



Brüssel, den 11. Juni 2015  
(OR. en)

9565/15

---

---

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

---

---

**DATAPROTECT 97  
JAI 420  
MI 369  
DIGIT 49  
DAPIX 94  
FREMP 133  
COMIX 259  
CODEC 823**

#### **VERMERK**

---

Absender: Vorsitz

Empfänger: Rat

---

Nr. Vordok.: 9398/15

---

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)  
– Vorbereitung einer allgemeinen Ausrichtung

---

#### Einleitung

Die Kommission hat ihren Vorschlag für die Datenschutz-Grundverordnung (Dokument 5853/12) am 25. Januar 2012 angenommen. Mit der neuen Verordnung soll die Richtlinie 95/46/EG ersetzt werden. Das Ziel der Verordnung besteht zum einen in einer Stärkung der Datenschutzrechte natürlicher Personen und zum anderen in verbesserten Geschäftsmöglichkeiten durch die Erleichterung des freien Verkehrs personenbezogener Daten im digitalen Binnenmarkt.

Parallel zu dem Vorschlag für die Datenschutz-Grundverordnung verabschiedete die Kommission eine Mitteilung zu ihren politischen Zielen (Dokument 5812/12) und den Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten für die Zwecke der Strafverfolgung (Dokument 5833/12). Mit der neuen Richtlinie soll der Datenschutz-Rahmenbeschluss von 2008 ersetzt werden.

Das Europäische Parlament hat seinen Standpunkt in erster Lesung zum Vorschlag für die Datenschutzverordnung und zum Vorschlag für die Datenschutzrichtlinie am 12. März 2014 angenommen.

### Kompromisstext

Mehrere partielle allgemeine Ausrichtungen haben zu einer Annäherung der Standpunkte im Rat zu dem Vorschlag für die Datenschutz-Grundverordnung insgesamt geführt. Der Text der Verordnung, wie ihn der Vorsitz nunmehr im Hinblick auf die Billigung als allgemeine Ausrichtung vorlegt, ist in der Anlage wiedergegeben. Alle Änderungen gegenüber dem ursprünglichen Vorschlag der Kommission sind unterstrichen wiedergegeben, Streichungen sind durch (...) gekennzeichnet. Textteile, die gestrichen und an anderer Stelle wieder eingefügt wurden, sind *kursiv* gedruckt. Die Bemerkungen der Delegationen zum Text der Verordnung – in dem die neuen Vorschläge des Vorsitzes zu den Erwägungsgründen 118 und 134 noch nicht enthalten waren – finden sich in der Darlegung der Ergebnisse der Beratungen des Ausschusses der Ständigen Vertreter auf seiner Tagung vom 9. Juni 2015 (Dokument 9788/15).

Unter Berücksichtigung der Tagung des Ausschusses der Ständigen Vertreter vom 9. Juni 2015 hat der Vorsitz zwei Änderungen vorgenommen.

#### *Haftung und Recht auf Schadenersatz – Artikel 77 und Erwägungsgrund 118*

Der Vorsitz schlägt vor, Erwägungsgrund 118 zu ändern, um zu präzisieren, dass das übergeordnete Ziel des Artikels 77 und des Erwägungsgrunds 118 darin besteht, der betroffenen Person einen vollständigen und wirksamen Schadenersatz für erlittenen Schaden zu gewährleisten. In Anbetracht dessen, dass die rechtlichen Regelungen bei Haftungsstreitigkeiten von Mitgliedstaat zu Mitgliedstaat unterschiedlich ausfallen, kann die betroffene Person einen derartigen Schadenersatz von dem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter erhalten, der gesamtschuldnerisch haftet, oder – in den Mitgliedstaaten, deren Rechtsordnung verbundene Verfahren zulässt – kann dieser Schadenersatz anteilmäßig auf mehr als einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter aufgeteilt werden.

Um denjenigen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern, die derzeit bei der Verarbeitung personenbezogener Daten die Richtlinie 95/46/EG einhalten, ein ausreichendes Maß an Rechtssicherheit zu gewährleisten, schlägt der Vorsitz vor, den Anwendungsbereich der Verordnung in Erwägungsgrund 134 zu präzisieren.

Fazit

Um den Vorsitz mit einem Mandat zur Aufnahme der Verhandlungen mit den Vertretern des Europäischen Parlaments auszustatten, wird der Rat ersucht, den Text der Datenschutz-Grundverordnung in der in der Anlage wiedergegebenen Fassung als allgemeine Ausrichtung zu billigen.

---

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)**

(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 Absatz 2 (...),

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,

nach Anhörung des Europäischen Datenschutzbeauftragten,

gemäß dem ordentlichen Gesetzgebungsverfahren,

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 Binnenmarktes sowie zum Wohlergehen der Menschen beitragen.
  - 3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr 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) Das Recht auf Schutz der personenbezogenen Daten kann keine uneingeschränkte Geltung beanspruchen; 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 Binnenmarktes hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs geführt. Der unionsweite Datenaustausch zwischen (...) öffentlichen und privaten Akteuren einschließlich Einzelpersonen 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, in dem Daten ausgetauscht und erhoben werden, ist dramatisch gestiegen. 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 Maß an Datenschutz zu gewährleisten ist.
- 6) Diese Entwicklungen erfordern einen soliden, kohärenteren und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, um eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Jede Person sollte die Kontrolle über ihre eigenen Daten besitzen, und private Nutzer, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.
- 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 Schutz der Rechte und Grundfreiheiten von Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, kann den 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 gleichmäßig hohes Maß an Datenschutz für den Einzelnen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte der Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit kohärent und einheitlich angewandt werden. 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. Innerhalb dieses Spielraums sollten die Mitgliedstaaten sektorspezifische Rechtsvorschriften, die sie zur Umsetzung der Richtlinie 95/46/EG erlassen haben, beibehalten können.

- 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 jeder in der Union das gleiche Maß an Datenschutz genießt und Unterschiede, die den freien Datenverkehr im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die überall in der Union für die Wirtschaftsteilnehmer einschließlich Kleinunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, den Einzelnen mit denselben durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter vorsieht (...) und eine einheitliche Kontrolle der Verarbeitung personenbezogener Daten und gleiche 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 Kleinunternehmen 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 Kleinunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs "Kleinunternehmen sowie kleines und mittleres 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) Die Verordnung behandelt weder Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Datenverkehrs im Zusammenhang mit Tätigkeiten, die (...) nicht in den Anwendungsbereich des Unionsrechts fallen, 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 werden.
- 15) Diese Verordnung sollte nicht für die Verarbeitung von personenbezogenen Daten gelten, die von einer natürlichen Person im Zuge einer persönlichen oder familiären Tätigkeit und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche und familiäre Tätigkeiten gelten auch die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher persönlichen und familiären Tätigkeiten. 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, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, zur Vollstreckung strafrechtlicher Sanktionen oder zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit sowie der freie Verkehr solcher Daten sind in einem eigenen EU-Rechtsinstrument geregelt.

Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen 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 für die Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt, als sie in den 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 die Verordnung für die Verarbeitung personenbezogener Daten durch (...) private Einrichtungen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen beschränken können, wenn dies in einer demokratischen Gesellschaft für den Schutz bestimmter wichtiger Interessen, wozu auch die öffentliche Sicherheit und die Verhütung, Untersuchung, Aufdeckung, und Verfolgung von Straftaten zählen, notwendig und verhältnismäßig ist. 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 Richtlinie 2000/31/EG gilt nicht für Dienste der Informationsgesellschaft betreffende Fragen, die von der vorliegenden Verordnung erfasst werden. Diese Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt. Ihre Anwendung sollte durch die vorliegende Verordnung nicht beeinträchtigt werden. Die vorliegende Verordnung sollte daher die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste nicht berühren.
- 18) (...)
- 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 ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen in der Union anzubieten. Um festzustellen, ob ein für die Verarbeitung Verantwortlicher diesen betroffenen Personen in der Union Waren oder Dienstleistungen anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Geschäfte mit in einem oder mehreren Mitgliedstaaten der Union ansässigen betroffenen Personen zu tätigen. Während die bloße Zugänglichkeit der Website eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters 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 ansässigen 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 ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser Personen in der Europäischen Union zu beobachten. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten mit Hilfe von Datenverarbeitungstechniken nachvollzogen werden, 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 EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.

23) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Daten einschließlich pseudo-  
nymisierter Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen  
Person zugeordnet werden könnten, sollten als Informationen über eine bestimmbare  
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. Bei Prüfung der Frage, ob Mittel nach  
allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden,  
sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür  
erforderliche Zeitaufwand, herangezogen werden, wobei sowohl die zum Zeitpunkt der  
Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu  
berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme  
Informationen gelten, d.h. für Informationen, die sich nicht auf eine bestimmte oder  
bestimmbare natürliche Person beziehen, oder Daten, die in einer Weise anonymisiert worden  
sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese  
Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für  
statistische und für Forschungszwecke. .

23aa) Die Grundsätze des Datenschutzes sollten nicht für die Daten Verstorbener gelten. Im  
nationalen Recht eines Mitgliedstaats können Vorschriften über die Verarbeitung der Daten  
Verstorbener vorgesehen sein.

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 verfügenden 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 die Umsetzung dieser Verordnung zu gewährleisten, wobei die jeweilige Datenverarbeitung zu berücksichtigen und 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. In diesem Fall stellt der für die Verarbeitung Verantwortliche jedoch sicher, dass in den Metadaten nicht auf die Personen Bezug genommen wird, die die Pseudonymisierung vornehmen.
- 24) Bei der Inanspruchnahme von Online-Diensten werden dem Nutzer unter Umständen Online-Kennungen wie IP-Adressen oder Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, zugeordnet. Dies kann Spuren hinterlassen, die 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. Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente sollten als solche nicht (...) als personenbezogene Daten betrachtet werden, wenn mit ihnen keine Person bestimmt oder bestimmbar gemacht wird.
- 25) Die Einwilligung sollte eindeutig auf beliebige geeignete Weise erfolgen, die eine ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene Willensbekundung der betroffenen Person in Form einer schriftlichen, auch elektronischen, oder mündlichen Erklärung oder, wenn aufgrund besonderer Umstände erforderlich, in Form einer anderen eindeutigen Handlung ermöglicht, mit der diese Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite geschehen oder durch jede sonstige Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Ein stillschweigendes Einverständnis ohne Zutun der betroffenen Person sollte daher keine Einwilligung darstellen. Soweit technisch machbar und wirksam, kann die Einwilligung der betroffenen Person durch die Benutzung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung erfolgen. In diesen Fällen ist es ausreichend, wenn die betroffene Person zu Beginn des Nutzungsvorgangs die Informationen erhält, die für eine ohne Zwang und in Kenntnis der Sachlage erteilte Einwilligung für den konkreten Fall erforderlich sind. (...). 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 eindeutige 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.

