#### **ABSCHNITT 4**

### **WIDERSPRUCHSRECHT UND AUTOMATISIERTE GENERIERUNG VON EINZELENTSCHEIDUNGEN**

#### *Artikel 19*

#### ***Widerspruchsrecht***

1. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der für die Verarbeitung Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
  2. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung zusammenhängt.
- 2a. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.
- 2b. (neu) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

- 2b. Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mithilfe automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.
- 2aa. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 83 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.
3. (...).

#### *Artikel 20*

##### ***Automatisierte Generierung von Einzelentscheidungen einschließlich Profiling***

1. Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
- 1a. Absatz 1 gilt nicht, wenn die Entscheidung
- (a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich ist oder
  - (b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
  - (c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

- 1b. In den in Absatz 1a Buchstaben a und c genannten Fällen trifft der für die Verarbeitung Verantwortliche geeignete Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des für die Verarbeitung Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.
2. (...)
3. Entscheidungen nach Absatz 1a dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.
4. (...)
5. (...)

## ABSCHNITT 5 BESCHRÄNKUNGEN

### *Artikel 21*

#### ***Beschränkungen***

1. Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 20 und Artikel 32 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 20 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die zu Folgendem dient:
  - (aa) zum Schutz der nationalen Sicherheit;
  - (ab) zur Landesverteidigung;
    - (a) zum Schutz der öffentlichen Sicherheit;
    - (b) zur Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt;
  - (c) zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;
    - (ca) zum Schutz der Unabhängigkeit der Justiz und zum Schutz von Gerichtsverfahren;
    - (d) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;
    - (e) für Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben aa, ab, a, b, c und d genannten Zwecke verbunden sind;

- (f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen;
  - (g) für die Durchsetzung zivilrechtlicher Ansprüche.
2. Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf
- (a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,
  - (b) die Kategorien personenbezogener Daten,
  - (c) den Umfang der vorgenommenen Beschränkungen,
  - (d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Weitergabe;
  - (e) die Angaben zu dem für die Verarbeitung Verantwortlichen oder den Kategorien von für die Verarbeitung Verantwortlichen,
  - (f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,
  - (g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und
  - (h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

# KAPITEL IV FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

## ABSCHNITT 1 ALLGEMEINE PFLICHTEN

### *Artikel 22*

#### *Verantwortung des für die Verarbeitung Verantwortlichen*

1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen durch, um sicherzustellen und den Nachweis dafür erbringen zu können, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden. Diese Maßnahmen werden überprüft und erforderlichenfalls aktualisiert.
2. (...)
- 2a. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den für die Verarbeitung Verantwortlichen umfassen.
- 2b. Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 38 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des für die Verarbeitung Verantwortlichen nachzuweisen.
3. (...)
4. (...)

## Artikel 23

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

1. Unter Berücksichtigung des Stands der Technik und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die persönlichen Rechte und Freiheiten trifft der für die Verarbeitung Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, mit denen die wirksame Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung erreicht werden sollen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.
  
2. Der für die Verarbeitung Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden; dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne Eingreifen einer natürlichen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
  
- 2a. Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 39 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen nachzuweisen.
  
3. (...)
  
4. (...)

## Artikel 24

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

1. Legen zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung personenbezogener Daten fest, so sind sie gemeinsam für die Verarbeitung Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 14 und 14a nachkommt, sofern und soweit die jeweiligen Aufgaben der für die Verarbeitung Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die für die Verarbeitung Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine einzige Anlaufstelle für die betroffenen Personen angegeben werden.
2. Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der für die Verarbeitung Verantwortlichen geltend machen.
3. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam für die Verarbeitung Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln, und der Kern der Vereinbarung wird den betroffenen Personen zur Verfügung gestellt.

## Artikel 25

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

1. In den Fällen gemäß Artikel 3 Absatz 2 benennt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union.
2. Diese Pflicht gilt nicht für
  - (a) (...);
  - (b) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 9a einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt, oder

- (c) Behörden oder öffentliche Stellen.
  - (d) (...)
3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, aufhältig sind.
- 3a. Der Vertreter wird durch den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter beauftragt, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.
4. Die Benennung eines Vertreters durch den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter selbst.

#### *Artikel 26*

#### ***Auftragsverarbeiter***

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

2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien von betroffenen Personen und die Pflichten und Rechte des für die Verarbeitung Verantwortlichen festgelegt sind und insbesondere vorgesehen ist, dass der Auftragsverarbeiter
- (a) die personenbezogenen Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem für die Verarbeitung Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung der Daten mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
  - (b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
  - (c) alle gemäß Artikel 30 erforderlichen Maßnahmen ergreift;
  - (d) die in den Absätzen 1a und 2a genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
  - (e) angesichts der Art der Verarbeitung den für die Verarbeitung Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
  - (f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den für die Verarbeitung Verantwortlichen bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;
  - (g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des für die Verarbeitung Verantwortlichen entweder zurückgibt oder löscht, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht;

- (h) dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom für die Verarbeitung Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. Der Auftragsverarbeiter informiert den für die Verarbeitung Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.
- 2a. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des für die Verarbeitung Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 2 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die entsprechenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.
- 2aa. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 durch den Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 2a nachzuweisen.
- 2ab. Unbeschadet eines individuellen Vertrags zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 2 und 2a ganz oder teilweise auf den in den Absätzen 2b und 2c genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 39 und 39a erteilten Zertifizierung sind.
- 2b. Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 2 und 2a genannten Fragen festlegen.

- 2c. Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 57 Standardvertragsklauseln zur Regelung der in den Absätzen 2 und 2a genannten Fragen festlegen.
3. Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 2 und 2a ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
4. Unbeschadet der Artikel 77, 79 und 79b gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Datenverarbeitung bestimmt, in Bezug auf diese Verarbeitung als für die Verarbeitung Verantwortlicher.
5. (...).

#### *Artikel 27*

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

Der Auftragsverarbeiter und jede dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

#### *Artikel 28*

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

1. Jeder für die Verarbeitung Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Diese Aufzeichnung enthält folgende Angaben:
  - (a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen und etwaiger gemeinsam mit ihm Verantwortlicher, des Vertreters des für die Verarbeitung Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
  - (b) (...)
  - (c) die Zwecke der Verarbeitung;

- (d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien personenbezogener Daten;
  - (e) die Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, einschließlich Empfänger in Drittländern;
  - (f) gegebenenfalls Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
  - (g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
  - (h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.
- 2a. Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten, die Folgendes enthält:
- (a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes für die Verarbeitung Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Vertreters des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
  - (b) (...)
  - (c) die Kategorien der Verarbeitungen, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden;
  - (d) gegebenenfalls Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
  - (e) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.

- 3a. Die in den Absätzen 1 und 2a genannten Aufzeichnungen sind schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde die Aufzeichnungen auf Anforderung zur Verfügung.
4. Die in den Absätzen 1 und 2a genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 9a einschließt.
5. (...)
6. (...).

#### *Artikel 29*

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

1. Der für die Verarbeitung Verantwortliche und der Auftragsarbeiter und der etwaige Vertreter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters arbeiten auf Verlangen mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
2. (...).

## ABSCHNITT 2 DATENSICHERHEIT

### *Artikel 30*

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

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls Folgendes ein:
  - (a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - (b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;
  - (c) die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - (d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
  
- 1a. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Datenverarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob zufällig oder unrechtmäßig, oder unbefugte Weitergabe von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
  
2. (...)
  
- 2a. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 genannten Anforderungen nachzuweisen.

- 2b. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.
3. (...)
4. (...).

### *Artikel 31*

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

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der für die Verarbeitung Verantwortliche ohne unangemessene Verzögerung und möglichst binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt. Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen.
  - 1a. (...)
  2. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung.
  3. Die in Absatz 1 genannte Meldung enthält mindestens folgende Informationen:
    - (a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze;
    - (b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;
    - (c) (...)

- (d) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - (e) eine Beschreibung der von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen.
  - (f) (...)
- 3a. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, stellt der für die Verarbeitung Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.
4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.
5. (...)
6. (...)

### *Artikel 32*

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

1. Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, so benachrichtigt der für die Verarbeitung Verantwortliche die betroffene Person ohne unangemessene Verzögerung von der Verletzung.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 31 Absatz 3 Buchstaben b, d und e genannten Informationen und Empfehlungen.

3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn
  - (a) der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die betreffenden Daten für alle Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht werden, etwa durch Verschlüsselung, oder
  - (b) der für die Verarbeitung Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht, oder
  - (c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesen Fällen hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.
4. Sofern der für die Verarbeitung Verantwortliche der betroffenen Person die Verletzung des Schutzes personenbezogener Daten nicht bereits mitgeteilt hat, kann die Aufsichtsbehörde unter Berücksichtigung dessen, dass die Verletzung voraussichtlich zu einem hohen Risiko führt, von dem für die Verarbeitung Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass alle in Absatz 3 genannten Voraussetzungen erfüllt sind.
5. (...)
6. (...).

