



**RAT DER  
EUROPÄISCHEN UNION**

**Brüssel, den 21. Juni 2013 (16.09)  
(OR. en)**

**11013/13**

---

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

---

**LIMITE**

**DATAPROTECT 78  
JAI 496  
MI 546  
DRS 119  
DAPIX 88  
FREMP 85  
COMIX 380  
CODEC 1475**

**VERMERK**

---

des	Vorsitzes
für die	Gruppe "Informationsaustausch und Datenschutz"
Nr. Vordok.:	9398/1/13 REV 1 DATAPROTECT 61 JAI 355 MI 383 DRS 96 DAPIX 80 FREMP 53 COMIX 276 CODEC 1033 + REV 1 ADD DATAPROTECT 67 9967/13 JAI 418 MI 436 DRS 103 DAPIX 85 FREMP 69 COMIX 330 CODEC 1175
Nr. Komm.dok.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
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)

---

Die Delegationen erhalten anbei eine überarbeitete Fassung des Entwurfs der Datenschutz-Grundverordnung. Die Ergebnisse der Beratungen über den Verordnungsentwurf, die in der Gruppe "Informationsaustausch und Datenschutz" stattgefunden haben, sind darin so weit wie möglich berücksichtigt. In den Artikeln 41 bis 43 des Kapitels V sind aufgrund der Beratungsergebnisse vom 14. Juni 2013 geringfügige Änderungen vorgenommen worden. Mit Ausnahme der Artikel 80 und 80a ist die Fassung des Kapitels IX vom 4. Dezember 2012 nicht angetastet worden.

Alle Änderungen gegenüber dem ursprünglichen Kommissionsvorschlag sind unterstrichen. Streichungen sind durch (...) gekennzeichnet. Textteile, die gestrichen und an anderer Stelle wieder eingefügt wurden, sind kursiv gedruckt.

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 <sup>1</sup>,

nach Anhörung des Europäischen Datenschutzbeauftragten <sup>2</sup>,

gemäß dem ordentlichen Gesetzgebungsverfahren,

---

<sup>1</sup> ABl. C , S. . .

<sup>2</sup> ABl. C , S. .

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 gewöhnlichen 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<sup>3</sup> 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.

---

<sup>3</sup> ABl. L 281 vom 23.11.1995, S. 31.

- 4) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarktes hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs geführt. Der unionsweite Datenaustausch zwischen (...) staatlichen Stellen und Privatpersonen und öffentlichen und privaten 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 ins weltweite Netz gestellt und damit öffentlich 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.

- 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 freien Verkehr solcher Daten in der gesamten Union behindern. Diese Unterschiede im Schutzniveau können ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.
- 8) Um ein 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.
- 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 Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtsicherheit und Transparenz schafft, den Einzelnen mit denselben durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter vorsieht und eine einheitliche Kontrolle der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten sowie gleiche Sanktionen und eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Damit der Binnenmarkt reibungslos funktioniert, darf der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten werden. Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine Reihe von Ausnahmen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs "Kleinstunternehmen sowie 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 Wohnorts. 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. Dies sollte auch dann gelten, wenn der Name der juristischen Person die Namen einer oder mehrerer natürlichen Personen enthält.

- 13) Der Schutz natürlicher Personen sollte technologieneutral sein und nicht von den verwendeten Verfahren abhängen, da andernfalls das Risiko einer Umgehung der Vorschriften groß wäre. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, die in einem Ablagesystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten vom Anwendungsbereich der Verordnung ausgenommen werden.
- 14) Die Verordnung behandelt weder Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Datenverkehrs im Zusammenhang mit Tätigkeiten, die nach Maßgabe der Artikel 3 bis 6 des Vertrags über die Arbeitsweise der Europäischen Union 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<sup>4</sup> (...) gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstigen Rechtsinstrumente der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst werden (...).
- 15) Die 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.

---

<sup>4</sup> ABl. L 8 vom 12.1.2001, S. 1.

- 16) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und zu diesen Zwecken der Aufrechterhaltung der öffentlichen Ordnung oder der Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden dient, 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.
- Soweit die Verordnung für die Verarbeitung personenbezogener Daten durch (...) private Einrichtungen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter gewissen 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 der kriminaltechnischen 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 in den Grenzen dieser Verordnung festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung von personenbezogenen Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben unangetastet bleibt, sollten die Aufsichtsbehörden nicht für personenbezogene Daten zuständig sein, die von Gerichten in ihrer gerichtlichen Eigenschaft verarbeitet werden.