- 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.
- 25aa) Oftmals kann der Zweck der Datenverarbeitung für wissenschaftliche Zwecke zum Zeitpunkt der Datenerhebung nicht vollständig angegeben werden. Daher sollten betroffene Personen ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung geben können, wenn anerkannte ethische Standards für die wissenschaftliche Forschung eingehalten werden. Unter der Voraussetzung, dass dies keinen unverhältnismäßigen Aufwand im Hinblick auf den Schutzzweck mit sich bringt, sollten die betroffenen Personen Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.
- 26) Zu den personenbezogenen Gesundheitsdaten sollten (...) Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über die bisherige, derzeitige und künftige körperliche oder geistige Gesundheit der betroffenen Person hervorgehen; dazu gehören auch Informationen über die Vormerkung der Person zur Erbringung medizinischer Leistungen, (...) 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 für die Verarbeitung verantwortlichen 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 von Eigentümerschaft, finanzieller Beteiligung oder sonstiger Bestimmungen, die die Tätigkeit des Unternehmens regeln, oder der Befugnis, Datenschutzvorschriften einzuführen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Eine 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.
- 30) Jede Verarbeitung personenbezogener Daten sollte nach Recht und Gesetz 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 für die Zwecke der Datenverarbeitung angemessen und sachlich relevant (...) sein; dies heißt insbesondere, dass nicht unverhältnismäßig viele Daten erfasst werden und die Speicherfrist auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. (...). Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht 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.
- 32) 31a) Wann immer sich diese Verordnung auf eine Rechtsgrundlage oder eine Legislativmaßnahme 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 Legislativmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte gefordert.
- 33) 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. Eine vom für die Verarbeitung Verantwortlichen vorformulierte Einwilligungserklärung sollte in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden; der Inhalt der Erklärung sollte im Gesamtkontext nicht unüblich sein. 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 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 Datenverarbeitungsprozessen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird, obwohl dies für diese Erfüllung nicht erforderlich ist, und der betroffenen Person ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht in zumutbarer Weise möglich ist.
- 35) Die Verarbeitung von Daten sollte rechtmäßig sein, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.
- 36) 35a) Diese Verordnung enthält allgemeine Vorschriften über den Datenschutz und sieht vor, dass in besonderen Fällen die Mitgliedstaaten auch befugt sind, einzelstaatliche Vorschriften über den Datenschutz zu erlassen. Die Verordnung schließt daher 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. Das nationale Recht kann auch spezielle Verarbeitungsbedingungen für spezifische Sektoren und für die Verarbeitung spezieller Kategorien von Daten vorsehen.
- 37) 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 hoheitlicher Gewalt erforderlich, muss hierfür eine (...) Grundlage im Unionsrecht oder im nationalen Recht eines Mitgliedstaats bestehen. (...). Desgleichen sollte im Unionsrecht oder im nationalen Recht 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 nach Recht und Gesetz erfolgt.

Desgleichen sollte im Unionsrecht oder im nationalen Recht geregelt werden, ob es sich bei dem für die Verarbeitung Verantwortlichen, der eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln soll, 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.

- 38) 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. (...). 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 erforderlich sein.
- 39) 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. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine relevante und angemessene Verbindung 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, absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Dabei ist besonders zu berücksichtigen, ob es sich bei der betroffenen Person um ein Kind handelt, da Kinder besonders schutzwürdig sind. Die betroffene Person sollte das Recht haben, aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Verarbeitung zu widersprechen, ohne dass ihr dadurch Kosten entstehen. Aus Transparenzgründen sollte der für die Verarbeitung Verantwortliche verpflichtet werden, seine berechtigten Interessen gegenüber der betroffenen Person ausdrücklich darzulegen und diese außerdem zu dokumentieren und die betroffene Person über ihr Widerspruchsrecht zu belehren. (...)

- 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 Mitarbeitern, 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 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, die Verbreitung schädlicher Programmcodes, die Abwehr von Angriffen in Form der gezielten Überlastung von Servern ("Denial of access"-Angriffe) sowie Schädigungen von Computer- und elektronischen Kommunikationssystemen zu verhindern. Die Verarbeitung personenbezogener Daten in dem für die Verhinderung von Betrug unbedingt erforderlichen Umfang ist ebenfalls ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

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 erfolgt sie in Ausübung hoheitlicher Gewalt, 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 rechtmäßig erachtet wird. (...) Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für statistische, wissenschaftliche oder historische Zwecke (...) oder im Hinblick auf eine künftige Streitbeilegung sollte als konformer rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung zu anderen Zwecken dienen, wenn diese Zwecke den zugewiesenen Aufgaben entsprechen und der für die Verarbeitung Verantwortliche in rechtlicher Hinsicht berechtigt ist, die Daten für diese anderen Zwecke zu erheben.

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, was die realistischen Erwartungen der betroffenen Person in Bezug auf die weitere Verwendung dieser Daten einschließt, 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 Verarbeitungsvorgang geeignete Garantien bestehen. Ist der beabsichtigte andere Zweck nicht mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar, so muss der für die Verarbeitung Verantwortliche hierfür die Einwilligung der betroffenen Person einholen oder die Verarbeitung auf einen anderen Rechtmäßigkeitsgrund stützen, der sich beispielsweise aus dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, ergibt. (...).

In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke unterrichtet wird und ihre Rechte einschließlich des Widerspruchsrechts gewahrt werden. (...). Der Hinweis des für die Verarbeitung Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung dieser Daten an eine zuständige Behörde sollten als im berechtigten 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 auf sonstige Weise verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

- 41) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und -freiheiten (...) besonders sensibel sind, bedürfen eines besonderen Schutzes, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und -freiheiten auftreten können. Diese Daten sollten auch personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Tatsache, dass in dieser Verordnung der Begriff "rassische Herkunft" verwendet wird, nicht bedeutet, dass die Europäische Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Derartige Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten konkreten 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 speziellen Kategorien personenbezogener Daten sollten u.a. 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.

Bestimmte Kategorien personenbezogener Daten können auch verarbeitet werden, wenn die Daten offenkundig öffentlich gemacht wurden oder dem für die Verarbeitung Verantwortlichen freiwillig und auf Wunsch der betroffenen Person für einen bestimmten, von der betroffenen Person angegebenen Zweck übermittelt wurden und die Verarbeitung im Interesse der betroffenen Person erfolgt.

Im Recht der Mitgliedstaaten und der Union kann vorgesehen werden, dass das allgemeine Verbot der Verarbeitung dieser speziellen Kategorien personenbezogener Daten in bestimmten Fällen durch die ausdrückliche Zustimmung der betroffenen Person nicht aufgehoben werden darf.

- 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 der sozialen Sicherheit und des Sozialschutzes einschließlich Renten und zwecks Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerer Gesundheitsgefahren oder zwecks Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung, den Gesundheitsdienstleistungen, Arzneimitteln und Medizinprodukten oder zwecks Bewertung der öffentlichen Maßnahmen im Gesundheitsbereich, u.a. durch die Ausarbeitung von Qualitäts- und Tätigkeitsindikatoren.

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 historischen, statistischen und wissenschaftlichen 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 der Gesundheitsversorgung oder Sozialfürsorge, 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 Gesundheitsversorgung und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu historischen, statistischen oder wissenschaftlichen Zwecken sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher die Bedingungen für die Verarbeitung spezieller 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 bzw. der Mitgliedstaaten sollten besondere und geeignete Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden. (...).
- 42b) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, spezielle Kategorien personenbezogener (...) Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung unterliegt geeigneten und besonderen Maßnahmen zum Schutz der Grundrechte und -freiheiten natürlicher Personen. 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.
- 46) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information leicht zugänglich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte auch 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, (...) was Instrumente zur Wahrnehmung insbesondere des Auskunftsrechts und des Rechts auf Berichtigung oder Löschung von Daten und zur Ausübung des Widerspruchsrechts einschließt. 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 ungebührliche Verzögerung und spätestens innerhalb einer festgelegten Frist von einem Monat zu beantworten und gegebenenfalls zu begründen, warum er ihn ablehnt.

Bei offenkundig unbegründeten oder unverhältnismäßigen Anträgen, zum Beispiel wenn die betroffene Person ungebührlich und wiederholt Informationen verlangt oder wenn die betroffene Person ihr Recht auf Information missbraucht, beispielsweise indem sie in ihrem Antrag falsche oder irreführende Angaben macht, könnte sich der für die Verarbeitung Verantwortliche weigern, aufgrund des Antrags tätig zu werden.

- 48) Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person (...) über die Existenz des Verarbeitungsvorgangs und seine Zwecke (...) informiert wird. Der für die Verarbeitung Verantwortliche sollte der betroffenen Person alle sonstigen Informationen zur Verfügung stellen, die 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.
- 49) Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung mitgeteilt werden oder, falls die Daten nicht bei ihr erhoben werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die Daten rechtmäßig an einen anderen Empfänger weitergegeben werden dürfen, sollte die betroffene Person bei der erstmaligen Weitergabe der Daten an diesen Empfänger darüber aufgeklärt werden. 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 historischen, statistischen oder wissenschaftlichen 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. Dabei dürfen die Grundrechte und Grundfreiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigem Eigentums und insbesondere das Urheberrecht an Software, nicht angetastet 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. (...) 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. 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 Unionsrecht oder gegen das Recht des Mitgliedstaats, 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 historischen, statistischen oder wissenschaftlichen 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 Querverweise zu diesen Daten oder Kopien oder Replikationen zu löschen sind.

Der für die Verarbeitung Verantwortliche sollte im Hinblick auf Daten, für deren Veröffentlichung er die Verantwortung trägt, (...) Schritte, auch technischer Art, unternehmen, die in Anbetracht der verfügbaren Technologie und der ihm zur Verfügung stehenden Mittel vertretbar sind, damit die genannte Information die betroffenen Dritten auch tatsächlich erreicht. (...).

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 erfolgen, 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 und maschinenlesbaren Format zu erhalten und sie einem anderen für die Verarbeitung Verantwortlichen zu übermitteln.

Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer ausdrücklichen Einwilligung oder im Zuge der Erfüllung eines Vertrags zur Verfügung gestellt hat. 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, personenbezogene Daten zu übermitteln, 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 Übermittlung der Daten die Anforderungen dieser Verordnung an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in Bezug auf eine andere betroffene Person 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. (...)

- 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 unentgeltlich, einfach und wirksam Widerspruch gegen eine solche ursprüngliche oder spätere – Verarbeitung einlegen können.

58) Die betroffene Person sollte das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in erheblichem Maße 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 erheblichem Maße beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich Profiling, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, zulässig ist, auch um 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 persönliches Eingreifen, 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 Überzeugung, Religion oder Weltanschauung, Mitgliedschaft in einer Gewerkschaft, sexueller Orientierung oder Geschlechtsidentität 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 (allgemeinen) Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten (Rechtsgrundlage für die Verarbeitung, Datenschutzgrundsätze usw.), wobei besondere Garantien gelten (beispielsweise Pflicht zur Durchführung einer Folgenabschätzung in einigen Fällen oder Bestimmungen über bestimmte Informationen, die der betroffenen Person zur Verfügung zu stellen sind). Der Europäische Datenschutzausschuss sollte die Möglichkeit haben, Leitlinien diesbezüglich herauszugeben.
- 59) Im Unionsrecht oder im Recht der Mitgliedstaaten können Beschränkungen bestimmter Grundsätze sowie des Rechts auf Unterrichtung, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch, von Maßnahmen, 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 und 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 – wie etwa die Ausführung einer der Internationalen Rotkreuz- und Rothalbmondbewegung obliegenden Aufgabe –, 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.
- 59a) Diese Verordnung sollte in keiner Weise von (...) dem auf internationalem Recht beruhendem, in Gerichts- und Verwaltungsverfahren anzuwendenden Privileg der Nichtoffenlegung vertraulicher Informationen des Internationalen Komitees vom Roten Kreuz abweichen. (...).

- 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 Maßnahmen treffen müssen und nachweisen können, dass (...) die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen (...). Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die persönlichen Rechte und Freiheiten berücksichtigen.
- 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 Umkehr der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische 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 und prognostiziert werden, um ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft (...).
- 60b) Eintrittswahrscheinlichkeit und Schwere des Risikos sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes Risiko der Beeinträchtigung der persönlichen Rechte und Freiheiten (...).