### **ABSCHNITT 3**

#### **DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION**

##### *Artikel 33*

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

1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge, so führt der für die Verarbeitung Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

- 1a. Der für die Verarbeitung Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.
2. Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
  - (a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;
  - (b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a;
  - (c) systematische weiträumige Überwachung öffentlich zugänglicher Bereiche;
  - (d) (...)
  - (e) (...)
- 2a. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss.
- 2b. Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss.
- 2c. Vor Festlegung der in den Absätzen 2a und 2b genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 57 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien **Verkehr** personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

3. Die Folgenabschätzung enthält zumindest Folgendes:
  - (a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen;
  - (b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
  - (c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1;
  - (d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.
- 3a. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 durch die zuständigen für die Verarbeitung Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
4. Der für die Verarbeitung Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
5. Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, beruht und falls die betreffenden Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 3 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

6. (...)
7. (...)
8. Erforderlichenfalls führt der für die Verarbeitung Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

#### *Artikel 34*

#### ***Vorherige Konsultation***

1. (...)
2. Der für die Verarbeitung Verantwortliche zieht vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 33 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.
3. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 2 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der für die Verarbeitung Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem für die Verarbeitung Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter spätestens acht Wochen nach dem Antrag auf Konsultation schriftlich entsprechende Empfehlungen und kann ihre in Artikel 53 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um weitere sechs Wochen verlängert werden. Kommt es zu einer Fristverlängerung, wird der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter innerhalb eines Monats nach Eingang des Antrags – auch über die Gründe für die Verzögerung – unterrichtet. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation gegebenenfalls angeforderten Informationen erhalten hat.

4. (...)
5. (...)
6. Der für die Verarbeitung Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 2 folgende Informationen zur Verfügung:
  - (a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des für die Verarbeitung Verantwortlichen, der gemeinsam für die Verarbeitung Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
  - (b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;
  - (c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
  - (d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
  - (e) die Datenschutz-Folgenabschätzung gemäß Artikel 33 und
  - (f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.
7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen zu Rate, die die Verarbeitung personenbezogener Daten betreffen.
- 7a. Ungeachtet des Absatzes 2 können für die Verarbeitung Verantwortliche durch Rechtsvorschriften der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung personenbezogener Daten zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung solcher Daten zu Zwecken des sozialen Schutzes und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.
8. (...)
9. (...).

## ABSCHNITT 4 DATENSCHUTZBEAUFTRAGTER

### *Artikel 35*

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

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
  - (a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die in ihrer gerichtlichen Eigenschaft handeln, oder
  - (b) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
  - (c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a besteht.
2. Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
4. In anderen als den in Absatz 1 genannten Fällen können der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die für die Verarbeitung Verantwortliche oder Auftragsverarbeiter vertreten, handeln.
5. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben.

6. (...)
7. (...)
8. Der Datenschutzbeauftragte kann Beschäftigter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
9. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.
10. (...)
11. (...).

#### *Artikel 36*

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

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
2. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 37 und stellt die für die Erfüllung dieser Aufgaben und für die Erhaltung seines Fachwissens erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung.
- 2a. (neu) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters.
4. Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.
- 4a. Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

#### *Artikel 37*

#### ***Aufgaben des Datenschutzbeauftragten***

1. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:
  - (a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie anderen Datenschutzvorschriften der Union oder der Mitgliedstaaten;
  - (b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten sowie der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
  - (c) (...)
  - (d) (...)
  - (e) (...)
  - (f) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 33;

- (g) Zusammenarbeit mit der Aufsichtsbehörde;
- (h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 34, und gegebenenfalls Beratung zu allen sonstigen Fragen.

2. (...)

2a. Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

## **ABSCHNITT 5**

### **VERHALTENSREGELN UND ZERTIFIZIERUNG**

#### *Artikel 38*

#### ***Verhaltensregeln***

1. Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.
  - 1a. Verbände und andere Vereinigungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, damit die Anwendung von Bestimmungen dieser Verordnung beispielsweise in Bezug auf folgende Aspekte präzisiert wird:
    - (a) faire und transparente Datenverarbeitung;
    - (aa) die berechtigten Interessen des für die Verarbeitung Verantwortlichen in bestimmten Zusammenhängen;
    - (b) Datenerhebung;

- (bb) Pseudonymisierung personenbezogener Daten;
- (c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;
- (d) Ausübung der Rechte betroffener Personen;
- (e) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Zustimmung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
- (ee) Maßnahmen und Verfahren gemäß den Artikeln 22 und 23 und Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 30;
- (ef) Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und Benachrichtigung der betroffenen Person von solchen Verletzungen;
- (f) Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen;
- (g) (...)
- (h) außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der Rechte der betroffenen Personen gemäß den Artikeln 73 und 75.

1ab. Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können Verhaltensregeln, die gemäß Absatz 2 genehmigt wurden und gemäß Absatz 4 allgemeine Gültigkeit besitzen, auch von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, die gemäß Artikel 3 nicht unter diese Verordnung fallen, eingehalten werden, um geeignete Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe des Artikels 42 Absatz 2 Buchstabe d zu bieten. Diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.

- 1b. Die Verhaltensregeln nach Absatz 1 müssen Verfahren vorsehen, die es der in Artikel 38a Absatz 1 genannten Stelle ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen durch die für die Verarbeitung Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen, unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde, die nach Artikel 51 oder 51a zuständig ist.
2. Verbände und andere Vereinigungen gemäß Absatz 1a, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, legen den Entwurf der Verhaltensregeln der Aufsichtsbehörde vor, die nach Artikel 51 zuständig ist. Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf der Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind und genehmigt diesen Entwurf oder diese geänderten oder erweiterten Verhaltensregeln, wenn sie der Auffassung ist, dass er/sie ausreichende geeignete Garantien bietet/bieten.
  - 2a. Wird durch die Stellungnahme nach Absatz 2 bestätigt, dass die Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind, so werden die Verhaltensregeln genehmigt, und beziehen sich die Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht sie.
  - 2b. Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die nach Artikel 51 zuständige Aufsichtsbehörde ihn – vor Genehmigung – nach dem Verfahren gemäß Artikel 57 dem Europäischen Datenschutzausschuss vor, der zu der Frage Stellung nimmt, ob der Entwurf der Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind oder – im Fall nach Absatz 1ab – geeignete Garantien vorsieht/vorsehen.
3. Wird durch die Stellungnahme nach Absatz 2b bestätigt, dass der Entwurf oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind oder – im Fall nach Absatz 1ab – geeignete Garantien vorsieht/vorsehen, so übermittelt der Europäische Datenschutzausschuss seine Stellungnahme der Kommission.

4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 übermittelten genehmigten Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender genehmigter Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.
5. Die Kommission trägt dafür Sorge, dass die genehmigten Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.
- 5a. Der Europäische Datenschutzausschuss nimmt alle genehmigten Verhaltensregeln beziehungsweise Änderungen daran in ein Register auf und veröffentlicht sie in geeigneter Weise.

*Artikel 38a*

***Überwachung der genehmigten Verhaltensregeln***

1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 38 von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde.
2. Eine Stelle gemäß Absatz 1 kann zu diesem Zweck akkreditiert werden, wenn
  - (a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;
  - (b) sie Verfahren festgelegt hat, die es ihr ermöglichen, zu bewerten, ob für die Verarbeitung Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der Verhaltensregeln durch die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter zu überwachen und die Anwendung der Verhaltensregeln regelmäßig zu überprüfen;
  - (c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;

- (d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
3. Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 57 an den Europäischen Datenschutzausschuss.
  4. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde und der Bestimmungen des Kapitels VIII ergreift eine Stelle gemäß Absatz 1 vorbehaltlich angemessener Garantien im Falle einer Verletzung der Verhaltensregeln durch einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter geeignete Maßnahmen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters von den Verhaltensregeln. Sie unterrichtet die zuständige Aufsichtsbehörde über solche Maßnahmen und deren Begründung.
  5. Die zuständige Aufsichtsbehörde widerruft die Akkreditierung einer Stelle gemäß Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.
  6. Dieser Artikel gilt nicht für die Verarbeitung personenbezogener Daten durch Behörden oder öffentliche Stellen.

### *Artikel 39*

#### ***Zertifizierung***

1. Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen, die von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern durchgeführt werden, eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

- 1a. Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 2a genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 42 Absatz 2 Buchstabe e geeignete Garantien bieten. Diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.
- 1b. Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.
2. Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörde, die gemäß Artikel 51 oder 51a zuständig ist.
- 2a. Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 39a oder durch die zuständige Aufsichtsbehörde anhand der von der zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – durch den Europäischen Datenschutzausschuss genehmigten Kriterien erteilt. Im letzteren Fall können die vom Europäischen Datenschutzausschuss genehmigten Kriterien zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.
3. (neu) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 39a oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.