- 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) 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 öffentlichen Einrichtung befinden, können von dieser Behörde oder Einrichtung freigegeben werden, sofern dies in den Rechtsvorschriften der Union oder des Mitgliedstaats, denen sie unterliegt, vorgesehen ist. Diese Rechtsvorschriften sollten das Interesse am Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten in Einklang bringen.
- 19) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

- 20) Um sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach dieser Verordnung ein Anrecht haben, sollte die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten oder das Verhalten dieser Personen in der Union zu beobachten. 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 oder das Verhalten dieser betroffenen Personen zu beobachten.
- 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 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 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, sollte die Verordnung auch auf einen nicht in der EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.
- 23) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Um festzustellen, ob eine Person bestimmbar ist, 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 Daten gelten, d.h. für Daten, 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. Die Grundsätze des Datenschutzes sollten nicht für Verstorbene gelten.

- 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 betroffenen Personen zu erstellen und sie zu identifizieren. Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente als solche sollten nicht (...) als personenbezogene Daten betrachtet werden, wenn mit ihnen keine Person bestimmt oder bestimmbar gemacht wird.<sup>5</sup>

---

<sup>5</sup> DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. UK suggests deleting the words 'provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers' and 'received by the servers'. It also suggests deleting 'need not necessarily be considered as personal data in all circumstances' and replacing it by 'can constitute personal data, but this will depend on the context'. COM referred to the ECJ case law (Scarlett C-70/10) according to which IP addresses should be considered as personal data if they actually could lead to the identification of data subjects. DE queried who would in practice be responsible for such metadata.

- 25) Die Einwilligung sollte eindeutig mittels einer geeigneten Methode erfolgen, die eine ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene Willensbekundung der betroffenen Person in Form einer schriftlich, mündlich oder auf andere Weise abgegebenen Erklärung oder einer 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 klar und deutlich ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Eine stillschweigende Einwilligung ohne Zutun der betroffenen Person stellt daher keine Einwilligung dar. Soweit technisch machbar und wirksam, kann die Einwilligung der betroffenen Person durch die Benutzung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung erfolgen. 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, 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.

- 26) Zu den personenbezogenen Gesundheitsdaten sollten (...) Daten gezählt werden, die sich auf den Gesundheitszustand einer betroffenen Person beziehen, außerdem 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, darunter genetische Daten und biologische 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) 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 begründet an sich noch keine Hauptniederlassung und ist daher kein ausschlaggebender Faktor für das Bestehen einer solchen Niederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, oder – wenn er keine Hauptverwaltung in der Union hat – der Ort, an dem die wesentlichen Verarbeitungstätigkeiten stattfinden.

Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, 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.
- 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. (...).<sup>6</sup>
- 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.

---

<sup>6</sup> COM reservation on deletion of the reference to the UN Convention on the Rights of the Child.

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 vor allem, dass nicht unverhältnismäßig viele Daten erfasst werden und die Speicherfrist auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. (...).

Es sollten alle vertretbaren Schritte unternommen werden, damit unzutreffende oder unvollständige personenbezogene Daten gelöscht oder berichtigt werden. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. 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 einer gesetzlichen 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) 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. Vor allem bei Abgabe einer schriftlichen Erklärung in anderem Zusammenhang sollten Vorkehrungen getroffen werden, die sicherstellen, dass die betroffene Person weiß, dass und wozu sie ihre Einwilligung erteilt.



- 33) 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.
- 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. (...)
- 35) Die Verarbeitung von Daten sollte rechtmäßig sein, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.
- 36) Erfolgt die Verarbeitung durch den für die Verarbeitung Verantwortlichen aufgrund einer ihm obliegenden gesetzlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt erforderlich, muss hierfür eine (...) Grundlage im Unionsrecht oder im nationalen Recht bestehen. (...). Desgleichen sollte im Unionsrecht oder im nationalen Recht geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnte in dieser Rechtsgrundlage – in den Grenzen dieser Verordnung – genauer 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.