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 geeignete 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 sicherstellen, dass die für die Verarbeitung Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

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 ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf in der Union ansässige betroffene Personen beziehen und dazu dienen, diesen Personen Waren oder Dienstleistungen anzubieten oder deren Verhalten in der Union zu beobachten, (...) sollte einen Vertreter benennen müssen, es sei denn, (...) die von ihm ausgeführte Verarbeitung erfolgt vereinzelt und bringt unter Berücksichtigung ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich kein Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich oder bei dem für die Verarbeitung Verantwortlichen handelt es sich um eine Behörde oder öffentliche Einrichtung (...). Der Vertreter sollte im Namen des für die Verarbeitung Verantwortlichen tätig werden und den Aufsichtsbehörden als Ansprechpartner dienen. Der für die Verarbeitung Verantwortliche 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 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 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 Unionsrecht oder dem Recht des betreffenden Mitgliedstaats erfolgen, der 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 oder Bestandteil einer im Rahmen des Zertifizierungsverfahrens erteilten Zertifizierung sind. Nach Beendigung der Verarbeitung im Namen des für die Verarbeitung Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten zurückgeben oder löschen, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er 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 Aufzeichnungen über alle Kategorien von 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 die entsprechenden Aufzeichnungen 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 treffen. Diese Maßnahmen müssen unter Berücksichtigung der verfügbaren Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. (...). Bei der Bewertung 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 Umkehr der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile. (...) Deshalb sollte der für die Verarbeitung Verantwortliche nach Bekanntwerden einer (...) Verletzung des Schutzes personenbezogener Daten, die einen (...) physischen, materiellen oder moralischen Schaden nach sich ziehen kann, die Aufsichtsbehörde ohne ungebührliche Verzögerung – falls möglich binnen 72 Stunden – davon in Kenntnis setzen. Falls die Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen. Natürliche Personen, deren Rechte und Freiheiten durch die Datenschutzverletzung erheblich beeinträchtigt werden könnten, sollten ohne unangemessene Verzögerung benachrichtigt werden, damit sie die erforderlichen Vorkehrungen treffen können. (...). Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden (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 ähnliche 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) Die Benachrichtigung der betroffenen Person von der Verletzung des Schutzes personenbezogener Daten sollte nicht erforderlich sein, wenn der für die Verarbeitung Verantwortliche geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Zu diesen technischen Sicherheitsvorkehrungen sollte zählen, dass die betreffenden Daten für alle Personen, die nicht zum Zugriff auf sie befugt sind, unverständlich gemacht werden, insbesondere durch Verschlüsselung der personenbezogenen Daten (...).
- 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 spezifischer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten in Bezug auf 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 Nutzung einer Dienstleistung hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung (...) personenbezogener Daten sollte ungeachtet des Volumens oder der Art der Daten nicht als umfangreich gelten, wenn die Verarbeitung dieser Daten dem Berufsgeheimnis unterliegt (...), wie etwa die Verarbeitung personenbezogener Daten von Patienten oder Kunden durch einen einzelnen Arzt, einen Angehörigen der Gesundheitsberufe, ein Krankenhaus oder einen Anwalt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

- 72) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten sinnvoll sein, eine Datenschutz-Folgenabschätzung nicht auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen – beispielsweise wenn Behörden oder öffentliche Einrichtungen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere für die Verarbeitung Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.
- 73) Datenschutz-Folgeabschätzungen können von einer Behörde oder öffentlichen Einrichtung durchgeführt werden, sofern eine solche Folgenabschätzung nicht schon anlässlich des Erlasses des Gesetzes erfolgt ist, auf dessen Grundlage die Behörde oder Einrichtung ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt.
- 74) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ungeachtet geplanter Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen (...), 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 einem bestimmtem Umfang und einer bestimmten Häufigkeit der Verarbeitung verbunden, die für die betroffenen Personen auch eine (...) Schädigung oder eine (...) Beeinträchtigung ihrer Rechte und Freiheiten mit sich bringen können. Sie sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende 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 im öffentlichen Sektor oder durch ein privates Großunternehmen erfolgt oder in denen die Kerntätigkeit eines Unternehmens ungeachtet seiner Größe Verarbeitungsvorgänge einschließt, die einer regelmäßigen und systematischen Überwachung bedürfen, kann 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. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich um Angestellte 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, im Einklang mit dieser Verordnung stehende Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Eigenheiten 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 Erzeugnisse und Dienstleistungen ermöglichen.

- 78) Der grenzüberschreitende Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und wieder zurück ist für die Entwicklung des internationalen Handels und der grenzüberschreitenden Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Der durch diese Verordnung unionsweit garantierte Schutz natürlicher Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an für die Verarbeitung Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht unterminiert werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation stammende personenbezogene Daten an für die Verarbeitung Verantwortliche, Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weitergegeben werden. 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 Schutzklauseln beinhalten, um die Rechte der betroffenen Personen zu schützen.

- 80) Die Kommission darf (...) mit Wirkung für die gesamte Union feststellen, dass bestimmte Drittländer oder ein Gebiet oder ein bestimmter Sektor wie z.B. der private Sektor oder ein oder mehrere bestimmte Wirtschaftszweige eines Drittlands oder eine internationale Organisation einen angemessenen Datenschutz bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, einen solchen Schutz zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne besondere Genehmigung an diese Länder übermittelt werden.
- 81) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung eines Drittlandes oder eines Gebietes oder eines bestimmten Sektors in einem Drittland berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, ein Rechtsschutz existiert und die internationalen Menschenrechtsbestimmungen eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und öffentliche Ordnung sowie das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor in einem Drittland sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmten Verarbeitungsvorgängen und des Geltungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, insbesondere in Fällen, in denen Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den europäischen Datenschutzbehörden vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame behördliche und gerichtliche Rechtsbehelfe eingeräumt werden.

- 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 Drittlandes zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Europäischen Datenschutzausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.
- 81b) Die Kommission sollte die Wirksamkeit von Feststellungen betreffend das Schutzniveau in einem Drittland oder einem Gebiet oder einem bestimmten Sektor in einem Drittland 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. Die Kommission sollte innerhalb einer angemessenen Frist die Wirksamkeit der letztgenannten Feststellungen bewerten und dem durch diese Verordnung eingesetzten Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 über alle relevanten Erkenntnisse Bericht erstatten.
- 82) Die Kommission kann (...) feststellen, dass ein Drittland oder ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation (...) keinen angemessenen Datenschutz 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 festgelegte Standarddatenschutzklauseln, von einer Aufsichtsbehörde genehmigte Ad-hoc-Vertragsklauseln oder auf sonstige geeignete, angemessene, aufgrund der Umstände einer Datenübermittlung oder einer Kategorie von Datenübermittlungen gerechtfertigte und von einer Aufsichtsbehörde gebilligte Maßnahmen zurückgegriffen wird. Diese Schutzklauseln sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame administrative und gerichtliche Rechtsbehelfe beachtet werden. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen sowie die Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen beziehen. Datenübermittlungen dürfen auch von staatlichen Behörden oder Stellen an staatliche Behörden oder Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen, beispielsweise eine Absichtserklärung, 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 -freiheiten der betroffenen Personen beschneiden.
- 85) Jede Unternehmensgruppe oder jede Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sollte für ihre grenzüberschreitenden Datenübermittlungen aus der Union an Organisationen derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen genehmigte verbindliche unternehmensinterne Datenschutzvorschriften anwenden dürfen, sofern diese Grundprinzipien und durchsetzbare 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 sporadisch (...) 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, erfolgt. 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 und wenn das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt ist, sollte die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.



87) Diese Vorschriften sollten insbesondere für Datenübermittlungen gelten, die aus gewichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den grenzüberschreitenden Datenaustausch (...) zwischen Wettbewerbsbehörden, zwischen 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, wie eine nationalen Rotkreuzgesellschaft (...) oder an das IKRK, die erfolgt, um eine der Internationalen Rotkreuz- und Rothalbmondbewegung 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 weder als umfangreich noch als häufig gelten können, könnten auch zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter sämtliche Umstände der Datenübermittlung geprüft hat. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter 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 -freiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogener Daten berücksichtigen. Bei der Verarbeitung zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Bei der Prüfung, ob eine Übermittlung umfangreich oder häufig ist, sollte berücksichtigt werden, wie viele personenbezogene Daten und wie viele Personen betroffen sind und ob die Übermittlung sporadisch oder regelmäßig erfolgt.

- 89) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Schutzes vorliegt, sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, durch die sichergestellt wird, dass die betroffenen Personen die für die Verarbeitung ihrer personenbezogenen Daten in der Union geltenden Grundrechte und Garantien auch nach Übermittlung der Daten genießen.
- 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. 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 Vorschriften dieser Verordnung, einschließlich der Vorschriften 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 Jahreshaushalt 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 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 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. (...).

- 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 öffentliche 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 aufgrund dieser Verordnung zur Zusammenarbeit untereinander und mit der Kommission verpflichtet und befugt sein, 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 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 weitestgehend Rechnung tragen sollte.
- 98) Die Vorschriften über die federführende Behörde und das Prinzip der zentralen Kontaktstelle sollten keine Anwendung finden, wenn die Verarbeitung durch öffentliche Behörden oder private Einrichtungen, die im öffentlichen Interesse handeln, erfolgt. In diesen Fällen sollte die Aufsichtsbehörde des Mitgliedstaats, in dem die öffentliche 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, die Verarbeitung, zu der die Behörde zu Rate gezogen wird, zu untersagen. 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 bevollmächtigen 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) Die Aufsichtsbehörde, bei der eine Beschwerde eingereicht wurde oder die auf andere Weise Situationen, die mögliche Verstöße gegen die Verordnung darstellen, aufgedeckt hat bzw. darüber informiert wurde, sollte versuchen, eine gütliche Einigung zu erzielen. Falls sich dies als nicht erfolgreich erweist, sollte sie die gesamte Bandbreite ihrer Befugnisse wahrnehmen, 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. 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. Erlässt eine Aufsichtsbehörde, die um Amtshilfe ersucht hat und binnen eines Monats nach Eingang des Ersuchens bei der ersuchten Aufsichtsbehörde keine Antwort von dieser erhalten hat, eine einstweilige Maßnahme, so sollte diese einstweilige Maßnahme hinreichend begründet und nur vorübergehend gültig sein.
- 104) Jede Aufsichtsbehörde sollte berechtigt sein, an gemeinsamen Maßnahmen von Aufsichtsbehörden teilzunehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer festgelegten Frist antworten müssen.
- 105) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) 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 sollten die Aufsichtsbehörden bei der Anwendung des Kohärenzverfahrens einstweilige Maßnahmen mit einer festgelegten Geltungsdauer treffen können.
- 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 oder dessen Vertreter(...) gebildet werden. Die Kommission und der Europäische Datenschutzbeauftragte sollten an seinen Beratungen ohne Stimmrecht 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, bei dem es sich um das Sekretariat des Europäischen Datenschutzbeauftragten handelt. Das Personal des Sekretariats 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. Die organisatorische Trennung des Personals sollte alle für das unabhängige Arbeiten des Europäischen Datenschutzausschusses benötigten Dienste betreffen.
- 111) Jede betroffene Person sollte das Recht haben, bei einer 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 sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Datenschutzes zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, zu beauftragen, in ihrem Namen Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen. 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 nicht gestattet werden, im Namen einer betroffenen Person Schadenersatz 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 Nichtigkeitserklärung 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 Nichtigkeitserklärung 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 in der Rechtssache "Foto-Frost"<sup>1</sup> 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) (...)