4. Die Zertifizierung wird einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die einschlägigen Voraussetzungen weiterhin erfüllt werden. Sie wird gegebenenfalls durch die Zertifizierungsstellen nach Artikel 39a oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.
5. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

#### *Artikel 39a*

#### ***Zertifizierungsstelle und verfahren***

1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung – nach Unterrichtung der Aufsichtsbehörde, damit sie erforderlichenfalls von ihren Befugnissen gemäß Artikel 53 Absatz 1b Buchstabe fa Gebrauch machen kann – von einer Zertifizierungsstelle erteilt und verlängert, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat regelt, ob diese Zertifizierungsstellen akkreditiert werden von
  - (a) der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde und/oder
  - (b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.
2. Die Zertifizierungsstelle nach Absatz 1 kann zu diesem Zweck nur akkreditiert werden, wenn
  - (a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

- (aa) sie sich verpflichtet hat, die Kriterien nach Artikel 39 Absatz 2a, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – von dem Europäischen Datenschutzausschuss genehmigt wurden, einzuhalten;
  - (b) sie Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung sowie der Datenschutzsiegel und -prüfzeichen festgelegt hat;
  - (c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;
  - (d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
3. Die Akkreditierung der Zertifizierungsstellen nach Absatz 1 erfolgt anhand der Kriterien, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – von dem Europäischen Datenschutzausschuss genehmigt wurden. Im Fall einer Akkreditierung nach Absatz 1 Buchstabe b ergänzen diese Anforderungen diejenigen, die in der Verordnung [765/2008](#) und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.
4. Die Zertifizierungsstelle nach Absatz 1 ist unbeschadet der Verantwortung, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die Stelle die Anforderungen erfüllt.
5. Die Zertifizierungsstelle nach Absatz 1 teilt der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

6. Die Anforderungen nach Absatz 3 und die Kriterien nach Artikel 39 Absatz 2a werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht. Die Aufsichtsbehörde übermittelt diese auch dem Europäischen Datenschutzausschuss. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise.
- 6a. Unbeschadet der Bestimmungen des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.
7. Der Kommission wird die Befugnis übertragen, gemäß Artikel 86 delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die für die in Artikel 39 Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind.
- 7a. (...)
8. Die Kommission kann technische Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.

# KAPITEL V

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

### *Artikel 40*

#### ***Allgemeine Grundsätze der Datenübermittlung***

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

### *Artikel 41*

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

1. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland bzw. ein Gebiet oder ein oder mehrere spezifische Sektoren dieses Drittlands oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.

2. Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere
- (a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Drittland bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften, die Datenschutzbestimmungen, Berufsvorschriften und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, juristische Präzedenzfälle sowie die Existenz wirksamer und durchsetzbarer Rechte der betroffenen Person und wirksamer verwaltungsrechtlicher und gerichtlicher Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,
  - (b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und
  - (c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtlich bindenden Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

3. Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen relevanten Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte(n) Aufsichtsbehörde(n) angegeben. Der Durchführungsrechtsakt wird gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.
  - 3a. (...)
  4. (...)
  - 4a. Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.
5. Die Kommission stellt, soweit entsprechende Informationen – insbesondere im Anschluss an die in Absatz 3 genannte Überprüfung – vorliegen, durch Beschluss fest, dass ein Drittland bzw. ein Gebiet oder ein spezifischer Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 mehr gewährleistet, und widerruft oder ändert die in Absatz 3 genannten Beschlüsse oder setzt sie aus, soweit dies nötig ist und ohne rückwirkende Kraft. Der Durchführungsrechtsakt wird gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 oder in äußerst dringlichen Fällen gemäß dem Verfahren nach Artikel 87 Absatz 3 erlassen.
  - 5a. Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

6. Übermittlungen personenbezogener Daten an das betreffende Drittland bzw. an das Gebiet oder den spezifischen Sektor dieses Drittlands oder an die betreffende internationale Organisation gemäß den Artikeln 42 bis 44 werden durch einen Beschluss nach Absatz 5 nicht berührt.
7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren eines Drittlands und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.
8. Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

#### *Artikel 42*

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

1. Falls kein Beschluss nach Artikel 41 Absatz 3 vorliegt, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.
2. Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in
  - (oa) einem rechtlich bindenden und durchsetzbaren Instrument zwischen den Behörden oder öffentlichen Stellen oder
  - (a) verbindlichen unternehmensinternen Datenschutzvorschriften gemäß Artikel 43 oder
  - (b) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen werden, oder
  - (c) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 genehmigt wurden, oder

- (d) genehmigten Verhaltensregeln gemäß Artikel 38 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder
- (e) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 39 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

2a. Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

- (a) Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder
- (b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

3. (...)

4. (...)

5. (...)

5a. Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 57 an, wenn ein Fall gemäß Absatz 2a vorliegt.

5b. Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

*Artikel 43*

***Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner  
Datenschutzvorschriften***

1. Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 57 verbindliche unternehmensinterne Datenschutzvorschriften, sofern diese
  - (a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt;
  - (b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen;
  - (c) die in Absatz 2 festgelegten Anforderungen erfüllen.
  
2. Die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:
  - (a) Struktur und Kontaktdaten der betreffenden Unternehmensgruppe und jedes ihrer Mitglieder;
  - (b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;
  - (c) interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Datenschutzvorschriften;
  - (d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Datenweitergabe an nicht an diese unternehmensinternen Datenschutzvorschriften gebundene Stellen;

- (e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;
- (f) die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Datenschutzvorschriften; der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann nur dann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;
- (g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 14 und 14a hinaus über die verbindlichen unternehmensinternen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;
- (h) die Aufgaben jedes gemäß Artikel 35 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften in der Unternehmensgruppe sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;
- (hh) die Beschwerdeverfahren;
- (i) die innerhalb der Gruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens oder der Gruppe von Unternehmen mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Ersuchen zur Verfügung gestellt werden;

- (j) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;
- (k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Gruppe gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde;
- (l) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Gruppe in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen unternehmensinternen Datenschutzvorschriften bieten, und
- (m) geeignete Datenschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

2a. (...)

3. (...)

4. Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche unternehmensinterne Datenschutzvorschriften im Sinne dieses Artikels zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.

*Artikel 43a (neu)*

***Nach dem Unionsrecht nicht zulässige Übermittlung oder Weitergabe***

1. Urteile eines Gerichts eines Drittlands und Entscheidungen einer Verwaltungsbehörde eines Drittlands, mit denen von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Weitergabe personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

*Artikel 44*

***Ausnahmen für Sonderfälle***

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 42, einschließlich verbindlicher unternehmensinterner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig, wenn
  - (a) die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde, oder
  - (b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder
  - (c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist oder
  - (d) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist oder
  - (e) die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist oder

- (f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, oder
- (g) die Übermittlung aus einem Register erfolgt, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder
- (h) die Übermittlung nicht auf eine Bestimmung der Artikel 41 oder 42 – einschließlich der verbindlichen unternehmensinternen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen Sonderfall gemäß den Buchstaben a bis g anwendbar ist; in diesem Fall darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und falls der für die Verarbeitung Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der für die Verarbeitung Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Er unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 14 und 14a mitgeteilten Informationen.

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

3. (...)

4. Absatz 1 Buchstaben a, b, c und h gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.
5. Das öffentliche Interesse im Sinne des Absatzes 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.
- 5a. 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 personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h in der Dokumentation gemäß Artikel 28.
7. (...).

#### *Artikel 45*

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

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur
  - (a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die tatsächliche Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,
  - (b) internationalen Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Meldungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,

- (c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zur Förderung der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten dienen,
- (d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praxis zum Schutz personenbezogener Daten, auch in Bezug auf Zuständigkeitskonflikte mit Drittländern.

2. (...)

## KAPITEL VI UNABHÄNGIGKEIT DER AUFSICHTSBEHÖRDEN

### ABSCHNITT 1 UNABHÄNGIGKEIT

#### *Artikel 46*

#### *Aufsichtsbehörde*

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

## Artikel 47

### **Unabhängigkeit**

1. Jede Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.
2. Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.
3. Die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.
4. (...)
5. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.
6. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der Aufsichtsbehörde untersteht.
7. Die Mitgliedstaaten stellen sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass jede Aufsichtsbehörde über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

## *Artikel 48*

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

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

## *Artikel 49*

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

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

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

*Artikel 50*

***Verschwiegenheitspflicht***

(...)

## ABSCHNITT 2 ZUSTÄNDIGKEIT, AUFGABEN UND BEFUGNISSE

### *Artikel 51*

#### ***Zuständigkeit***

1. Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.
2. Erfolgt die Verarbeitung durch Behörden oder private Einrichtungen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 51a keine Anwendung.
3. Die Aufsichtsbehörden sind nicht zuständig für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen.

### *Artikel 51a*

#### ***Zuständigkeit der federführenden Aufsichtsbehörde***

1. Unbeschadet des Artikels 51 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 54a die zuständige federführende Aufsichtsbehörde für die grenzüberschreitende Verarbeitung dieses für die Verarbeitung Verantwortlichen oder dieses Auftragsverarbeiters.
- 2a. Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.

- 2b. In den in Absatz 2a genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie den Fall gemäß dem Verfahren nach Artikel 54a regelt oder nicht, wobei sie berücksichtigt, ob der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.
- 2c. Entscheidet die federführende Aufsichtsbehörde, den Fall zu regeln, so findet das Verfahren nach Artikel 54a Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 54 Absatz 2 weitestgehend Rechnung.
- 2d. Entscheidet die federführende Aufsichtsbehörde, den Fall nicht selbst zu regeln, so regelt die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, den Fall gemäß den Artikeln 55 und 56.
3. Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der für die Verarbeitung Verantwortlichen oder der Auftragsverarbeiter für Fragen der grenzüberschreitenden Verarbeitung durch diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter.