- 37) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen Person zu schützen.
- 38) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines für die Verarbeitung Verantwortlichen, auch eines für die Verarbeitung Verantwortlichen, an den die Daten weitergegeben werden dürfen, begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Diese Interessen sind besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Datenerhebung und angesichts der Umstände, unter denen sie erfolgt, voraussehen kann, dass eine Verarbeitung für diesen Zweck erfolgen kann. 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. Da die (...) Grundlage für die Verarbeitung von Daten durch Behörden im Unionsrecht oder im nationalen Recht (...) geschaffen werden muss, sollte diese nicht für die von Behörden in Erfüllung ihrer öffentlichen Aufgaben vorgenommene Verarbeitung gelten.
- 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 und Überwachung von Betrug unbedingt erforderlichen Umfang ist ebenfalls ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen. Ein berechtigtes Interesse eines für die Verarbeitung Verantwortlichen könnte auch darin bestehen, dass personenbezogene Daten zum Zwecke der Anonymisierung oder Pseudoanonymisierung personenbezogener Daten verarbeitet werden. Die Verarbeitung personenbezogener Daten um Zwecke der Direktwerbung kann als einem rechtmäßigen Interesse dienende Verarbeitung betrachtet werden.

- 40) Die Verarbeitung personenbezogener Daten für andere Zwecke sollte nur zulässig sein, wenn diese mit den Zwecken, für die sie ursprünglich erhoben wurden, vereinbar sind, beispielsweise dann, wenn die Verarbeitung für historische, statistische (...) oder wissenschaftliche Zwecke (...) erforderlich ist. 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 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 geeignete Garantien bestehen. Ist der beabsichtigte andere Zweck nicht mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar, 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 die betroffene Person über diese anderen Zwecke unterrichtet wird. Die Weiterverarbeitung personenbezogener Daten sollte unzulässig sein, wenn die Verarbeitung nicht mit einer rechtlichen, geschäftlichen oder auf sonstige Weise verbindlichen Pflicht zur Geheimhaltung vereinbar ist.

- 41) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und -freiheiten (...) besonders sensibel sind, bedürfen eines besonderen Schutzes. Dies sollte auch für personenbezogene Daten gelten, 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 dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot sollten im Bedarfsfall jedoch ausdrücklich vorgesehen werden, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.
- 42) Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien sollten auch dann erlaubt sein, wenn es dafür eine gesetzliche Grundlage gibt, und – vorbehaltlich bestimmter Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte – wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, speziell wenn es um gesundheitliche Belange geht, wie die Gewährleistung der öffentlichen Gesundheit oder der sozialen Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, vor allem wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sichergestellt werden soll, oder wenn die Verarbeitung historischen, 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.
- 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, weil er beispielsweise pseudoanonymisierte Daten verarbeitet, 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, Informationen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen, entgegenzunehmen.
- 46) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information leicht zugänglich sowie in einfacher und verständlicher Sprache abgefasst ist. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt ganz besonders für bestimmte Situationen wie etwa Werbung im Internet, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck seine Daten erfasst werden. Wenn sich die Verarbeitung (...) 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 diese Verordnung zustehenden Rechte wahrzunehmen, etwa dass sie ein (...) Auskunftsrecht oder ein Recht auf Berichtigung oder Löschung von Daten besitzt oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der für die Verarbeitung Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, vor allem wenn die personenbezogenen Daten elektronisch verarbeitet werden. Der für die Verarbeitung Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person innerhalb einer bestimmten Frist zu beantworten und gegebenenfalls zu begründen, warum er ihn ablehnt.