---

<sup>1</sup> Rechtssache C-314/85.

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 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 können 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. Sind im nationalen Recht eines Mitgliedstaats keine Geldbußen vorgesehen, so kann dieser Mitgliedstaat davon absehen, für Verstöße gegen diese Verordnung, die bereits in seinem nationalen Recht strafrechtlichen Sanktionen unterliegen, Geldbußen vorzusehen, wobei zu gewährleisten ist, dass diese Sanktionen wirksam, verhältnismäßig und abschreckend sind und der Höhe der in dieser Verordnung vorgesehenen Geldbußen Rechnung getragen wird.

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 Personen auferlegt, bei denen es sich nicht um Unternehmen mit Erwerbscharakter handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat 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) 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 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 Rechtsvorschriften zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und die Kohärenz 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 öffentlichen Behörde oder einer öffentlichen Einrichtung befinden, sollten von dieser Behörde oder Einrichtung 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 gegebenenfalls notwendige Abweichungen von den Bestimmungen dieser Verordnung vorsehen. Die Bezugnahme auf öffentliche Behörden und Einrichtungen 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 den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des einzelstaatlichen 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 nationalen Recht oder in Kollektivverträgen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Arbeitnehmerdaten 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 sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorgesehen werden.

125) Die Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen (...) Zwecken und zu im öffentlichen Interesse liegenden Archivzwecken sollte zusätzlich zu den allgemeinen Grundsätzen und spezifischen Vorschriften dieser Verordnung, insbesondere hinsichtlich der Voraussetzungen für die rechtmäßige Verarbeitung, auch anderen einschlägigen Rechtsvorschriften, beispielsweise für klinische Versuche, genügen. Die Weiterverarbeitung personenbezogener Daten zu historischen, statistischen und wissenschaftlichen Zwecken und zu im öffentlichen Interesse liegenden Archivzwecken (...) sollte nicht als unvereinbar mit den Zwecken gelten, zu denen die Daten ursprünglich erhoben wurden, und die Daten können zu diesen Zwecken während eines längeren Zeitraums verarbeitet werden, als für den ursprünglichen Zweck notwendig war (...). Es sollte den Mitgliedstaaten erlaubt sein, unter bestimmten Bedingungen und bei Vorhandensein geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen zu den Informationsanforderungen und dem Recht auf Auskunft, Berichtigung, Löschung, Vergessenwerden, Einschränkung der Verarbeitung und Datenübertragbarkeit sowie zu dem Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen Zwecken oder zu Archivzwecken 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.

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. Daher können personenbezogene Daten zur Erleichterung der wissenschaftlichen Forschung zu wissenschaftlichen Zwecken verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Recht der Mitgliedstaaten oder im Unionsrecht festgelegt sind. Deshalb sollte die Einwilligung der betroffenen Person nicht bei jeder Weiterverarbeitung für wissenschaftliche Zwecke erforderlich sein.

125b) In der Entschließung des Rates vom 6. Mai 2003 zum Archivwesen in den Mitgliedstaaten wurde betont, dass Archive für das Verständnis der Geschichte und der Kultur Europas sehr wichtig sind und dass gut geführte und zugängliche Archive einen Beitrag zum Funktionieren der Demokratie in unseren Gesellschaften leisten<sup>2</sup>. Diese Verordnung sollte daher auch für die Verarbeitung personenbezogener Daten zu Zwecken der Archivierung gelten, wobei darauf hinzuweisen ist, dass die Verordnung nicht für verstorbene Personen gelten sollte.

Öffentliche Behörden oder öffentliche oder private Einrichtungen, die Aufzeichnungen von öffentlichem Interesse führen, sollten Dienststellen sein, die gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten 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.

---

<sup>2</sup> ABl. C 113 vom 13.5.2003, S. 2.

Verhaltensregeln können zur ordnungsgemäßen Anwendung dieser Verordnung beitragen, unter anderem bei der Verarbeitung personenbezogener Daten zu Zwecken der Archivierung im öffentlichen Interesse, durch eine weitere Spezifizierung angemessener Garantien für die Rechte und Freiheiten der betroffenen Personen. Solche Verhaltensregeln sollten von den amtlichen Archiven der Mitgliedstaaten oder von der Europäischen Archivgruppe erarbeitet werden. Was die internationale Übermittlung von in den Archiven enthaltenen personenbezogenen Daten betrifft, so muss sie unbeschadet der geltenden europäischen und einzelstaatlichen Vorschriften für den Austausch von Kulturgütern und nationalem Kulturgut erfolgen.

126) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken gelten. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken im Sinne dieser Verordnung sollte die Verarbeitung für die Grundlagenforschung, angewandte Forschung und privat finanzierte Forschung einschließen und darüber hinaus dem in Artikel 179 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Wissenschaftliche Zwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken 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 Zwecken 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.

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 zur Wahrung des Berufsgeheimnisses, 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 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 in Bezug auf Folgendes übertragen werden: (...) 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; Standarddatenschutzklauseln; 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. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ausgeübt werden. Die Kommission sollte besondere Maßnahmen für Kleinunternehmen sowie kleine und mittlere Unternehmen erwägen.



- 131) Da es sich um Rechtsakte von allgemeiner Tragweite handelt, sollten im Wege des Prüfverfahrens Durchführungsrechtsakte in Bezug auf Folgendes erlassen werden: 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; Standarddatenschutzklauseln; 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.
- 132) Die Kommission sollte in hinreichend begründeten Fällen äußerster Dringlichkeit, die ein Drittland oder ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder eine internationale Organisation betreffen, die kein angemessenes Schutzniveau gewährleisten, (...) sofort geltende Durchführungsrechtsakte erlassen.
- 133) Da die Ziele dieser Verordnung, nämlich ein gleiches Maß an Datenschutz für den Einzelnen und freier Datenverkehr 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 des Inkrafttretens dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Finden die Verarbeitungen jedoch nach Maßgabe der Richtlinie 95/46/EG statt, so sollten die Anforderungen der vorliegenden Verordnung betreffend die Durchführung der Datenschutz-Folgenabschätzung und die vorherige Konsultation der Aufsichtsbehörde nicht für Verarbeitungsvorgänge gelten, die bereits vor dem Inkrafttreten der vorliegenden Verordnung eingeleitet wurde, da diese Anforderungen naturgemäß vor der Verarbeitung erfüllt sein müssen. Finden die Verarbeitungen nach Maßgabe der Richtlinie 95/46/EG statt, so ist es ebenfalls nicht erforderlich, dass die betroffene Person erneut ihre Zustimmung dazu erteilt, dass der für die Verarbeitung Verantwortliche die Verarbeitung nach dem Inkrafttreten 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) (...)

HABEN FOLGENDE VERORDNUNG ERLASSEN:

## KAPITEL I ALLGEMEINE BESTIMMUNGEN

### *Artikel 1*

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

1. Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
2. Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- 2a. Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die 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, oder für andere spezifische Verarbeitungssituationen gemäß 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 Verarbeitung nach Recht und Gesetz zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.
3. Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt oder verboten werden.

### *Artikel 2*

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

1. Diese Verordnung gilt 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) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union,
  - (c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union fallen,
  - (d) durch natürliche Personen zu (...) persönlichen oder familiären Zwecken (...),
  - (e) durch die zuständigen (...) Behörden zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, zur Vollstreckung strafrechtlicher Sanktionen oder zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit.
3. (...).

### *Artikel 3*

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

1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.
2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, 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 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;
- (2a) (...)
- (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;
- (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 bestimmbaren 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 einzelstaatliches oder Unionsrecht vorgegeben, so können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach einzelstaatlichem oder Unionsrecht bestimmt werden;
- (6) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- (7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere (...) Stelle – unabhängig davon, ob es sich um einen Dritten handelt oder nicht –, an die personenbezogene Daten weitergegeben werden; Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;
- (8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage 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 unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
- (10) "genetische Daten" personenbezogene Daten jedweder Art zu den (...) ererbten oder erworbenen genetischen Merkmalen eines Menschen, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden;
- (11) "biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die die eindeutige Identifizierung dieses Menschen ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

- (12) "Gesundheitsdaten" Daten, die sich auf die körperliche oder geistige Gesundheit einer Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
- (12a) "Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren und vorherzusagen;
- (12b) (...)
- (13) "Hauptniederlassung"
- 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;
  - 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 (...) schriftlich gemäß Artikel 25 bestellt wurde und den für die Verarbeitung Verantwortlichen in Bezug auf die diesem 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) "betreffene 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) die zugrunde liegende 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 -freiheiten der betroffenen  
Personen und gegebenenfalls den freien Verkehr personenbezogener Daten  
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 Informations-  
gesellschaft;
- (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;
- (b) für genau 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, statistische oder historische Zwecke gilt gemäß Artikel 83 nicht als unvereinbar mit den ursprünglichen Zwecken;
- (c) dem Verarbeitungszweck entsprechen, sachlich relevant und in Bezug auf die Zwecke, für die sie verarbeitet werden, verhältnismäßig sein (...);
- (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;
- (e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Realisierung der Zwecke, für die sie verarbeitet werden, erforderlich ist (...); personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten vorbehaltlich der Durchführung angemessener technischer und organisatorischer Maßnahmen, die von der Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche, statistische oder historische Zwecke (...) gemäß Artikel 83 verarbeitet werden (...);
- (ee) so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist;
- (f) (...)

2. Der für die Verarbeitung Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich.

*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 unmissverständliche Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben;
  - (b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, 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 nötig, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen;
  - (e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher 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. (...).
2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke oder für historische, statistische oder wissenschaftliche Zwecke unterliegt auch den Bedingungen und Garantien des Artikels 83.

3. Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e muss festgelegt werden im Einklang mit
- (a) dem Unionsrecht oder
  - (b) dem nationalen Recht des Mitgliedstaats, dem 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, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer Verarbeitung nach Recht und Gesetz, unter anderem für sonstige spezifische Verarbeitungssituationen gemäß Kapitel IX.

- 3a. Um sich in Fällen, in denen die betroffene Person keine Einwilligung erteilt hat, zu vergewissern, ob ein Zweck der Weiterverarbeitung (...) mit demjenigen vereinbar ist, zu dem die Daten ursprünglich erhoben wurden, berücksichtigt der für die Verarbeitung Verantwortliche 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 Daten erhoben wurden,
  - (c) die Art der personenbezogenen Daten, insbesondere ob besondere Datenkategorien gemäß Artikel 9 verarbeitet werden,
  - (d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
  - (e) das Vorhandensein angemessener Garantien.

4. Wenn der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten von demselben für die Verarbeitung Verantwortlichen erhoben wurden, nicht vereinbar ist, muss auf die Weiterverarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Die Weiterverarbeitung durch denselben für die Verarbeitung Verantwortlichen für nicht konforme Zwecke aufgrund der berechtigten Interessen dieses für die Verarbeitung Verantwortlichen oder eines Dritten ist rechtmäßig, wenn diese Interessen die Interessen der betroffenen Person überwiegen.
5. (...)

#### *Artikel 7*

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

1. In den Fällen, in denen Artikel 6 Absatz 1 Buchstabe a zur Anwendung kommt, muss der für die Verarbeitung Verantwortliche nachweisen können, dass die betroffene Person ihre unmissverständliche Einwilligung erteilt hat.
- 1a. In den Fällen, in denen Artikel 9 Absatz 2 Buchstabe a zur Anwendung kommt, muss der für die Verarbeitung Verantwortliche nachweisen können, dass die betroffene Person ihre ausdrückliche Einwilligung erteilt hat.
2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, 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.
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.
4. (...)