#### *Artikel 52*

#### ***Aufgaben***

1. Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet
- (a) die Anwendung dieser Verordnung überwachen und durchsetzen;
  - (aa) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

- (ab) im Einklang mit dem einzelstaatlichen Recht das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten von natürlichen Personen in Bezug auf die Verarbeitung personenbezogener Daten beraten;
- (ac) die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter über die ihnen aus dieser Verordnung entstehenden Pflichten aufklären;
- (ad) auf Antrag jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;
- (b) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 76 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer über den Fortgang und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
- (c) mit anderen Aufsichtsbehörden zusammenarbeiten, Informationen austauschen und Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;
- (d) Untersuchungen über die Anwendung dieser Verordnung auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde durchführen;
- (e) relevante Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
- (f) Standardvertragsklauseln im Sinne des Artikels 26 Absatz 2c und des Artikels 42 Absatz 2 Buchstabe c festlegen;

- (fa) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 33 Absatz 2a eine Datenschutz-Folgenabschätzung durchzuführen ist;
- (g) Beratung in Bezug auf die in Artikel 34 Absatz 3 genannten Verarbeitungsvorgänge leisten;
- (ga) die Ausarbeitung von Verhaltensregeln gemäß Artikel 38 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 38 Absatz 2 bieten müssen, Stellungnahmen abgeben und sie billigen;
- (gb) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 39 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 39 Absatz 2a billigen;
- (gc) gegebenenfalls die nach Artikel 39 Absatz 4 erteilten Zertifizierungen regelmäßig überprüfen;
- (h) die Kriterien für die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 38a und einer Zertifizierungsstelle gemäß Artikel 39a abfassen und veröffentlichen;
- (ha) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 38a und einer Zertifizierungsstelle gemäß Artikel 39a vornehmen;
- (hb) Vertragsklauseln und Bestimmungen im Sinne des Artikels 42 Absatz 2a genehmigen;
- (i) verbindliche unternehmensinterne Vorschriften gemäß Artikel 43 genehmigen;
- (j) Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses leisten;
- (jb) interne Aufzeichnungen über Verstöße gegen diese Verordnung und ergriffene Maßnahmen, insbesondere Warnungen und Sanktionen, führen;
- (k) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

2. (...)

3. (...)

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

#### *Artikel 53*

#### ***Befugnisse***

1. Jede Aufsichtsbehörde verfügt über die folgenden Untersuchungsbefugnisse, die es ihr gestatten,
  - (a) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
    - (aa) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
    - (ab) eine Überprüfung der nach Artikel 39 Absatz 4 erteilten Zertifizierungen durchzuführen,
  - (b) (...)
  - (c) (...)
  - (d) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
    - (da) von dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter Zugriff auf alle personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,
    - (db) im Einklang mit dem Unionsrecht oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters zu erhalten.

- 1b. Jede Aufsichtsbehörde verfügt über die folgenden Abhilfebefugnisse, die es ihr gestatten,
- (a) einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
  - (b) einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter zu tadeln, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
  - (ca) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
  - (d) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
  - (da) den für die Verarbeitung Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
  - (e) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
  - (f) die Berichtigung, Einschränkung oder Löschung von Daten gemäß den Artikeln 16, 17 und 17a und die Unterrichtung der Empfänger, an die diese Daten gemäß Artikel 17 Absatz 2a und Artikel 17b weitergegeben wurden, über solche Maßnahmen anzuordnen,
  - (fa) (neu) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 39 und 39a erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
  - (g) eine Geldbuße gemäß Artikel 79 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,
  - (h) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.
  - (i) (...)
  - (j) (...)

- 1c. Jede Aufsichtsbehörde verfügt über die folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,
- (a) gemäß dem Verfahren der vorherigen Zurateziehung nach Artikel 34 den für die Verarbeitung Verantwortlichen zu beraten,
  - (aa) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem einzelstaatlichen Recht an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,
  - (ab) die Verarbeitung gemäß Artikel 34 Absatz 7a zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,
  - (ac) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 38 Absatz 2 zu billigen,
  - (ad) Zertifizierungsstellen gemäß Artikel 39a zu akkreditieren,
  - (ae) im Einklang mit Artikel 39 Absatz 2a Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,
  - (b) Standarddatenschutzklauseln nach Artikel 26 Absatz 2c und Artikel 42 Absatz 2 Buchstabe c festzulegen,
  - (c) Vertragsklauseln gemäß Artikel 42 Absatz 2a Buchstabe a zu genehmigen,
  - (ca) Verwaltungsvereinbarungen gemäß Artikel 42 Absatz 2a Buchstabe d zu genehmigen,
  - (d) verbindliche unternehmensinterne Vorschriften gemäß Artikel 43 zu genehmigen.
2. Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse gemäß diesem Artikel erfolgt vorbehaltlich angemessener Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta der Grundrechte der Europäischen Union.
3. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um dieser Verordnung Geltung zu verschaffen.

4. Jeder Mitgliedstaat kann durch Gesetz regeln, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 1a und 1c aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Wirkungsweise der Bestimmungen des Kapitels VII beeinträchtigen.

*Artikel 54*

***Tätigkeitsbericht***

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

# KAPITEL VII ZUSAMMENARBEIT UND KOHÄRENZ

## ABSCHNITT 1 ZUSAMMENARBEIT

### *Artikel 54a*

#### ***Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden***

1. Die federführende Aufsichtsbehörde arbeitet mit den anderen betroffenen Aufsichtsbehörden im Einklang mit diesem Artikel zusammen und bemüht sich dabei, einen Konsens zu erzielen. Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen aus.
- 1a. Die federführende Aufsichtsbehörde kann jederzeit andere betroffene Aufsichtsbehörden um Amtshilfe gemäß Artikel 55 ersuchen und gemeinsame Maßnahmen gemäß Artikel 56 durchführen, insbesondere zur Durchführung von Untersuchungen oder zur Überwachung der Umsetzung einer Maßnahme in Bezug auf einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter, der in einem anderen Mitgliedstaat niedergelassen ist.
2. Die federführende Aufsichtsbehörde übermittelt den anderen betroffenen Aufsichtsbehörden unverzüglich die zweckdienlichen Informationen zu der Angelegenheit. Sie legt den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vor und trägt deren Standpunkten gebührend Rechnung.
3. Legt eine der anderen betroffenen Aufsichtsbehörden innerhalb von vier Wochen, nachdem sie gemäß Absatz 2 konsultiert wurde, gegen diesen Beschlussentwurf einen relevanten und begründeten Einspruch ein und schließt sich die federführende Aufsichtsbehörde dem Einspruch nicht an oder ist der Einspruch nicht relevant und begründet, so leitet die federführende Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 57 für die Angelegenheit ein.

- 3a. Beabsichtigt die federführende Aufsichtsbehörde, sich dem Einspruch anzuschließen, so legt sie den anderen betroffenen Aufsichtsbehörden einen überarbeiteten Beschlussentwurf zur Stellungnahme vor. Der überarbeitete Beschlussentwurf wird innerhalb von zwei Wochen dem Verfahren nach Absatz 3 unterzogen.
4. Legt keine der anderen betroffenen Aufsichtsbehörden Einspruch gegen den Beschlussentwurf ein, der von der federführenden Aufsichtsbehörde innerhalb der in den Absätzen 3 und 3a festgelegten Frist vorgelegt wurde, so gelten die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden als mit dem Beschlussentwurf einverstanden und sind an ihn gebunden.
- 4a. Die federführende Aufsichtsbehörde erlässt den Beschluss und teilt ihn der Hauptniederlassung oder der einzigen Niederlassung des für die Verarbeitung Verantwortlichen oder gegebenenfalls des Auftragsverarbeiters mit und setzt die anderen betroffenen Aufsichtsbehörden und den Europäischen Datenschutzausschuss von dem betreffenden Beschluss einschließlich einer Zusammenfassung der relevanten Fakten und Gründe in Kenntnis. Die Aufsichtsbehörde, bei der eine Beschwerde eingereicht worden ist, unterrichtet den Beschwerdeführer über den Beschluss.
- 4b. Wird eine Beschwerde abgelehnt oder abgewiesen, so erlässt die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, abweichend von Absatz 4a den Beschluss, teilt ihn dem Beschwerdeführer mit und setzt den für die Verarbeitung Verantwortlichen in Kenntnis.
- 4bb. Sind sich die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörde darüber einig, Teile der Beschwerde abzulehnen oder abzuweisen und bezüglich anderer Teile dieser Beschwerde tätig zu werden, so wird in dieser Angelegenheit für jeden dieser Teile ein eigener Beschluss erlassen. Die federführende Aufsichtsbehörde erlässt den Beschluss für den Teil, der das Tätigwerden in Bezug auf den für die Verarbeitung Verantwortlichen betrifft, teilt ihn der Hauptniederlassung oder einzigen Niederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats mit und setzt den Beschwerdeführer hiervon in Kenntnis, während die für den Beschwerdeführer zuständige Aufsichtsbehörde den Beschluss für den Teil erlässt, der die Ablehnung oder Abweisung dieser Beschwerde betrifft, und ihn diesem Beschwerdeführer mitteilt und den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter hiervon in Kenntnis setzt.