- 48) Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person (...) über die Existenz des Verarbeitungsvorgangs und seine Zwecke (...) 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, 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. Konnte der betroffenen Person nicht mitgeteilt werden, woher die Daten stammen, weil verschiedene Quellen benutzt wurden, 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 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 Daten, die bei ihr erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich von der Rechtmäßigkeit der Verarbeitung überzeugen zu können. 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 Daten verarbeitet werden und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling basiert. 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 diese 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 Falle von Online-Kennungen. Ein für die Verarbeitung Verantwortlicher sollte personenbezogene Daten nicht allein speichern, um 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 unter Verstoß gegen die Verordnung erfolgt ist. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht weiter verarbeitet werden, wenn sich die Zwecke, für die die Daten erhoben wurden, erübrigt haben, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen unter Verstoß gegen die Verordnung erfolgt ist. 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 Daten – besonders die im Internet gespeicherten – später löschen möchte. Die weitere Speicherung der Daten sollte jedoch zulässig sein, wenn dies für historische, statistische oder wissenschaftliche Zwecke (...), aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zur Ausübung des Rechts auf freie Meinungsäußerung erforderlich ist, wenn es hierfür eine gesetzliche Grundlage gibt oder wenn eine beschränkte Verarbeitung der Daten anstatt ihrer Löschung gerechtfertigt ist.
- 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 eine betroffene Person die Löschung von Links zu diesen Daten oder von Kopien oder Reproduktionen dieser Daten verlangt. 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 diese 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) Damit die betroffenen Personen eine bessere Kontrolle über ihre eigenen Daten haben und ihr Auskunftsrecht besser ausüben können, sollten sie im Falle einer elektronischen Verarbeitung ihrer personenbezogenen Daten in einem strukturierten gängigen Format ebenfalls Anspruch auf Erhalt einer Kopie der sie betreffenden Daten in einem gängigen elektronischen Format haben. Die betroffene Person sollte auch befugt sein, die von ihr zur Verfügung gestellten Daten von einer automatisierten Anwendung (...) auf eine andere Anwendung zu übertragen. Dies sollte dann möglich sein, wenn die betroffene Person die Daten dem automatisierten Verarbeitungssystem mit ihrer ausdrücklichen Einwilligung oder im Zuge der Erfüllung eines Vertrags zur Verfügung gestellt hat. Das Recht, die Daten auf ein anderes automatisiertes Verarbeitungssystem zu übertragen, sollte nicht bedeuten, dass personenbezogene Daten, die von der betroffenen Person zur Erfüllung eines Vertrags übermittelt worden sind, gelöscht werden, sofern und solange diese Daten für die Erfüllung des Vertrags notwendig sind. Dieses Recht kann naturgemäß nicht gegen für die Verarbeitung Verantwortliche, die Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten, ausgeübt werden.
- 56) In Fällen, in denen die personenbezogenen Daten (...) aufgrund der berechtigten Interessen des für die Verarbeitung Verantwortlichen rechtmäßig verarbeitet werden dürfen, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sie betreffenden Daten einzulegen. (...) Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.