## 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, nur rechtmäßig, wenn und insoweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung oder in Fällen, in denen dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten als gültig angesehen wird, durch das Kind erteilt wird.
  - 1a. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie 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, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind, unberührt.
3. (...)
4. (...).

## Artikel 9

### **Verarbeitung besonderer Datenkategorien**

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 und Daten über Gesundheit oder Sexualleben (...) ist untersagt.
2. Absatz 1 gilt nicht in folgenden Fällen (...):
  - (a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten (...) 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 einem Kollektivvertrag nach dem Recht eines Mitgliedstaats, das angemessene Garantien vorsieht, zulässig ist, oder
- (c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich und die betroffene Person ist aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder
- (d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, 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 nur auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder
- (e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat (...), oder
- (f) die Verarbeitung ist zur 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 angemessene und besondere Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, aus (...) Gründen des öffentlichen Interesses erforderlich (...) oder
- (h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten der Gesundheits- oder Sozialfürsorge 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
- (ha) (...);

(hb) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsbedrohungen 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 angemessene und besondere Garantien zum Schutz der Rechte und Freiheiten der betroffenen Person vorsieht, erforderlich oder

(i) die Verarbeitung ist vorbehaltlich der im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Bedingungen und Garantien, einschließlich derjenigen des Artikels 83, (...) für im öffentlichen Interesse liegende Archivzwecke oder für historische, statistische oder wissenschaftliche Zwecke erforderlich,

(j) (...)

3. (...)

4. Die in Absatz 1 genannten personenbezogenen Daten können auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats 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 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 Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

4a. (...).

5. Die Mitgliedstaaten können spezifischere Bestimmungen in Bezug auf genetische Daten oder Gesundheitsdaten beibehalten oder einführen. Dies schließt die Möglichkeit ein, dass die Mitgliedstaaten (...) weitere Bedingungen für die Verarbeitung dieser Daten vorsehen.



### Artikel 9a

#### **Verarbeitung von Daten über Strafurteile und Straftaten**

Die Verarbeitung von Daten über Strafurteile 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 vollständiges Strafregister 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 oder einzuholen oder eine zusätzliche Verarbeitung vorzunehmen, um die betroffene Person zu bestimmen.
2. Kann der für die Verarbeitung Verantwortliche in derartigen Fällen die betroffene Person nicht bestimmen, so gelten die Artikel 15, 16, 17, 17a, 17b und 18 nicht, 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 19 und Artikel 32, die sich auf die Verarbeitung personenbezogener Daten beziehen, in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls in elektronischer Form. Stellt die betroffene Person den Antrag in elektronischer Form, so kann sie in der Regel auf elektronischem Weg unterrichtet werden, sofern sie nichts anderes angibt. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person nachgewiesen ist.
- 1a. Der für die Verarbeitung Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 19. In den in Artikel 10 Absatz 2 genannten Fällen kann sich der für die Verarbeitung Verantwortliche nur weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 19 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 auf Antrag gemäß den Artikeln 15 und 16 bis 19 ergriffene Maßnahmen ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Antrags zur Verfügung (...). Diese Frist kann um 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 informiert.

3. Wird der für die Verarbeitung Verantwortliche auf Antrag der betroffenen Person nicht tätig, so unterrichtet er die betroffene Person ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen (...).
4. Informationen gemäß den Artikeln 14 und 14a (...) und alle Mitteilungen gemäß den Artikeln 16 bis 19 und Artikel 32 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall ihrer Häufung – unverhältnismäßigen Anträgen einer betroffenen Person kann sich der für die Verarbeitung Verantwortliche weigern, aufgrund des Antrags tätig zu werden (...). In diesem Fall hat er 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.
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.
  
- 1a. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung der personenbezogenen Daten folgende weitere Informationen zur Verfügung, 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:
  - (a) (...);
  - (b) 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) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
  - (d) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, personenbezogene Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln;

- (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) 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 Angaben zu (...) der verwendeten Logik sowie zur Tragweite und zu den 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.
2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person folgende weitere Informationen zur Verfügung, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:
  - (a) die Kategorien personenbezogener Daten, die verarbeitet werden;
  - (b) (...)

- (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) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
  - (da) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, personenbezogene Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln;
  - (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, sofern diese nicht aus öffentlich zugänglichen Quellen stammen;
  - (h) *das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und Angaben zu der verwendeten Logik sowie zur Tragweite und zu den 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 Erhebung der Daten, längstens jedoch innerhalb eines Monats, oder,



- (b) 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 erhoben 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; in diesen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person; oder
- (c) die Erhebung 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) (...);
- (e) die Daten gemäß dem Unionsrecht oder dem einzelstaatlichen Recht (...) vertraulich behandelt werden müssen.

5. (...)

6. (...)

*Artikel 15*  
***Auskunftsrecht der betroffenen Person***

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen in angemessenen Abständen unentgeltlich (...) 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) (...)
  - (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) wenn möglich, die geplante Speicherfrist;
  - (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) im Fall von Entscheidungen, die auf einer automatisierten Verarbeitung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 beruhen, Angaben zu der verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung.
- 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. Auf Antrag stellt der für die Verarbeitung Verantwortliche der betroffenen Person, ohne eine überhöhte Gebühr zu verlangen, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.
2. (...)
- 2a. Der Anspruch auf eine Kopie gemäß Absatz 1b (...) besteht nicht, wenn eine solche nicht zur Verfügung gestellt werden kann, ohne personenbezogene Daten anderer betroffener Personen oder vertrauliche Daten des für die Verarbeitung Verantwortlichen offenzulegen. Ferner besteht dieser Anspruch nicht, wenn die Offenlegung personenbezogener Daten Rechte an geistigem Eigentum in Bezug auf die Verarbeitung dieser personenbezogenen Daten verletzen würde.
3. (...)
4. (...)

## ABSCHNITT 3

### BERICHTIGUNG UND LÖSCHUNG

#### *Artikel 16*

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

1. (...) Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung sie betreffender unzutreffender personenbezogener Daten ohne ungebührliche 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.
2. (...)

#### *Artikel 17*

#### ***Recht auf Löschung und auf "Vergessenwerden"***

1. (...) Der für die Verarbeitung Verantwortliche ist verpflichtet, personenbezogene Daten ohne ungebührliche Verzögerung zu löschen, insbesondere personenbezogene Daten, die erhoben wurden, als die betroffene Person ein Kind war, und die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten ohne ungebührliche Verzögerung gelöscht werden, 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 ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.
- 1a. Die betroffene Person hat ferner das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung sie betreffender personenbezogener Daten ohne ungebührliche Verzögerung zu verlangen, wenn die Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben wurden.
- (...).
2. (...).
- 2a. *Hat der (...) für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so unternimmt er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten (...) vertretbare Schritte, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.*
3. Die Absätze 1, 1a und 2a 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 Unionsrecht oder dem einzelstaatlichen Recht, 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 für wissenschaftliche, statistische und historische Zwecke gemäß Artikel 83;

- e. (...)
  - f. (...)
  - g. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
4. (...)
5. (...)

#### Artikel 17a

#### **Recht auf Einschränkung der Verarbeitung**

1. Die betroffene Person hat das Recht, den für die Verarbeitung Verantwortlichen zur Einschränkung der Verarbeitung personenbezogener Daten zu veranlassen, 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,
  - (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. (...)
3. 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 verarbeitet werden.

4. Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 veranlasst hat, wird von dem für die Verarbeitung Verantwortlichen informiert, bevor die Einschränkung aufgehoben wird.
5. (...)
- 5a. (...)

#### *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 17 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

#### *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 die Verarbeitung auf einer Zustimmung 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 die Verarbeitung mit automatischen Mitteln erfolgt.

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 gilt nicht, wenn die Offenlegung personenbezogener Daten die Rechte an geistigem Eigentum im Zusammenhang mit der Verarbeitung dieser personenbezogenen Daten verletzen würde.

3. (...)

4. (...).



## 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, von Artikel 6 Absatz 4 erster Satz in Verbindung mit Artikel 6 Absatz 1 Buchstabe e oder von Artikel 6 Absatz 4 zweiter Satz erfolgt, Widerspruch einzulegen.  
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.
- 1a. (...)
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. Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich (...) auf dieses Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.
- 2a. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.
- 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 historischen, statistischen oder wissenschaftlichen Zwecken erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.
3. (...)
4. (...)

Artikel 20

**Automatisierte Generierung von Einzelentscheidungen**

1. Die betroffene Person hat das Recht, nicht einer allein auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie 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 persönliches Eingreifen 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 Legislativmaßnahmen beschränkt werden, sofern eine solche Beschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist
  - (aa) zum Schutz der nationalen Sicherheit;
  - (ab) zur Landesverteidigung;
  - (a) zum Schutz der öffentlichen Sicherheit;
  - (b) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen oder zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit;
  - (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 und zum Schutz der Marktstabilität und Marktintegrität;
  - (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 Legislativmaßnahme im Sinne des Absatzes 1 muss gegebenenfalls spezifische Vorschriften zumindest zu den Zwecken der Verarbeitung oder den Verarbeitungskategorien, den Kategorien personenbezogener Daten, dem Umfang der vorgenommenen Beschränkungen, den Angaben zu dem für die Verarbeitung Verantwortlichen oder den Kategorien von Verantwortlichen, den jeweiligen Speicherfristen sowie den geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien und der Risiken für die Rechte und Freiheiten der betroffenen Personen enthalten.

**KAPITEL IV**

**FÜR DIE VERARBEITUNG VERANTWORTLICHER UND  
AUFTRAGSVERARBEITER**

**ABSCHNITT 1**

**ALLGEMEINE PFLICHTEN**

*Artikel 22*

*Pflichten 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 Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete Maßnahmen durch und muss den Nachweis dafür erbringen können, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden.
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 datenschutzfreundliche Voreinstellungen***

1. (...) Die für die Verarbeitung Verantwortlichen treffen unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Schwere und Eintrittswahrscheinlichkeit dieser Risiken für die Rechte und Freiheiten natürlicher Personen der Verarbeitungstätigkeit und ihren Zielen angemessene technische und organisatorische Maßnahmen – wie z.B. Datenminimierung und Pseudonymisierung –, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und dass die Rechte (...) der betroffenen Personen (...) geschützt werden.
  
2. Der für die Verarbeitung Verantwortliche trifft geeignete Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur (...) personenbezogene Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung (...) erforderlich sind; (...) dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Besteht der Zweck der Verarbeitung nicht darin, der Öffentlichkeit Informationen zur Verfügung zu stellen, müssen diese Verfahren durch Voreinstellung sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne menschliches Eingreifen 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 wird angegeben, welcher der gemeinsam für die Verarbeitung Verantwortlichen als einzige Anlaufstelle für die betroffenen Personen handeln soll, wenn es um die Ausübung ihrer Rechte geht.
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. Absatz 2 gilt nicht, wenn die betroffene Person in transparenter und eindeutiger Form darüber informiert wurde, welcher der gemeinsam für die Verarbeitung Verantwortlichen zuständig ist, es sei denn, eine solche Vereinbarung – soweit es sich nicht um eine durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegte Vereinbarung handelt – ist im Hinblick auf die Rechte der betroffenen Person unbillig (...).

## 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 schriftlich einen Vertreter in der Union.

2. Diese Pflicht gilt nicht für
  - (a) (...), oder
  - (b) eine Verarbeitung, die gelegentlich erfolgt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung (...) voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder
  - (c) Behörden oder öffentliche Einrichtungen;
  - (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, ansässig sind.
  - 3a. Der Vertreter wird durch den für die Verarbeitung Verantwortlichen 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 erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen.