- 4c. Nach der Unterrichtung über den Beschluss der federführenden Aufsichtsbehörde gemäß den Absätzen 4a und 4bb ergreift der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die erforderlichen Maßnahmen, um die Verarbeitungstätigkeiten all seiner Niederlassungen in der Union mit dem Beschluss in Einklang zu bringen. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter teilt der federführenden Aufsichtsbehörde die Maßnahmen mit, die zur Einhaltung des Beschlusses ergriffen wurden; diese wiederum unterrichtet die anderen betroffenen Aufsichtsbehörden.
- 4d. Hat – in Ausnahmefällen – eine betroffene Aufsichtsbehörde Grund zu der Annahme, dass zum Schutz der Interessen betroffener Personen dringender Handlungsbedarf besteht, so kommt das Dringlichkeitsverfahren nach Artikel 61 zur Anwendung.
5. Die federführende Aufsichtsbehörde und die anderen betroffenen Aufsichtsbehörden übermitteln einander die nach diesem Artikel geforderten Informationen auf elektronischem Wege unter Verwendung eines standardisierten Formats.

#### *Artikel 55*

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

1. Die Aufsichtsbehörden übermitteln einander zweckdienliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Zurateziehung, um Vornahme von Nachprüfungen und Untersuchungen.
2. Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu können insbesondere auch die Übermittlung zweckdienlicher Informationen über die Durchführung einer Untersuchung gehören.

3. Das Amtshilfeersuchen enthält alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.
4. Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn
  - (a) sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder
  - (b) ein Eingehen auf das Ersuchen gegen die Bestimmungen dieser Verordnung verstoßen würde oder gegen das Unionsrecht oder das Recht des Mitgliedstaats, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt.
5. Die Aufsichtsbehörde, an die das Ersuchen gerichtet wurde, informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um auf das Ersuchen zu antworten. Bei einer Ablehnung gemäß Absatz 4 erläutert sie ihre Gründe für die Ablehnung des Ersuchens.
6. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.
7. Maßnahmen, die aufgrund eines Amtshilfeersuchens getroffen werden, sind gebührenfrei. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.
8. Erteilt eine ersuchte Aufsichtsbehörde nicht binnen eines Monats nach Eingang des Ersuchens einer anderen Aufsichtsbehörde die Informationen gemäß Absatz 5, so kann die ersuchende Aufsichtsbehörde eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 61 Absatz 1 ausgegangen, der einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Europäischen Datenschutzausschusses gemäß Artikel 61 Absatz 2 erforderlich macht.
9. (...)

10. Die Kommission kann Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere das in Absatz 6 genannte standardisierte Format, festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.

#### *Artikel 56*

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

1. Die Aufsichtsbehörden führen gegebenenfalls gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen durch, an denen Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.
2. In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über Niederlassungen in mehreren Mitgliedstaaten verfügt oder in denen die Verarbeitungsvorgänge voraussichtlich auf eine bedeutende Zahl betroffener Personen in mehr als einem Mitgliedstaat erhebliche Auswirkungen haben werden, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, gegebenenfalls an den gemeinsamen Maßnahmen teilzunehmen. Die zuständige Aufsichtsbehörde gemäß Artikel 51a Absatz 1 oder Absatz 2c lädt die Aufsichtsbehörde jedes dieser Mitgliedstaaten zur Teilnahme an den betreffenden gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme.
3. Eine Aufsichtsbehörde kann gemäß den Rechtsvorschriften ihres Mitgliedstaats und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde Befugnisse einschließlich Untersuchungsbefugnisse übertragen oder, soweit dies nach dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Untersuchungsbefugnisse nach dem Recht des Mitgliedstaats der unterstützenden Aufsichtsbehörde auszuüben. Diese Untersuchungsbefugnisse können nur unter der Leitung und in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem nationalen Recht der einladenden Aufsichtsbehörde.

- 3a. Sind gemäß Absatz 1 Bedienstete einer unterstützenden Aufsichtsbehörde in einem anderen Mitgliedstaat im Einsatz, so übernimmt der Mitgliedstaat der einladenden Aufsichtsbehörde nach Maßgabe des Rechts des Mitgliedstaats, in dessen Hoheitsgebiet der Einsatz erfolgt, die Verantwortung für ihr Handeln, einschließlich der Haftung für alle von ihnen bei ihrem Einsatz verursachten Schäden.
- 3b. Der Mitgliedstaat, in dessen Hoheitsgebiet der Schaden verursacht wurde, ersetzt diesen Schaden so, wie er ihn ersetzen müsste, wenn seine eigenen Bediensteten ihn verursacht hätten. Der Mitgliedstaat der unterstützenden Aufsichtsbehörde, deren Bedienstete im Hoheitsgebiet eines anderen Mitgliedstaats einer Person Schaden zugefügt haben, erstattet diesem anderen Mitgliedstaat den Gesamtbetrag des Schadenersatzes, den dieser an die Berechtigten geleistet hat.
- 3c. Unbeschadet der Ausübung seiner Rechte gegenüber Dritten und mit Ausnahme des Absatzes 3b verzichtet jeder Mitgliedstaat in dem Fall des Absatzes 1 darauf, den Betrag des erlittenen Schadens anderen Mitgliedstaaten gegenüber geltend zu machen.
4. (...)
5. Ist eine gemeinsame Maßnahme geplant und kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 Satz 2 nach, so können die anderen Aufsichtsbehörden eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 61 Absatz 1 ausgegangen, der eine im Dringlichkeitsverfahren angenommene Stellungnahme oder einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Europäischen Datenschutzausschusses gemäß Artikel 61 Absatz 2 erforderlich macht.
6. (...)

## **ABSCHNITT 2**

### **KOHÄRENZ**

#### *Artikel 57*

#### ***Kohärenzverfahren***

1. Um zur einheitlichen Anwendung dieser Verordnung in der gesamten Union beizutragen, arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.

#### *Artikel 58*

#### ***Stellungnahme des Europäischen Datenschutzausschusses***

1. Der Europäische Datenschutzausschuss gibt eine Stellungnahme ab, wenn die zuständige Aufsichtsbehörde beabsichtigt, eine der nachstehenden Maßnahmen zu erlassen. Zu diesem Zweck übermittelt die zuständige Aufsichtsbehörde dem Europäischen Datenschutzausschuss den Entwurf des Beschlusses, wenn dieser
  - (c) der Annahme einer Liste der Verarbeitungsvorgänge dient, die der Anforderung einer Datenschutz-Folgenabschätzung gemäß Artikel 33 Absatz 2a unterliegen, oder
  - (ca) eine Angelegenheit gemäß Artikel 38 Absatz 2b und damit die Frage betrifft, ob ein Entwurf von Verhaltensregeln oder eine Änderung oder Ergänzung von Verhaltensregeln mit dieser Verordnung in Einklang steht, oder
  - (cb) der Billigung der Kriterien für die Akkreditierung einer Stelle nach Artikel 38a Absatz 3 oder einer Zertifizierungsstelle nach Artikel 39a Absatz 3 dient, oder
  - (d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c und Artikel 26 Absatz 2c dient, oder

- (e) der Genehmigung von Vertragsklauseln gemäß Artikels 42 Absatz 2a Buchstabe a dient, oder
  - (f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dient.
2. Jede Aufsichtsbehörde, der Vorsitz des Europäischen Datenschutzausschusses oder die Kommission können beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Europäischen Datenschutzausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 nicht nachkommt.
  3. In den in den Absätzen 1 und 2 genannten Fällen gibt der Europäische Datenschutzausschuss eine Stellungnahme zu der Angelegenheit ab, die ihm vorgelegt wurde, sofern er nicht bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat. Diese Stellungnahme wird binnen acht Wochen mit der einfachen Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen verlängert werden. Was den in Absatz 1 genannten Beschlussentwurf angeht, der gemäß Absatz 6 den Mitgliedern des Ausschusses übermittelt wird, so wird angenommen, dass ein Mitglied, das innerhalb einer vom Vorsitz angegebenen angemessenen Frist keine Einwände erhoben hat, dem Beschlussentwurf zustimmt.
  4. (...)
  5. Die Aufsichtsbehörden und die Kommission übermitteln ohne unangemessene Verzögerung dem Europäischen Datenschutzausschuss auf elektronischem Wege unter Verwendung eines standardisierten Formats alle zweckdienlichen Informationen, einschließlich – je nach Fall – einer kurzen Darstellung des Sachverhalts, des Beschlussentwurfs, der Gründe, warum eine solche Maßnahme ergriffen werden muss, und der Standpunkte anderer betroffener Aufsichtsbehörden.

6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet ohne unangemessene Verzögerung auf elektronischem Wege
  - (a) unter Verwendung eines standardisierten Formats die Mitglieder des Europäischen Datenschutzausschusses und die Kommission über alle zweckdienlichen Informationen, die ihm zugegangen sind. Soweit erforderlich stellt das Sekretariat des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung;
  - (b) je nach Fall die in den Absätzen 1 und 2 genannte Aufsichtsbehörde und die Kommission über die Stellungnahme und veröffentlicht sie.
7. (...)
- 7a. Die zuständige Aufsichtsbehörde nimmt den in Absatz 1 genannten Beschlussentwurf nicht vor Ablauf der in Absatz 3 genannten Frist an.
- 7b. (...)
8. Die in Absatz 1 genannte Aufsichtsbehörde trägt der Stellungnahme des Europäischen Datenschutzausschusses weitestgehend Rechnung und teilt dessen Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme elektronisch unter Verwendung eines standardisierten Formats mit, ob sie den Beschlussentwurf beibehält oder ändert; gegebenenfalls übermittelt sie den geänderten Beschlussentwurf.
9. Teilt die betroffene Aufsichtsbehörde dem Vorsitz des Europäischen Datenschutzausschusses innerhalb der Frist nach Absatz 8 unter Angabe der maßgeblichen Gründe mit, dass sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen, so gilt Artikel 58a Absatz 1.