- 57) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, sollte die betroffene Person unentgeltlich, einfach und effektiv Widerspruch gegen eine solche Verarbeitung einlegen können.
- 58) Jeder betroffene Person sollte das Recht haben, keiner Entscheidung unterworfen zu werden, die auf Profiling (...) basiert. Eine solches Profiling sollte allerdings erlaubt sein, wenn es nach dem Unionsrecht und dem Recht der Mitgliedstaaten ausdrücklich erlaubt ist, auch um Betrug zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem für die Verarbeitung Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn es bei Abschluss oder in Erfüllung eines Vertrags zwischen der betroffenen Person und einem für die Verarbeitung Verantwortlichen durchgeführt wird oder wenn die betroffene Person ihre Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden werden wie der Unterrichtung der betroffenen Person oder dem Anspruch auf direkten persönlichen Kontakt (...). Profiling zum Zwecke der Direktwerbung oder unter Zugrundelegung besonderer Kategorien von personenbezogenen Daten sollte nur unter bestimmten Bedingungen erlaubt sein.
- 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 sowie die Verhütung, Aufdeckung und Verfolgung von Straftaten und von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen 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 zu schützen. Diese Beschränkungen müssen mit der Charta der Grundrechte der Europäischen Union und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

- 60) Die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte (...) geregelt werden. Insbesondere sollte der für die Verarbeitung Verantwortliche geeignete Maßnahmen ergreifen und nachweisen müssen, dass (...) die Verarbeitungsvorgänge im Einklang mit dieser Verordnung stehen, beispielsweise durch Aufzeichnung der Vorgänge, durch technische und organisatorische Maßnahmen, die ein hinreichendes Sicherheitsniveau gewährleisten oder im Wege einer Datenschutz-Folgenabschätzung. Dabei sollte er die Art, den Umfang, die Umstände und den Zweck der Verarbeitung und die Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigen. Diese Risiken mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere bestehen in einer Datenverarbeitung, die zu einer physischen, materiellen oder moralischen Schädigung führen könnte, insbesondere in folgenden Fällen:
- Wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führt oder
  - 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 Rasse oder ethnische Herkunft, politische Überzeugungen, die Religions- oder Glaubenszugehörigkeit oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten oder Daten über die Gesundheit oder das Sexualleben oder über Strafurteile 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;
  - wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft.
- 60a. Ist die Verarbeitung aller Wahrscheinlichkeit nach mit konkreten Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden, sollte der für die Verarbeitung Verantwortliche [oder Auftragsverarbeiter] vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchführen.
- 60b. Werden die personenbezogenen Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, so sollte es zu den genannten Maßnahmen zählen, dass ausschließlich Auftragsverarbeiter gewählt werden, die hinreichende Garantien für ausreichende technische und organisatorische Vorkehrungen bieten.
- 60c. Anleitungen, wie der für die Verarbeitung Verantwortliche [oder Auftragsverarbeiter] diese Maßnahmen durchzuführen hat, insbesondere was die Ermittlung der Risiken, ihre Abschätzung in Bezug auf ihre Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für ihre Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsmechanismen, Leitlinien des Europäischen Datenschutzausschusses oder von einem eigens benannten Datenschutzbeauftragten gegeben werden, oder, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitungsvorgänge mit hohen konkreten Risiken verbunden sind, könnte vorab die Aufsichtsbehörde zu Rate gezogen werden.
- 61) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten der betroffenen Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachzuweisen zu können, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und geeignete Maßnahmen ergreifen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

- 62) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie zur Klärung der Verantwortung und der Haftung der für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, insbesondere für Fälle, in denen ein für die Verarbeitung Verantwortlicher die Verarbeitungszwecke (...) 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, dieser für die Verarbeitung Verantwortliche ist in einem Drittland niedergelassen, das einen angemessenen Schutz bietet, oder es handelt sich um ein kleines oder mittleres Unternehmen – sofern die von diesem Unternehmen ausgeführten Verarbeitungsvorgänge aufgrund ihrer Art, ihres Umfangs und ihrer Zwecke keine konkreten Risiken für die Rechte und Freiheiten betroffener Personen bergen – oder es handelt sich um eine Behörde oder um eine 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 ihn 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.

- 64) (...).
- (64a) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, besser eingehalten wird, sollte der für die Verarbeitung Verantwortliche [oder Auftragsverarbeiter] für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Eintrittswahrscheinlichkeit und Schwere dieser Risiken evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche (...) Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht.
- 65) Zum Nachweis der Einhaltung dieser Verordnung sollte der für die Verarbeitung Verantwortliche Aufzeichnungen über alle Kategorien von Verarbeitungsvorgängen, 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 konkreten Risiken ermitteln und Maßnahmen zu ihrer Eindämmung ergreifen. Diese Maßnahmen müssen unter Berücksichtigung der verfügbaren Technik und der dabei anfallenden Kosten ein Schutzniveau, das sich auch auf die Vertraulichkeit erstreckt, gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. (...).

67) Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen schweren materiellen oder moralischen Schaden für die betroffenen Personen nach sich ziehen, etwa den Verlust der Kontrolle über ihre persönlichen Daten oder eine Einschränkung ihrer Rechte, eine Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Deshalb sollte der für die Verarbeitung Verantwortliche nach Bekanntwerden einer (...) Verletzung, die einen schweren materiellen oder moralischen Schaden nach sich ziehen kann, die Aufsichtsbehörde ohne unangemessene 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 personenbezogene Daten durch die Datenschutzverletzung erheblich beeinträchtigt werden könnten, sollten ohne unangemessene Verzögerung benachrichtigt werden, damit sie die erforderlichen Vorkehrungen treffen können. Die Auswirkungen einer solchen Verletzung sollten als erhebliche Beeinträchtigung des Schutzes der personenbezogenen Daten oder der Privatsphäre einer natürlichen Person angesehen werden, wenn sie zum Beispiel einen Identitätsdiebstahl oder -betrug, eine physische Schädigung, eine erhebliche Demütigung oder Rufschädigung zur Folge haben. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung 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 beispielweise das Risiko eines unmittelbaren Schadens klein halten 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 ergreifen.