#### *Artikel 26*

#### ***Auftragsverarbeiter***

1. (...). Der für die Verarbeitung Verantwortliche arbeitet 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 (...).
  - 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.



- 1b. (...).
2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats, der 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 Rechte des Auftragsverarbeiters festgelegt sind und insbesondere vorgesehen ist, dass der Auftragsverarbeiter
- (a) die personenbezogenen Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeitet, sofern er nicht durch das Unionsrecht oder das Recht des Mitgliedstaats, 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) (...)
  - (c) alle gemäß Artikel 30 erforderlichen Maßnahmen ergreift;
  - (d) die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters (...) einhält, wie etwa die Anforderung, dass der für die Verarbeitung Verantwortliche diese zuvor ausdrücklich genehmigt haben muss;
  - (e) angesichts der Art der Verarbeitung (...) den für die Verarbeitung Verantwortlichen dabei unterstützt, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
  - (f) (...) den für die Verarbeitung Verantwortlichen bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;
  - (g) die personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen, die in dem Vertrag oder dem sonstigen Rechtsinstrument angegeben sind, zurückgibt bzw. löscht – nach Wahl des für die Verarbeitung Verantwortlichen –, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, 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, die vom für die Verarbeitung Verantwortlichen 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 oder aber auf Standardvertragsklauseln beruhen, die 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. (...)
5. (...)

*Artikel 27*

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

(...)

*Artikel 28*

***Aufzeichnungen zu den Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten***

1. Alle für die Verarbeitung Verantwortlichen (...) und gegebenenfalls ihre Vertreter führen eine Aufzeichnung zu allen Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten, die ihrer Zuständigkeit unterliegen. Diese Aufzeichnung enthält folgende Angaben:
  - (a) Name und 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) Angaben über die Zwecke der Verarbeitung einschließlich des berechtigten Interesses, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet;
  - (d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;
  - (e) die (...) Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern;

- (f) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation (...);
  - (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 führt eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten, die Folgendes enthält:
- (a) Name und 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;
  - (b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;
  - (c) die Kategorien der Verarbeitungen, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden;
  - (d) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation.
  - (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; dies schließt elektronische oder andere ohne technische Vermittlung nicht lesbare Formate, die in ein lesbares Format umgewandelt werden können, ein.
3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen der Aufsichtsbehörde die Aufzeichnung (...) auf Anforderung zur Verfügung.
4. Die in den Absätzen 1 und 2a genannten Pflichten gelten nicht für:
- (a) (...);

- (b) Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht aufgrund ihrer Art, ihres Umfangs, ihrer Umstände oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, unbefugte Umkehr der Pseudonymisierung, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile für die betroffenen Personen.
5. (...)
6. (...)

*Artikel 29*

***Zusammenarbeit mit der Aufsichtsbehörde***

(...)

## ABSCHNITT 2 DATENSICHERHEIT

### *Artikel 30*

#### *Sicherheit der Verarbeitung*

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung der verfügbaren Technologie, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Wahrscheinlichkeit und der Höhe des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen, wie z.B. (...) der Pseudonymisierung personenbezogener Daten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
  - 1a. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, (...) die mit der Datenverarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt 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 Unionsrecht oder mitgliedstaatlichem Recht zur Verarbeitung verpflichtet.
3. (...)
4. (...)

## Artikel 31

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

1. Bei einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, wie etwa Diskriminierung, Identitätsdiebstahl oder betrug, finanzielle Verluste, unbefugte Umkehr der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, meldet der für die Verarbeitung Verantwortliche der gemäß Artikel 51 zuständigen Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung und nach Möglichkeit binnen 72 Stunden nach Feststellung der Verletzung. Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen.
  - 1a. Eine Meldung gemäß Absatz 1 muss nicht erfolgen, wenn eine Benachrichtigung der betroffenen Person gemäß Artikel 32 Absatz 3 Buchstaben a und b nicht erforderlich ist.
2. (...) Nach Feststellung einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter diese dem für die Verarbeitung Verantwortlichen ohne ungebührliche 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 und angezeigt mit Angabe der ungefähren Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze;
  - (b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;
  - (c) (...)
  - (d) eine Beschreibung der wahrscheinlichen Folgen der von dem für die Verarbeitung Verantwortlichen festgestellten Verletzung des Schutzes personenbezogener Daten;

- (e) eine Beschreibung der von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und
  - (f) gegebenenfalls eine Angabe von Maßnahmen zur Eindämmung etwaiger nachteiliger Auswirkungen der Verletzung des Schutzes personenbezogener Daten.
- 3a. Wenn und soweit die in Absatz 3 Buchstaben d, e und f genannten Informationen nicht zur gleichen Zeit wie die in Absatz 3 Buchstaben a und b genannten bereitgestellt werden können, stellt der für die Verarbeitung Verantwortliche diese Informationen ohne ungebührliche weitere Verzögerung zur Verfügung.
4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten, auf die in den Absätzen 1 und 2 Bezug genommen wird, 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. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, unbefugte Umkehr der Pseudonymisierung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, so benachrichtigt der für die Verarbeitung Verantwortliche (...) die betroffene Person ohne ungebührliche Verzögerung von der Verletzung.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 31 Absatz 3 Buchstaben b, e und f 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 insbesondere angesichts der Zahl der betroffenen Fälle 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, oder
  - d. sie ein wichtiges öffentliches Interesse beeinträchtigen würde.
4. (...)
5. (...)
6. (...)

# ABSCHNITT 3

## DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION

*Artikel 33*

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

1. Wenn 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 hat, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, unbefugte Umkehr der Pseudonymisierung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, so führt der für die Verarbeitung Verantwortliche (...) vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (...).
- 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 Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber betroffenen Personen entfalten oder erhebliche Auswirkungen für diese mit sich bringen;
  - (b) Verarbeitung spezieller Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 (...), biometrischen Daten oder Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen, wenn die Daten in großem Umfang im Hinblick auf Entscheidungen verarbeitet werden, die sich auf spezifische Einzelpersonen beziehen sollen;

- (c) *weiträumige* Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen (...);
  - (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 eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung des Risikos, auf das in Absatz 1 Bezug genommen wird, sowie der 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 Rechtmäßigkeit und der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgängen, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
4. *Der für die Verarbeitung Verantwortliche holt 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, 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. (...)

#### *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 der Daten Verantwortlichen spätestens sechs 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 der Auftragsverarbeiter innerhalb eines Monats nach Eingang des Antrags über die Gründe für die Verzögerung informiert.
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 Gesetzesvorschriften oder von auf solchen Gesetzesvorschriften basierenden Regelungsvorschriften zu Rate, die die Verarbeitung personenbezogener Daten vorsehen (...).
- 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 oder der Auftragsverarbeiter kann – bzw. sofern im Unionsrecht oder im nationalen Recht vorgesehen, muss – einen Datenschutzbeauftragten benennen (...).
2. Eine Gruppe von Unternehmen darf einen gemeinsamen Datenschutzbeauftragten ernennen.
3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann für mehrere solcher Behörden oder Einrichtungen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
4. (...).
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, namentlich des Nichtvorhandenseins von Interessenkonflikten. (...).
6. (...)
7. (...). Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 37 nicht mehr erfüllt, außer es liegen schwerwiegende Gründe nach dem Recht des betreffenden Mitgliedstaats vor, die eine Entlassung eines Beschäftigten oder Bediensteten rechtfertigen.
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. 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.
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 erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben unabhängig handeln kann und 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 benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters.
4. 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 (...) 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 anderer 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) Überwachung von auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutzbeauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;
- (h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung 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 Kleinst-, Klein- 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 der Eltern oder des Vormundes 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) (...).

1ab. Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können die genehmigten Verhaltensregeln nach Absatz 2 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 Instrumente oder auf andere Weise die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.

1b. Die Verhaltensregeln sehen Verfahren vor, 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 die Einzelheiten der Verhaltensregeln.

- 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 vorgeschlagenen genehmigten Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender genehmigter Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Die genannten 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, z.B. über das Europäische Justizportal.

*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 Absatz 1b 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 des Kapitels VIII kann 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 ergreifen, 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 Einrichtungen.

## Artikel 39

### Zertifizierung

1. Die Mitgliedstaaten, 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 Kleinunternehmen 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 Instrumente oder auf andere Weise die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.
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 gegebenenfalls durch die zuständige Aufsichtsbehörde anhand der von der zuständigen Aufsichtsbehörde genehmigten Kriterien oder – gemäß Artikel 57 – durch den Europäischen Datenschutzausschuss erteilt.
3. 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 durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls 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 in ein Register auf und veröffentlicht sie in geeigneter Weise, z.B. über das Europäische Justizportal.

*Artikel 39a*

**Zertifizierungsstelle und -verfahren**

1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat teilt mit, ob diese Zertifizierungsstellen akkreditiert wurden 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 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, z.B. über das Europäische Justizportal.
- 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 Kriterien und Anforderungen festzulegen, die für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind (...).
- 7a. Der Europäische Datenschutzausschuss gibt der Kommission gegenüber eine Stellungnahme zu den Kriterien und Anforderungen, auf die in Absatz 7 Bezug genommen wird, ab.
8. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen festlegen. Die genannten 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*

(...)

### *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 einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.
2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission insbesondere
  - (a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die (...) in dem betreffenden Drittland bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, Datenschutzbestimmungen und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation sowie die Existenz wirksamer und durchsetzbarer Rechte der betroffenen Person und wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen (...), deren personenbezogene Daten übermittelt werden;

- (b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind;
- (c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere (...) Verpflichtungen, die sich aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.
- 2a. Der Europäische Datenschutzausschuss richtet eine Stellungnahme an die Kommission, in der er die Angemessenheit des gebotenen Schutzes in einem Drittland oder einer internationalen Organisation beurteilt und prüft, ob das Drittland, das Gebiet, die internationale Organisation oder der spezifische Sektor keinen angemessenen Datenschutz mehr bietet.
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 einen angemessenen Schutz im Sinne des Absatzes 2 bietet. (...). In jedem Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte(n) (unabhängige(n)) Aufsichtsbehörde(n) angegeben. Der Durchführungsrechtsakt wird gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.
- 3a. *Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Beschlüsse bleiben so lange in Kraft, bis (...) sie mit einem nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 erlassenen Beschluss der Kommission ersetzt oder aufgehoben werden.*

4. (...)
- 4a. Die Kommission überwacht die Wirksamkeit der nach Absatz 3 sowie nach Artikel 25 Absatz 6 und Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse.
5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland bzw. ein Gebiet oder ein spezifischer Sektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne des Absatzes 2 mehr bietet, und erforderlichenfalls derartige Beschlüsse ohne rückwirkende Kraft widerrufen, ändern oder aussetzen. Die Durchführungsrechtsakte werden 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* eine Liste aller Drittländer bzw. Gebiete und spezifischen Sektoren eines Drittlandes und aller internationalen Organisationen, zu denen Beschlüsse gemäß den Absätzen 3, 3a und 5 gefasst wurden.
8. (...)