#### *Artikel 58a*

#### ***Streitbeilegung durch den Europäischen Datenschutzausschuss***

1. Um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung in Einzelfällen sicherzustellen, erlässt der Europäische Datenschutzausschuss in den folgenden Fällen einen verbindlichen Beschluss:

- (a) wenn eine betroffene Aufsichtsbehörde in einem Fall nach Artikel 54a Absatz 3 einen relevanten und begründeten Einspruch gegen einen Beschlussentwurf der federführenden Behörde eingelegt hat oder die federführende Behörde einen Einspruch als nicht relevant und/oder nicht begründet abgelehnt hat. Der verbindliche Beschluss betrifft alle Angelegenheiten, die Gegenstand des relevanten und begründeten Einspruchs sind, insbesondere die Frage, ob ein Verstoß gegen die Verordnung vorliegt;
  - (b) wenn es widersprüchliche Standpunkte dazu gibt, welche der betroffenen Aufsichtsbehörden für die Hauptniederlassung zuständig ist;
  - (d) wenn eine zuständige Aufsichtsbehörde in den in Artikel 58 Absatz 1 genannten Fällen keine Stellungnahme des Europäischen Datenschutzausschusses einholt oder der Stellungnahme des Europäischen Datenschutzausschusses gemäß Artikel 58 nicht folgt. In diesem Fall kann jede betroffene Aufsichtsbehörde oder die Kommission die Angelegenheit dem Europäischen Datenschutzausschuss vorlegen.
2. Der in Absatz 1 genannte Beschluss wird innerhalb eines Monats nach der Befassung mit der Angelegenheit mit einer Mehrheit von zwei Dritteln der Mitglieder des Ausschusses angenommen. Diese Frist kann wegen der Komplexität der Angelegenheit um einen weiteren Monat verlängert werden. Der in Absatz 1 genannte Beschluss wird begründet und an die federführende Aufsichtsbehörde und alle betroffenen Aufsichtsbehörden übermittelt und ist für diese verbindlich.
  3. War der Ausschuss nicht in der Lage, innerhalb der in Absatz 2 genannten Fristen einen Beschluss anzunehmen, so nimmt er seinen Beschluss innerhalb von zwei Wochen nach Ablauf des in Absatz 2 genannten zweiten Monats mit einfacher Mehrheit der Mitglieder des Ausschusses an. Bei Stimmgleichheit zwischen den Mitgliedern des Ausschusses gibt die Stimme des Vorsitzes den Ausschlag.
  4. Die betroffenen Aufsichtsbehörden nehmen vor Ablauf der in den Absätzen 2 und 3 genannten Fristen keinen Beschluss über die dem Ausschuss vorgelegte Angelegenheit an.
  5. (...)

6. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die betroffenen Aufsichtsbehörden ohne ungebührliche Verzögerung über den in Absatz 1 genannten Beschluss. Er setzt die Kommission hiervon in Kenntnis. Der Beschluss wird unverzüglich auf der Website des Europäischen Datenschutzausschusses veröffentlicht, nachdem die Aufsichtsbehörde den in Absatz 7 genannten endgültigen Beschluss mitgeteilt hat.
  
7. Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, trifft den endgültigen Beschluss auf der Grundlage des in Absatz 1 genannten Beschlusses ohne unangemessene Verzögerung und spätestens einen Monat, nachdem der Europäische Datenschutzausschuss seinen Beschluss mitgeteilt hat. Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, setzt den Europäischen Datenschutzausschuss von dem Zeitpunkt, zu dem ihr endgültiger Beschluss dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter bzw. der betroffenen Person mitgeteilt wird, in Kenntnis. Der endgültige Beschluss der betroffenen Aufsichtsbehörden wird gemäß Artikel 54a Absätze 4a, 4b und 4bb angenommen. Im endgültigen Beschluss wird auf den in Absatz 1 genannten Beschluss verwiesen und festgelegt, dass der in Absatz 1 genannte Beschluss gemäß Absatz 6 auf der Website des Europäischen Datenschutzausschusses veröffentlicht wird. Dem endgültigen Beschluss wird der in Absatz 1 genannte Beschluss beigelegt.

#### *Artikel 59*

#### ***Stellungnahme der Kommission***

(...)

#### *Artikel 60*

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

(...)

## Artikel 61

### *Dringlichkeitsverfahren*

1. Unter außergewöhnlichen Umständen kann eine betroffene Aufsichtsbehörde abweichend vom Kohärenzverfahren nach Artikel 57, 58 und 58a oder dem Verfahren nach Artikel 54a sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer von höchstens drei Monaten treffen, die in ihrem Hoheitsgebiet rechtliche Wirkung entfalten sollen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um Rechte und Freiheiten von betroffenen Personen zu schützen. Die Aufsichtsbehörde setzt die anderen betroffenen Aufsichtsbehörden, den Europäischen Datenschutzausschuss und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis.
2. Hat eine Aufsichtsbehörde eine Maßnahme nach Absatz 1 ergriffen und ist sie der Auffassung, dass dringend endgültige Maßnahmen erlassen werden müssen, kann sie unter Angabe von Gründen im Dringlichkeitsverfahren um eine Stellungnahme oder einen verbindlichen Beschluss des Europäischen Datenschutzausschusses ersuchen.
3. Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme oder gegebenenfalls einen verbindlichen Beschluss des Europäischen Datenschutzausschusses ersuchen, wenn eine zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine geeignete Maßnahme getroffen hat, um die Rechte und Freiheiten von betroffenen Personen zu schützen.
4. Abweichend von Artikel 58 Absatz 3 und Artikel 58a Absatz 2 wird eine Stellungnahme oder ein verbindlicher Beschluss im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen mit einfacher Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen.

*Artikel 62*

***Informationsaustausch***

1. Die Kommission kann zu folgenden Zwecken Durchführungsrechtsakte von allgemeiner Tragweite erlassen:
  - (a) (...)
  - (b) (...)
  - (c) (...)
  - (d) Festlegung der Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss, insbesondere des standardisierten Formats nach Artikel 58.

Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.

2. (...)

3. (...)

*Artikel 63*

***Durchsetzung***

(...)

### ABSCHNITT 3

## EUROPÄISCHER DATENSCHUTZAUSSCHUSS

#### *Artikel 64*

#### ***Europäischer Datenschutzausschuss***

- 1a. Der Europäische Datenschutzausschuss wird hiermit als Einrichtung der Union mit eigener Rechtspersönlichkeit geschaffen.
- 1b. Der Europäische Datenschutzausschuss wird von seinem Vorsitz vertreten.
2. Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern.
3. Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Verordnung erlassenen Vorschriften zuständig, so wird im Einklang mit den nationalen Rechtsvorschriften dieses Mitgliedstaats ein gemeinsamer Vertreter benannt.
4. Die Kommission ist berechtigt, ohne Stimmrecht an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen. Die Kommission benennt einen Vertreter. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die Kommission über die Tätigkeiten des Europäischen Datenschutzausschusses.
5. In Fällen, die mit Artikel 58a im Zusammenhang stehen, ist der Europäische Datenschutzbeauftragte nur bei Beschlüssen stimmberechtigt, die Grundsätze und Vorschriften betreffen, die für die Organe, Einrichtungen, Ämter und Agenturen der Union gelten und inhaltlich den Grundsätzen und Vorschriften dieser Verordnung entsprechen.

## *Artikel 65*

### ***Unabhängigkeit***

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

## *Artikel 66*

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

1. Der Europäische Datenschutzausschuss stellt die einheitliche Anwendung dieser Verordnung sicher. Zu diesem Zweck nimmt der Europäische Datenschutzausschuss von sich aus oder gegebenenfalls auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr:
  - (aa) Überwachung und Sicherstellung der ordnungsgemäßen Anwendung dieser Verordnung in den in Artikel 57 Absatz 3 genannten Fällen unbeschadet der Aufgaben der nationalen Aufsichtsbehörden;
  - (a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, einschließlich etwaiger Vorschläge zur Änderung dieser Verordnung;
  - (aa) Beratung der Kommission über das Format und die Verfahren für den Austausch von Informationen zwischen den für die Verarbeitung Verantwortlichen, den Auftragsverarbeitern und den Aufsichtsbehörden in Bezug auf verbindliche unternehmensinterne Datenschutzvorschriften;
  - (ab) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zu Verfahren für die Löschung gemäß Artikel 17 Absatz 2 von Links zu personenbezogenen Daten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten;
  - (b) Prüfung – von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission – von die Anwendung dieser Verordnung betreffenden Fragen und Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;

- (ba) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen gemäß Artikel 20 Absatz 2;
- (bb) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zur Feststellung von Verletzungen der Datensicherheit sowie zur Bestimmung, was unter einer unangemessenen Verzögerung gemäß Artikel 31 Absätze 1 und 2 zu verstehen ist, und zu den spezifischen Umständen, unter denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden hat.
- (bc) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zu den Umständen, unter denen gemäß Artikel 32 Absatz 1 eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat;
- (bd) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zur näheren Bestimmung der in Artikel 43 aufgeführten Kriterien und Anforderungen für die Datenübermittlungen, die auf verbindlichen unternehmensinternen Datenschutzvorschriften von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern beruhen, und der dort aufgeführten weiteren erforderlichen Anforderungen zum Schutz personenbezogener Daten der betroffenen Personen;
- (be) (neu) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zur näheren Bestimmung der Kriterien und Bedingungen für die Datenübermittlungen gemäß Artikel 44 Absatz 1;
- (ba) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 53 Absätze 1, 1b und 1c und die Festsetzung von Geldbußen gemäß Artikel 79;
- (c) Überprüfung der praktischen Anwendung der unter den Buchstaben b und ba genannten Leitlinien, Empfehlungen und bewährten Verfahren;