- 68) Um bestimmen zu können, ob eine Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde und der betroffenen Person ohne unangemessene Verzögerung gemeldet wurde, muss der für die Verarbeitung Verantwortliche 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, bevor persönliche oder wirtschaftliche Interessen Schaden genommen haben, wobei die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren negative Folgen für die betroffene Person zu berücksichtigen sind.
- (68a) Die Benachrichtigung der betroffenen Person über die 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 und durch Verwendung pseudoanonymer 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 jenen Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können. In derartigen Fällen sollte der für die Verarbeitung Verantwortliche (...) vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die Schwere und Eintrittswahrscheinlichkeit dieser konkreten Risiken unter Berücksichtigung der Art, des Umfangs und des Zwecks der Verarbeitung und der Ursachen der Risiken bewertet werden und die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen.
- 71) Dies sollte insbesondere für neu eingeführte umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, und die eine große Zahl von Personen betreffen könnten.
- 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) In Fällen, in denen die Datenschutz-Folgenabschätzung ergibt, dass der Verarbeitungsvorgang ungeachtet geplanter Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung der Risiken große konkrete Risiken für die Rechte und Freiheiten der betroffenen Personen bergen könnte, zum Beispiel das Risiko, dass infolge des Rückgriffs auf neue Technologien die betroffenen Personen nicht von ihren Rechten Gebrauch machen können oder unrechtmäßige oder willkürliche Diskriminierungen, einen schweren Identitätsdiebstahl, einen erheblichen finanziellen Schaden, eine erhebliche Rufschädigung oder einen anderen erheblichen wirtschaftlichen oder gesellschaftlichen Schaden erleiden, sollte die Aufsichtsbehörde vor Beginn dieser Verarbeitungsvorgänge zu Rate gezogen werden. Sie sollte Ratschläge zu der Frage erteilen, inwieweit der geplante Verarbeitungsvorgang gegen diese Verordnung verstoßen könnte. Sie sollte das Beratungersuchen innerhalb einer bestimmten Frist beantworten (...). Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen. Eine solche Konsultation sollte auch bei der Ausarbeitung von Rechts- oder Verwaltungsvorschriften, die die Verarbeitung von personenbezogenen Daten vorsehen und aufgrund der Art, des Umfangs und des Zwecks der Verarbeitung bestimmte Kategorien von betroffenen Personen erheblich beeinträchtigen können, erfolgen.

- 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 Vertreter bestimmter Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern sollten ermutigt werden, im Einklang mit dieser Verordnung stehende Verhaltenskodizes zu erstellen, 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 sollten in diesen Verhaltenskodizes unter Berücksichtigung der mit der Verarbeitung einhergehenden Risiken für die Rechte und Freiheiten der betroffenen Personen genau die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter festgelegt werden.
- 76a) Beim Verfassen oder bei der Änderung oder Ergänzung solcher Verhaltenskodizes sollten Verbände und oder andere Vertreter bestimmter Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern 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 Zertifizierungsmechanismen 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 von personenbezogenen Daten aus Drittländern und internationalen Organisationen und wieder zurück ist für die Entwicklung des internationalen Handels und der grenzübergreifenden Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Der durch diese Verordnung unionsweit garantierte Schutz natürlicher Personen sollte jedoch bei der Übermittlung von personenbezogenen Daten aus der Union in Drittländer oder an internationale Organisationen nicht unterminiert werden, und zwar auch dann, wenn aus einem Drittland oder von einer internationalen Organisation stammende personenbezogene Daten an ein anderes Drittland oder eine andere internationale Organisation weitergegeben werden. In jedem Fall sollten derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig sein. 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.
- 80) Die Kommission kann nach Erhalt und unter weitestgehender Berücksichtigung der Stellungnahme des Europäischen Datenschutzausschusses mit Wirkung für die gesamte Union beschließen, dass bestimmte Drittländer oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation einen angemessenen Datenschutz bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, einen solchen Schutz zu bieten, in der gesamten Union für Rechtssicherheit und eine einheitliche Rechtsanwendung sorgen. 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 Inaugenscheinnahme eines Drittlandes 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.
- 82) Die Kommission kann ebenso per Beschluss feststellen, dass ein bestimmtes Drittland oder bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation keinen angemessenen Datenschutz mehr bieten. Die Übermittlung personenbezogener Daten in dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen der Artikel 42 bis 43 werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden.
- 83) Bei Fehlen eines Angemessenheitsbeschlusses sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese Garantien können darin bestehen, dass auf verbindliche unternehmensinterne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, von einer Aufsichtsbehörde genehmigte 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. Sie sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame administrative und gerichtliche Rechtsbehelfe beachtet werden.