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 übermitteln, sofern der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien, einschließlich für die Datenweitergabe (...), vorgesehen hat.
2. Die in Absatz 1 genannten geeigneten Garantien können (...), ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in
  - (oa) einem rechtsverbindlichen und durchsetzbaren Instrument zwischen den staatlichen Behörden oder 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 erlassen 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) (...)
  - (c) (...)
  - (d) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind (...).
3. (...)
4. (...)
5. (...)
- 5a. Die Aufsichtsbehörde wendet das Kohärenzverfahren an, wenn ein Fall gemäß Artikel 57 Absatz 2 Buchstaben ca, d, e oder f 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 in Kraft, bis sie 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 Beschlüsse bleiben so lange in Kraft, bis sie mit einem nach Absatz 2 erlassenen Beschluss der Kommission ersetzt oder aufgehoben werden.*

#### Artikel 43

#### **Verbindliche unternehmensinterne Datenschutzvorschriften**

1. Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 57 *verbindliche unternehmensinterne Datenschutzvorschriften*, sofern diese
- (a) rechtsverbindlich sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern angewendet werden;

- (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 Datenübermittlungskategorien 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, (...) die Datenqualität, die Rechtsgrundlage für die Verarbeitung, die Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die 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 allein 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 teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;
  - (g) die Art und Weise, wie die betroffenen Personen gemäß den Artikeln 14 und 14a 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. Der Europäische Datenschutzausschuss berät die 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.

3. (...)



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

#### *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 Kategorie 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 darüber unterrichtet wurde, dass derartige Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien *Risiken* für sie beinhalten kann, 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 Begründung, Geltendmachung 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 Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder

- (h) die nicht in großem Maßstab oder häufig erfolgende Übermittlung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, und falls der für die Verarbeitung Verantwortliche (...) alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und (...) auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.
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 nationalen Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein. (...)
- 5a. 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 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 (...).
- 6a. (...)
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 (...), 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.
  
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.
- 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. (...)
4. (...)
5. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit (...) den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss effektiv wahrnehmen zu können.
6. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde über eigenes Personal verfügt, das 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 tragen dafür Sorge, dass das Mitglied oder die Mitglieder jeder Aufsichtsbehörde (...) vom Parlament und/oder von der Regierung oder vom Staatsoberhaupt des betreffenden Mitgliedstaats oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens 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 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. (...)
5. (...).

#### *Artikel 49*

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

1. Jeder Mitgliedstaat regelt durch Gesetz
  - (a) die Errichtung jeder Aufsichtsbehörde (...),
  - (b) die Qualifikationen (...), die für die Wahrnehmung der Aufgaben eines Mitglieds der Aufsichtsbehörde notwendig sind,
  - (c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde (...),
  - (d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde, 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 und beruflichen Tätigkeiten 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 mitgliedstaatlichen Recht sowohl während ihrer Amtsbeziehungsweise 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.

*Artikel 50*

***Berufsgeheimnis***

(...)

**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.
2. (...)
- 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 ihrer grenzüberschreitenden Verarbeitung.
4. (...).

*Artikel 51b*

**Bestimmung der für die Hauptniederlassung zuständigen Aufsichtsbehörde**

(...)

*Artikel 51c*

**Register der zentralen Kontaktstellen**

(...)

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 einer Stelle, einer Organisation oder eines Verbandes befassen, die diese Personen gemäß Artikel 73 vertreten, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und die betroffene Person oder die Stelle, die Organisation oder den Verband 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 festlegen;
  - (fa) eine Liste der Verarbeitungsarten erstellen, 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 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 im Sinne des Artikels 42 Absatz 2a Buchstabe a genehmigen;
  - (i) verbindliche unternehmensinterne Vorschriften gemäß Artikel 43 genehmigen;
  - (j) Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses leisten;
  - (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 sich die Aufsichtsbehörde 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. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde mindestens über die folgenden Untersuchungsbefugnisse verfügt, die es ihr gestatten,
- (a) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des für die Verarbeitung Verantwortlichen 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.
- 1a. (...).
- 1b. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde über die folgenden Abhilfebefugnisse verfügt, 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,
- (c) (...);
- (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 mit dieser Verordnung in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung, Einschränkung oder Löschung von Daten gemäß den Artikeln 16, 17 und 17a und der Unterrichtung der Empfänger, an die diese Daten gemäß Artikel 17 Absatz 2a und Artikel 17b weitergegeben wurden, über solche Maßnahmen,
- (e) eine vorübergehende oder endgültige Einschränkung der Verarbeitung zu verhängen (...),
- (f) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen,
- (g) eine Geldbuße gemäß Artikel 79 oder 79a zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz erwähnten Maßnahmen, je nach den Umständen des Einzelfalles.
- 1c. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde über die folgenden Genehmigungsbefugnisse und beratenden Befugnisse verfügt, 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 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 auf andere Weise Klage einzureichen oder zu erheben, um dieser Verordnung Geltung zu verschaffen.
4. (...)
5. (...)

*Artikel 54*

***Tätigkeitsbericht***

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit. Gemäß dem nationalen Recht wird der Bericht dem nationalen Parlament, der Regierung und anderen Behörden übermittelt. Er wird der Öffentlichkeit, der Europäischen 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 54b*

***Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden in einzelnen Fällen etwaiger Nichteinhaltung der Verordnung***

(...)

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 und die Angelegenheit dem Europäischen Datenschutzausschuss (...) gemäß dem Kohärenzverfahren nach Artikel 57 vorlegen.
9. Die Aufsichtsbehörde legt die Gültigkeitsdauer dieser einstweiligen Maßnahme fest, die drei Monate nicht übersteigen darf. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss (...) gemäß dem Kohärenzverfahren nach Artikel 57 unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis.
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.

***Gemeinsame Maßnahmen der Aufsichtsbehörden***

1. Die Aufsichtsbehörden können gegebenenfalls gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen durchführen, 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 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 haftet der Mitgliedstaat der einladenden Aufsichtsbehörde nach Maßgabe des Rechts des Mitgliedstaats, in dessen Hoheitsgebiet der Einsatz erfolgt, 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 Absatz 1 ergreifen.

6. Die Aufsichtsbehörde legt die Geltungsdauer einer einstweiligen Maßnahme nach Absatz 5 fest, die drei Monate nicht überschreiten darf. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss (...) gemäß dem Kohärenzverfahren nach Artikel 57 unverzüglich von dieser Maßnahme und von ihren Gründen für deren Erlass in Kenntnis.

## ABSCHNITT 2

### KOHÄRENZ

#### *Artikel 57*

#### ***Kohärenzverfahren***

1. Zu dem in Artikel 46 Absatz 1a genannten Zweck arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens zusammen.
  
2. 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
  - (a) (...);
  
  - (b) (...);
  
  - (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,

- (d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dient oder
- (e) der Genehmigung von Vertragsklauseln gemäß Artikel 42 Absatz 2 Buchstabe d dient oder
- (f) der Annahme verbindlicher unternehmensinterner Vorschriften im Sinne von Artikel 43 dient.

3. Der Europäische Datenschutzausschuss erlässt in folgenden Fällen verbindliche Beschlüsse:

- 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;
- c) (...)
- d) wenn eine zuständige Aufsichtsbehörde in den in Absatz 2 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.

4. 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.

5. Die Aufsichtsbehörden und die Kommission übermitteln 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 ungebührliche Verzögerung auf elektronischem Wege 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.

#### *Artikel 58*

#### *Stellungnahme des Europäischen Datenschutzausschusses*

1. (...)

2. (...)

3. (...)



4. (...)

5. (...)

6. (...)

7. In den in Artikel 57 Absätze 2 und 4 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 einem Monat mit der einfachen Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit um einen weiteren Monat verlängert werden. Was den Beschlussentwurf angeht, der gemäß Artikel 57 Absatz 6 den Mitgliedern des Ausschusses übermittelt wird, so wird angenommen, dass ein Mitglied, das innerhalb einer vom Vorsitz festgelegten Frist keine Einwände erhoben hat, dem Beschlussentwurf zustimmt.

7a. Die zuständige Aufsichtsbehörde nimmt den Beschlussentwurf nach Artikel 57 Absatz 2 nicht vor Ablauf der in Absatz 7 genannten Frist an.

7b. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die in Artikel 57 Absatz 2 bzw. Absatz 4 genannte Aufsichtsbehörde und die Kommission ohne ungebührliche Verzögerung über die Stellungnahme und veröffentlicht sie.

8. Die in Artikel 57 Absatz 2 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 57 Absatz 3.

10. (...)

11. (...)

#### Artikel 58a

##### *Beschlüsse des Europäischen Datenschutzausschusses*

1. In den Fällen nach Artikel 57 Absatz 3 erlässt der Europäische Datenschutzausschuss einen Beschluss über die ihm vorgelegte Angelegenheit, um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung in Einzelfällen sicherzustellen. Dieser Beschluss wird begründet und an die federführende Aufsichtsbehörde und alle betroffenen Aufsichtsbehörden übermittelt und ist für diese verbindlich.

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.

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 ungebührliche 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 beigefügt.

*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 oder dem Verfahren nach Artikel 54a sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer treffen, die im Hoheitsgebiet ihres eigenen Mitgliedsstaats 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 7 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*  
**Durchführungsrechtsakte**

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 57 Absätze 5 und 6 sowie Artikel 58 Absatz 8.

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 oder dessen Vertreter und dem Europäischen Datenschutzbeauftragten.
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 und der Europäische Datenschutzbeauftragte oder dessen Vertreter sind 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.

*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 fördert die einheitliche Anwendung dieser Verordnung. Zu diesem Zweck geht der Europäische Datenschutzausschuss von sich aus oder auf Ersuchen der Kommission insbesondere folgenden Tätigkeiten nach:

(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;

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

(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 den Artikeln 79 und 79a;

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

(ca) Förderung der Ausarbeitung von Verhaltensregeln und der Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und -zeichen 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;

(ce) Abgabe einer Stellungnahme für die Kommission zum Schutzniveau personenbezogener Daten in Drittländern oder internationalen Organisationen, insbesondere in den in Artikel 41 genannten Fällen;

(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;
- (h) (...);
- (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.

*Artikel 67*

***Berichterstattung***

1. (...)
2. Der Europäische Datenschutzausschuss erstellt einen jährlichen Bericht 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. Der Europäische Datenschutzausschuss nimmt bindende Beschlüsse gemäß Artikel 57 Absatz 3 mit den in Artikel 58a Absätze 2 und 3 festgelegten Mehrheiten an. Beschlüsse im Hinblick auf die anderen in Artikel 66 aufgeführten Aufgaben werden mit der einfachen Mehrheit seiner Mitglieder angenommen.
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 Datenausschusses 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, bei dem es sich um das Sekretariat des Europäischen Datenschutzbeauftragten (...) handelt.

1a. Das Sekretariat führt seine Aufgaben ausschließlich auf Anweisung des Vorsitzenden des Europäischen Datenschutzausschusses aus.

1b. Das Personal des Sekretariats des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Europäischen Datenschutzausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, ist von dem Personal, das an der Wahrnehmung der dem Europäischen Datenschutzbeauftragten übertragenen Aufgaben beteiligt ist, organisatorisch getrennt und unterliegt getrennten Berichtspflichten.

1c. Erforderlichenfalls erstellt und veröffentlicht der Europäische Datenschutzausschuss in Absprache mit dem Europäischen Datenschutzbeauftragten Verhaltensregeln zur Anwendung dieses Artikels, die für das Personal des Sekretariats des Europäischen Datenschutzbeauftragten gelten, 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 vertraulich.
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.

## KAPITEL VIII

### RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

#### *Artikel 73*

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

1. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer einzigen 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 wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde***

1. Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen administrativen 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 administrativen 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 oder einer nach dem Unionsrecht oder dem Recht des Mitgliedstaats vorgesehenen kürzeren Frist 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. Eine betroffene Person hat unbeschadet eines verfügbaren administrativen 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 verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat (...). Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde, 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 Organisation oder eine Vereinigung, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist und zu deren satzungsmäßigen Zielen der Schutz der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten gehört, zu beauftragen, in ihrem Namen Beschwerde zu erheben und die in den Artikeln 73, 74 und 75 genannten Rechte wahrzunehmen (...).
  - 1a. (...)
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 73, 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. (...)