- (ca0) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Artikel 66 Absatz 1 Buchstabe b zur Festlegung gemeinsamer Verfahren für die von natürlichen Personen vorgenommene Meldung von Verstößen gegen diese Verordnung gemäß Artikel 49 Absatz 2;
- (ca) Förderung der Ausarbeitung von Verhaltensregeln und der Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und -prüfzeichen gemäß den Artikeln 38 und 39;
- (cb) Akkreditierung von Zertifizierungsstellen und deren regelmäßige Überprüfung gemäß Artikel 39a und Führung eines öffentlichen Registers der akkreditierten Einrichtungen gemäß Artikel 39a Absatz 6 und der in Drittländern niedergelassenen akkreditierten für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gemäß Artikel 39 Absatz 4;
- (cd) Präzisierung der in Artikel 39a Absatz 3 genannten Anforderungen im Hinblick auf die Akkreditierung von Zertifizierungsstellen gemäß Artikel 39;
- (cda) Abgabe einer Stellungnahme für die Kommission zu den Zertifizierungsanforderungen gemäß Artikel 39a Absatz 7;
- (cdb) Abgabe einer Stellungnahme für die Kommission zu den Bildsymbolen gemäß Artikel 12 Absatz 4b;
- (ce) Abgabe einer Stellungnahme für die Kommission, in der die Angemessenheit des gebotenen Schutzniveaus in einem Drittland oder einer internationalen Organisation beurteilt und geprüft wird, ob das Drittland, das Gebiet, die internationale Organisation oder der spezifische Sektor kein angemessenes Schutzniveau mehr gewährleistet. Zu diesem Zweck versorgt die Kommission den Europäischen Datenschutzausschuss mit allen erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlands, dem Gebiet oder dem Verarbeitungssektor in diesem Drittland oder der internationalen Organisation;
- (d) Abgabe von Stellungnahmen im Kohärenzverfahren zu Beschlussentwürfen von Aufsichtsbehörden gemäß Artikel 57 Absatz 2 und zu Angelegenheiten, die nach Artikel 57 Absatz 4 vorgelegt wurden;

- (e) Förderung der Zusammenarbeit und eines effizienten bilateralen und multilateralen Austauschs von Informationen und Verfahren zwischen den Aufsichtsbehörden;
  - (f) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit Aufsichtsstellen internationaler Organisationen;
  - (g) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und -praxis mit Datenschutzaufsichtsbehörden in aller Welt;
  - (gb) Abgabe von Stellungnahmen zu den auf Unionsebene erarbeiteten Verhaltensregeln gemäß Artikel 38 Absatz 4;
  - (i) Führung eines öffentlich zugänglichen elektronischen Registers der Beschlüsse der Aufsichtsbehörden und Gerichte in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden.
2. Die Kommission kann, wenn sie den Europäischen Datenschutzausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist angeben.
  3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 87 genannten Ausschuss weiter und veröffentlicht sie.
  4. (...)
  - 4a. Der Europäische Datenschutzausschuss konsultiert gegebenenfalls interessierte Kreise und gibt ihnen Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Unbeschadet des Artikels 72 macht der Europäische Datenschutzausschuss die Ergebnisse der Konsultation der Öffentlichkeit zugänglich.

*Artikel 67*

***Berichterstattung***

1. (...)
2. Der Europäische Datenschutzausschuss erstellt einen Jahresbericht über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union und gegebenenfalls in Drittländern und internationalen Organisationen. Der Bericht wird veröffentlicht und dem Europäischen Parlament, dem Rat und der Kommission übermittelt.
3. Der Jahresbericht enthält eine Überprüfung der praktischen Anwendung der in Artikel 66 Absatz 1 Buchstabe c genannten Leitlinien, Empfehlungen und bewährten Verfahren sowie der in Artikel 57 Absatz 3 genannten verbindlichen Beschlüsse.

*Artikel 68*

***Verfahrensweise***

1. Sofern in dieser Verordnung nichts anderes bestimmt ist, fasst der Europäische Datenschutzausschuss seine Beschlüsse mit einfacher Mehrheit seiner Mitglieder.
2. Der Europäische Datenschutzausschuss gibt sich mit einer Mehrheit von zwei Dritteln seiner Mitglieder eine Geschäftsordnung und legt seine Arbeitsweise fest.

## *Artikel 69*

### *Vorsitz*

1. Der Europäische Datenschutzausschuss wählt aus dem Kreis seiner Mitglieder mit einfacher Mehrheit einen Vorsitzenden und zwei stellvertretende Vorsitzende.
2. Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre einmalige Wiederwahl ist zulässig.

## *Artikel 70*

### *Aufgaben des Vorsitzes*

1. Der Vorsitz hat folgende Aufgaben:
  - (a) Einberufung der Sitzungen des Europäischen Datenschutzausschusses und Erstellung der Tagesordnungen,
  - (aa) Übermittlung der Beschlüsse des Europäischen Datenschutzausschusses nach Artikel 58a an die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden,
  - (b) Sicherstellung einer rechtzeitigen Ausführung der Aufgaben des Europäischen Datenschutzausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 57.
2. Der Europäische Datenschutzausschuss legt die Aufteilung der Aufgaben zwischen dem Vorsitzenden und dessen Stellvertretern in seiner Geschäftsordnung fest.

## *Artikel 71*

### *Sekretariat*

1. Der Europäische Datenschutzausschuss wird von einem Sekretariat unterstützt, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird.
  - 1a. Das Sekretariat führt seine Aufgaben ausschließlich auf Anweisung des Vorsitzenden des Europäischen Datenschutzausschusses aus.

- 1b. Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Europäischen Datenschutzausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, unterliegt anderen Berichtspflichten als das Personal, das an der Wahrnehmung der dem Europäischen Datenschutzbeauftragten übertragenen Aufgaben beteiligt ist.
- 1c. Soweit angebracht, erstellen und veröffentlichen der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte eine Vereinbarung zur Anwendung dieses Artikels, in der die Bedingungen ihrer Zusammenarbeit festgelegt sind und die für das Personal des Europäischen Datenschutzbeauftragten gilt, das an der Wahrnehmung der dem Europäischen Datenschutzausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist.
2. Das Sekretariat leistet dem Europäischen Datenschutzausschuss analytische, administrative und logistische Unterstützung.
3. Das Sekretariat ist insbesondere verantwortlich für
  - (a) das Tagesgeschäft des Europäischen Datenschutzausschusses,
  - (b) die Kommunikation zwischen den Mitgliedern des Europäischen Datenschutzausschusses, seinem Vorsitz und der Kommission sowie die Kommunikation mit anderen Organen und mit der Öffentlichkeit,
  - (c) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation,
  - (d) die Übersetzung sachdienlicher Informationen,
  - (e) die Vor- und Nachbereitung der Sitzungen des Europäischen Datenschutzausschusses,
  - (f) die Vorbereitung, Abfassung und Veröffentlichung von Stellungnahmen, von Beschlüssen über die Beilegung von Streitigkeiten zwischen Aufsichtsbehörden und von sonstigen vom Europäischen Datenschutzausschuss angenommenen Dokumenten.

*Artikel 72*

***Vertraulichkeit***

1. Die Beratungen des Europäischen Datenschutzausschusses sind gemäß seiner Geschäftsordnung vertraulich, wenn der Ausschuss dies für erforderlich hält.
2. Der Zugang zu Dokumenten, die Mitgliedern des Europäischen Datenschutzausschusses, Sachverständigen und Vertretern von Dritten vorgelegt werden, wird durch die Verordnung (EG) Nr. 1049/2001 geregelt.
3. (...)

## KAPITEL VIII

### RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

#### *Artikel 73*

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

1. Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.
2. (...)
3. (...)
4. (...)
5. Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 74.

#### *Artikel 74*

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

1. Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine sie betreffende rechtsverbindliche Entscheidung einer Aufsichtsbehörde.

2. Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 51 und 51a zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 73 erhobenen Beschwerde in Kenntnis gesetzt hat.
3. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.
- 3a. Kommt es zu einem Verfahren gegen den Beschluss einer Aufsichtsbehörde, dem eine Stellungnahme oder ein Beschluss des europäischen Datenschutzausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.
4. (...)
5. (...)

#### *Artikel 75*

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

1. Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 73 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser erfolgenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.
2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

3. (...)

4. (...)

#### *Artikel 76*

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

1. Die betroffene Person hat das Recht, eine Einrichtung, eine Organisationen oder eine Vereinigung, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, die keinen Erwerbszweck verfolgt, deren satzungsmäßige Ziele von öffentlichem Interesse sind und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen Beschwerde zu erheben, die in den Artikeln 73, 74 und 75 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz gemäß Artikel 77 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.
2. Die Mitgliedstaaten können vorsehen, dass jede der in Absatz 1 genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der zuständigen Aufsichtsbehörde gemäß Artikel 73 eine Beschwerde einzulegen und die in den Artikeln 74 und 75 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte der betroffenen Person infolge einer nicht dieser Verordnung entsprechenden Datenverarbeitung verletzt worden sind.
3. (...)
4. (...)
5. (...)