## 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.

3. (...).

#### *Artikel 77*

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

1. Jede Person, der wegen einer Verarbeitung, die nicht mit dieser Verordnung zu vereinbaren ist, 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.

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**

1. Jede Aufsichtsbehörde (...) stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß Artikel 79a 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 f 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) (...);
  - (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 Buchstaben a, d, e und f 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) (...);
  - (l) (...);
  - (m) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall.
3. (...)
- 3a. (...)

3b. Jeder Mitgliedstaat kann Vorschriften dafür festlegen, ob und in welchem Umfang gegen öffentliche Behörden und öffentliche Einrichtungen, 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. Die Mitgliedstaaten können darauf verzichten, Vorschriften für Geldbußen nach Artikel 79a Absätze 1, 2 und 3 vorzusehen, wenn in ihrem Rechtssystem keine Geldbußen vorgesehen sind und bis zum [in Artikel 91 Absatz 2 genannter Zeitpunkt] bereits nach ihrem nationalen Recht strafrechtliche Sanktionen für die darin genannten Verstöße vorgesehen sind; dabei sorgen sie dafür, dass diese strafrechtlichen Sanktionen wirksam, verhältnismäßig und abschreckend sind, und berücksichtigen die Höhe der in dieser Verordnung vorgesehenen Geldbußen.

Beschließen die Mitgliedstaaten dies, so melden sie der Kommission die entsprechenden Bestimmungen ihres Strafrechts in ihren Einzelheiten.

#### *Artikel 79a*

#### **Geldbußen**

1. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 250 000 EUR oder im Fall eines Unternehmens 0,5 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen verhängen, der vorsätzlich oder fahrlässig

(a) Anträge der betroffenen Person nicht (...) innerhalb des Zeitraums nach Artikel 12 Absatz 2 beantwortet;

(b) unter Verstoß gegen Artikel 12 Absatz 4 Satz 1 eine Gebühr (...) verlangt.

2. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 500 000 EUR oder im Fall eines Unternehmens 1 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig

- (a) der betroffenen Person die Auskünfte gemäß (...) Artikel 12 Absatz 3 sowie den Artikeln 14 und 14a nicht [rechtzeitig oder] in [hinreichend] transparenter Weise erteilt;
- (b) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt oder personenbezogene Daten nicht gemäß Artikel 16 berichtigt (...);
- (c) personenbezogene Daten unter Verstoß gegen das Recht auf Löschung und "Vergessenwerden" nach Artikel 17 Absatz 1 Buchstaben a, b d oder e nicht löscht;
- (d) (...)
- (da) personenbezogene Daten unter Verletzung des Rechts auf Einschränkung der Verarbeitung nach Artikel 17a verarbeitet oder die betroffene Person nicht vor Aufhebung der Einschränkung nach Artikel 17a Absatz 4 unterrichtet;
- (db) unter Verstoß gegen Artikel 17b nicht jeden Empfänger, an den der für die Verarbeitung Verantwortliche personenbezogene Daten weitergegeben hat, über jegliche Berichtigung, Löschung oder Einschränkung der Verarbeitung unterrichtet;
- (dc) der betroffenen Person unter Verstoß gegen Artikel 18 (...) nicht die sie betreffenden personenbezogenen Daten bereitstellt;
- (dd) personenbezogene Daten nach dem Einspruch der betroffenen Person gemäß Artikel 19 Absatz 1 verarbeitet, 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;
- (de) der betroffenen Person nicht gemäß Artikel 19 Absatz 2 Informationen über das Recht übermittelt, gegen eine Verarbeitung für Zwecke der Direktwerbung Einspruch einzulegen, oder unter Verstoß gegen Artikel 19 Absatz 2a die Verarbeitung von Daten auch nach einem Einspruch der betroffenen Person fortsetzt;
- (e) die jeweilige Verantwortung der gemeinsam für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt;

(f) die Dokumentation gemäß Artikel 28 und Artikel 31 Absatz 4 nicht oder nicht hinreichend gewährleistet.

(g) (...)

3. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 1 000 000 EUR oder im Fall eines Unternehmens 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig

(a) personenbezogene Daten ohne (...) Rechtsgrundlage verarbeitet oder die Bedingungen für die Einwilligung gemäß den Artikeln 6, 7, 8 und 9 nicht beachtet;

(b) (...);

(c) (...);

(d) die Bedingungen gemäß Artikel 20 in Bezug auf (...) eine automatisierte Entscheidungsfindung einschließlich Profiling nicht beachtet;

(da) (...) keine geeigneten Maßnahmen trifft oder nicht in der Lage ist, die Einhaltung der Anforderungen (...) nachzuweisen, wie dies in den Artikeln 22 (...) und 30 vorgesehen ist;

(db) unter Verstoß gegen Artikel 25 keinen Vertreter benennt;

(dc) unter Verstoß gegen Artikel 26 (...) personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;

(dd) die Aufsichtsbehörde bei einer Verletzung des Schutzes personenbezogener Daten nicht alarmiert oder sie oder die betroffene Person unter Verstoß gegen die Artikel 31 und 32 nicht [rechtzeitig oder nicht ]vollständig von einer solchen Verletzung benachrichtigt;

(de) unter Verstoß gegen Artikel 33 keine Datenschutz-Folgenabschätzung vornimmt oder personenbezogene Daten unter Verstoß gegen Artikel 34 ohne vorherige Zurateziehung der Aufsichtsbehörde verarbeitet;

(e) (...);

- (f) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht oder die in den Artikeln 38a und 39a festgelegten Bedingungen und Verfahren nicht einhält;
- (g) unter Verstoß gegen die Artikel 41 bis 44 eine Datenübermittlung an einen Empfänger in einem Drittland oder an eine internationale Organisation vornimmt oder anordnet;
- (h) einer Anweisung oder einer vorübergehenden oder endgültigen Einschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1b nicht Folge leistet oder unter Verstoß gegen Artikel 53 Absatz 1 keinen Zugang gewährt.
- (i) (...)
- (j) (...).
- 3a. Verstößt ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen mehrere der in den Absätzen 1, 2 oder 3 aufgeführten Bestimmungen dieser Verordnung, so darf der Gesamtbetrag der Geldbuße den Betrag für den schwerwiegendsten Verstoß nicht übersteigen.
4. (...)

#### *Artikel 79b*

#### ***Sanktionen***

1. Bei (...) Verstößen (...) gegen diese Verordnung, insbesondere bei Verstößen, die keiner Geldbuße nach Artikel 79a unterliegen, legen die Mitgliedstaaten fest, welche Sanktionen bei diesen Verstößen gegen diese Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen (...). 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 mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.*

# KAPITEL IX

## VORSCHRIFTEN FÜR BESONDERE DATENVERARBEITUNGSSITUATIONEN

### *Artikel 80*

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

1. Im nationalen Recht der Mitgliedstaaten (...) wird das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung personenbezogener Daten zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang gebracht.
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) und des Kapitels VII (Zusammenarbeit und Kohärenz) 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.

### *Artikel 80a*

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

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



Artikel 80aa

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

Personenbezogene Daten in Informationen des öffentlichen Sektors, die sich im Besitz einer öffentlichen 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 öffentliche Behörde oder Einrichtung unterliegt, freigegeben werden, um die Weiterverwendung dieser amtlichen Dokumente und Informationen des öffentlichen Sektors mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung in Einklang zu bringen.

Artikel 80b

**Verarbeitung einer nationalen Kennziffer**

Die Mitgliedstaaten können 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 Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Arbeitnehmerdaten 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. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.
3. Die Mitgliedstaaten können durch Rechtsvorschriften die Bedingungen festlegen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Arbeitnehmers verarbeitet werden dürfen.

*Artikel 82a*

**Verarbeitung zu Zwecken der sozialen Sicherheit**

(...)

Artikel 83

**Ausnahmen in Bezug auf die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke und zu wissenschaftlichen, statistischen und historischen Zwecken**

1. Werden personenbezogene Daten zu wissenschaftlichen, statistischen oder historischen Zwecken verarbeitet, so können im Unionsrecht oder im Recht der Mitgliedstaaten vorbehaltlich angemessener Garantien für die Rechte und Freiheiten der betroffenen Person Ausnahmen von Artikel 14a Absätze 1 und 2 und den Artikeln 15, 16, 17, 17a, 17b, 18 und 19 vorgesehen werden, insofern eine solche Ausnahme für die Erfüllung der spezifischen Zwecke erforderlich ist.
- 1a. Werden personenbezogene Daten zu im öffentlichen Interesse liegenden Archivzwecken verarbeitet, so können im Unionsrecht oder im Recht der Mitgliedstaaten vorbehaltlich angemessener Garantien für die Rechte und Freiheiten der betroffenen Person Ausnahmen von Artikel 14a Absätze 1 und 2, den Artikeln 15, 16, 17, 17a, 17b, 18, 19, 23, 32 und 33 sowie von Artikel 53 Absatz 1b Buchstaben d und e vorgesehen werden, insofern eine solche Ausnahme für die Erfüllung dieser Zwecke erforderlich ist.
- 1b. Falls eine der in den Absätzen 1 und 1a genannten Verarbeitungsarten gleichzeitig einem anderen Zweck dient, dürfen die zulässigen Ausnahmen nur für die Verarbeitung zu den in jenen Absätzen genannten Zwecken gelten.
2. Die in den Absätzen 1 und 1a genannten angemessenen Garantien müssen im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden und so gestaltet sein, dass sie gewährleisten, dass die technischen und/oder organisatorischen Schutzmaßnahmen gemäß dieser Verordnung auf die personenbezogenen Daten (...) zur Minimierung der Verarbeitung personenbezogener Daten im Hinblick auf die Grundsätze der Verhältnismäßigkeit und der Notwendigkeit angewandt werden, wie z.B. *Pseudonymisierung der Daten*, es sei denn diese Maßnahmen verhindern die Erfüllung des Zwecks der Verarbeitung und dieser Zweck kann nicht mit vertretbaren Mitteln auf andere Weise erfüllt werden.
3. (...).

## 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 einzelstaatlichen Stellen erlassenen Regelungen dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht oder berufsständischen Regeln, die von Berufsverbänden überwacht und durchgesetzt werden, 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

(1) 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 39a Absatz 7 (...) wird der Kommission auf unbestimmte Zeit ab dem Zeitpunkt des Inkrafttretens dieser Verordnung übertragen.
3. Die Befugnisübertragung gemäß 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 (...) 39a Absatz 7 (...) erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um zwei 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 aufgehoben.
2. Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

### *Artikel 89*

#### ***Verhältnis zur Richtlinie 2002/58/EG und Änderung dieser Richtlinie***

1. Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.
2. (...)

*Artikel 89a*

***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 der Richtlinie 95/46/EG 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 zur Bewertung und Überprüfung dieser Verordnung vor.
2. Im Rahmen dieser Bewertungen prüft die Kommission insbesondere die Anwendung und die Wirkungsweise der Bestimmungen des Kapitels VII über Zusammenarbeit und Kohärenz.
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 und zur Anpassung anderer Rechtsinstrumente vor, wobei sie insbesondere der Entwicklung der Informationstechnologie und den Fortschritten in der Informationsgesellschaft Rechnung trägt.



*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*].

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*