#### *Artikel 76a*

#### ***Aussetzung des Verfahrens***

1. Erhält ein zuständiges Gericht in einem Mitgliedstaat Kenntnis von einem Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, das vor einem Gericht in einem anderen Mitgliedstaat anhängig ist, so nimmt es mit diesem Gericht Kontakt auf, um sich zu vergewissern, dass ein solches Verfahren existiert.

2. Ist ein Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen.
- 2a. Sind diese Verfahren in erster Instanz anhängig, so kann sich jedes später angerufene Gericht auf Antrag einer Partei auch für unzuständig erklären, wenn das zuerst angerufene Gericht für die betreffenden Klagen zuständig ist und die Verbindung der Klagen nach seinem Recht zulässig ist.

#### *Artikel 77*

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

1. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder moralischer Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.
2. Jeder an der Verarbeitung beteiligte für die Verarbeitung Verantwortliche haftet für den Schaden, der durch die nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch die Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
4. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

5. Hat ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser für die Verarbeitung Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.
6. Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 75 Absatz 2 genannten nationalen Rechtsvorschriften des Mitgliedstaats zuständig sind.

*Artikel 78*

***Sanktionen***

(...)

*Artikel 79*

***Allgemeine Bedingungen für die Verhängung von Geldbußen***

- 1a. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 3 (neu), 3a (neu) und 3aa (neu) in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
2. (...)
- 2a. Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 53 Absatz 1b Buchstaben a bis fa und h verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
  - (a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

- (b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- (c) (...)
- (d) die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- (e) Grad der Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 23 und 30 getroffenen technischen und organisatorischen Maßnahmen;
- (f) etwaige einschlägige frühere Verstöße des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters;
- (g) (neu) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- (ga) (neu) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- (h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- (i) Einhaltung der nach Artikel 53 Absatz 1b früher gegen den für den betreffenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, falls solche Maßnahmen angeordnet wurden;
- (j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 38 oder genehmigten Zertifizierungsverfahren nach Artikel 39;
- (k) (...)
- (m) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

2b. Verstößt ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so darf der Gesamtbetrag der Geldbuße den Betrag für den schwerwiegendsten Verstoß nicht übersteigen.

3. (...)

3(new). Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2a Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

(a) die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 10, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39 und 39a;

(aa) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 39 und 39a;

(ab) die Pflichten der Überwachungsstelle gemäß Artikel 38a Absatz 4.

3a(neu). Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2a Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

(a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

(b) die Rechte der betroffenen Person gemäß den Artikeln 12-20;

(ba) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 40-44;

(bb) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

(c) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1b oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 53 Absatz 1.

- 3aa(neu). Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 53 Absatz 1b werden im Einklang mit Absatz 2a Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.
- 3b. Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 53 Absatz 1b kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.
4. Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien in Übereinstimmung mit dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.
5. Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann Artikel 79 so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die entsprechenden Rechtsvorschriften sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.
6. (...)
7. (...)

*Artikel 79b*

***Sanktionen***

1. Die Mitgliedstaaten legen die Vorschriften über Sanktionen für Verstöße gegen diese Verordnung – insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 79 unterliegen – fest und ergreifen alle erforderlichen Maßnahmen, um deren Durchführung zu gewährleisten. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.
2. (...)
3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er nach Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

# KAPITEL IX

## VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN

### *Artikel 80*

#### *Verarbeitung personenbezogener Daten und Freiheit der Meinungsäußerung und Informationsfreiheit*

1. Die Mitgliedstaaten bringen durch Gesetz das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung personenbezogener Daten zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.
2. Für die Verarbeitung personenbezogener Daten, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von den Bestimmungen des Kapitels II (Grundsätze), des Kapitels III (Rechte der betroffenen Person), des Kapitels IV (Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter), des Kapitels V (Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen), des Kapitels VI (Unabhängige Aufsichtsbehörden), des Kapitels VII (Zusammenarbeit und Kohärenz) und des Kapitels IX (Besondere Datenverarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.
3. Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er nach Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

*Artikel 80a*

***Verarbeitung personenbezogener Daten und Zugang der Öffentlichkeit zu amtlichen Dokumenten***

Personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, können von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die Behörde oder Einrichtung unterliegt, freigegeben werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung in Einklang zu bringen.

*Artikel 80aa*

***Verarbeitung personenbezogener Daten und Weiterverwendung von Informationen des öffentlichen Sektors***

(...)

*Artikel 80b*

***Verarbeitung einer nationalen Kennziffer***

Die Mitgliedstaaten können näher bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. In diesem Fall darf die nationale Kennziffer oder das andere Kennzeichen von allgemeiner Bedeutung nur unter Wahrung angemessener Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung verwendet werden.

*Artikel 81*

***Verarbeitung personenbezogener Daten für Gesundheitszwecke***

(...)

*Artikel 81a*

***Verarbeitung genetischer Daten***

(...)

## Artikel 82

### *Datenverarbeitung im Beschäftigungskontext*

1. Die Mitgliedstaaten können durch Gesetz oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.
2. Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Datenübermittlung innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen und die Überwachungssysteme am Arbeitsplatz.
- 2a. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er nach Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.
3. (...)

### *Artikel 83*

#### *Garantien und Ausnahmen in Bezug auf die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken und zu statistischen Zwecken*

1. Die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken unterliegt gemäß dieser Verordnung angemessenen Garantien für die Rechte und Freiheiten der betroffenen Person. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung von Daten, bei der die Bestimmung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.
2. Werden personenbezogene Daten zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 17a und 19 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.
3. Werden personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 17a, 17b, 18 und 19 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.
4. Dient die in den Absätzen 2 und 3 genannte Verarbeitung gleichzeitig einem anderen Zweck, gelten die Ausnahmen nur für die Verarbeitung zu den in diesen Absätzen genannten Zwecken.

## *Artikel 84*

### ***Geheimhaltungspflichten***

1. Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 53 Absatz 1 Buchstaben da und db gegenüber den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeitern, die nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder nach von den zuständigen nationalen Stellen erlassenen Regelungen dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in Bezug auf personenbezogene Daten, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.
2. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Vorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

## *Artikel 85*

### ***Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften***

1. Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.
2. Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Kontrolle durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

# KAPITEL X

## DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

### *Artikel 86*

#### *Ausübung der Befugnisübertragung*

1. Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.
2. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 12 Absatz 4c und Artikel 39a Absatz 7 wird der Kommission auf unbestimmte Zeit ab dem Zeitpunkt des Inkrafttretens dieser Verordnung übertragen.
3. Die Befugnisübertragung gemäß Artikel 12 Absatz 4c und Artikel 39a Absatz 7 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.
4. Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.
5. Ein delegierter Rechtsakt, der gemäß Artikel 12 Absatz 4c und Artikel 39a Absatz 7 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

*Artikel 87*

***Ausschussverfahren***

1. Die Kommission wird von einem Ausschuss unterstützt. Bei diesem Ausschuss handelt es sich um einen Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.
2. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.
3. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

# KAPITEL XI

## SCHLUSSBESTIMMUNGEN

### *Artikel 88*

#### ***Aufhebung der Richtlinie 95/46/EG***

1. Die Richtlinie 95/46/EG wird zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt aufgehoben.
2. Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

### *Artikel 89*

#### ***Verhältnis zur Richtlinie 2002/58/EG***

Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

### *Artikel 89b*

#### ***Verhältnis zu bereits geschlossenen Übereinkünften***

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

## Artikel 90

### **Bewertung**

1. Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor.
2. Im Rahmen dieser Bewertungen prüft die Kommission insbesondere die Anwendung und die Wirkungsweise der Bestimmungen
  - (a) des Kapitels V über die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen insbesondere im Hinblick auf die gemäß Artikel 41 Absatz 3 erlassenen Beschlüsse sowie die gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen,
  - (b) des Kapitels VII über Zusammenarbeit und Kohärenz.
- 2a. Für den in Absatz 1 genannten Zweck kann die Kommission von den Mitgliedstaaten und den Aufsichtsbehörden Informationen anfordern.
- 2b. Bei den in den Absätzen 1 und 2 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.
3. Der erste Bericht wird spätestens vier Jahre nach Inkrafttreten dieser Verordnung vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Die Berichte werden veröffentlicht.
4. Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor, wobei sie insbesondere der Entwicklung der Informationstechnologie und den Fortschritten in der Informationsgesellschaft Rechnung trägt.

*Artikel 90a (neu)*

***Überprüfung anderer Datenschutzinstrumente der EU***

Die Kommission legt gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsinstrumente der EU zum Schutz personenbezogener Daten vor, damit ein einheitlicher und kohärenter Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sichergestellt wird. Dies betrifft insbesondere die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien **Verkehr** solcher Daten.

*Artikel 91*

***Inkrafttreten und Anwendung***

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

***\*ABL.: Bitte Datum einfügen.***

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

Geschehen zu Brüssel am

*Im Namen des Europäischen Parlaments*

*Im Namen des Rates*

*Der Präsident*

*Der Präsident*