- 84) Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter offen stehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln zurückzugreifen, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter keinesfalls daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, 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 der gleichen Unternehmensgruppe genehmigte verbindliche unternehmensinterne Datenschutzvorschriften anwenden dürfen, sofern in diesen unternehmensinternen Vorschriften Grundprinzipien und durchsetzbare Rechte enthalten sind, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.
- 86) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre Einwilligung erteilt hat, wenn die Übermittlung im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Verfahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist. Die Übermittlung sollte zudem möglich sein, wenn sie zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaats festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn sie aus einem gesetzlich vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In diesem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

- 87) Diese Ausnahmeregelung sollte insbesondere für Datenübermittlungen gelten, die zur Wahrung eines wichtigen öffentlichen Interesses erforderlich sind, beispielsweise für den grenzüberschreitenden Datenaustausch zwischen Wettbewerbs-, Steuer-, Zoll- oder Finanzaufsichtsbehörden, zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten oder zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, insbesondere für die Verhinderung von Geldwäsche und die Bekämpfung der Terrorismusfinanzierung zuständigen Behörden. Die Übermittlung von personenbezogenen Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen Person zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben.
- 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 Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen und der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter sämtliche Umstände der Datenübermittlung geprüft hat. 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 Beurteilung der Frage, 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 Rechte und Garantien genießen, sobald die Daten übermittelt sind.

- 90) Manche Drittländer erlassen Gesetze, Verordnungen und sonstige Rechtsakte, durch die die Datenverarbeitungstätigkeiten von natürlichen und juristischen Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar reguliert werden. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets 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 in dieser Verordnung festgelegten Bedingungen für Datenübermittlungen in Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Weitergabe aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist. Die Bedingungen für das Bestehen eines wichtigen öffentlichen Interesses sollten von der Kommission in einem delegierten Rechtsakt näher festgelegt werden.
- 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 außerhalb der Grenzen ihres Mitgliedstaats durchzuführen. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, nicht übereinstimmende rechtliche Regelungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Daher bedarf es der Förderung einer engeren Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. 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 ermächtigt sind, ihre Aufgaben völlig unabhängig zu erfüllen, ist ein wesentliches Element des Schutzes des Einzelnen im Hinblick auf die Verarbeitung personenbezogener Daten. Die Mitgliedstaaten können mehr als eine Aufsichtsbehörde errichten, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.
- (92a) Die Tatsache, dass die Aufsichtsbehörden unabhängig sind, sollte nicht bedeuten, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden können.<sup>7</sup>
- 93) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er durch ein Rechtsinstrument sicherstellen, dass diese Aufsichtsbehörden am Kohärenz-Verfahren beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Kommission gewährleistet.
- 94) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die 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 Haushalt verfügen, der Teil des gesamten Staatshaushalts oder nationalen Haushalts sein kann.

---

<sup>7</sup> Presidency proposal in order to accommodate concerns raised by delegations that the wording of Article 47 would prevent this type of actions with regard to the supervisory authorities.

- 95) Die allgemeinen Anforderungen an die Mitglieder der Aufsichtsbehörde sollten gesetzlich von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des Mitgliedstaats ernannt werden (...).

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. Sie sollten sich nach Ablauf ihrer Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen ehrenhaft und zurückhaltend verhalten.

- 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 sie miteinander und mit der Kommission zusammenarbeiten.

- 97) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat statt, sollte eine einzige Aufsichtsbehörde für die Überwachung dieser Verarbeitungstätigkeiten des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der gesamten Union zuständig sein und die entsprechenden Entscheidungen, die den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter betreffen, fassen, damit die einheitliche Anwendung der Vorschriften verbessert, Rechtssicherheit gewährleistet und der Verwaltungsaufwand der für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verringert wird. Dies sollte nicht gelten, wenn der für die Verarbeitung Verantwortliche nicht in der Union niedergelassen ist; dann kann sein Vertreter von jeder Aufsichtsbehörde zusätzlich zu dem für die Verarbeitung Verantwortlichen oder an seiner Stelle als Ansprechpartner betrachtet werden.

Die Zuständigkeit der einzigen Aufsichtsbehörde sollte sich auf Maßnahmen erstrecken, die rechtliche Wirkungen entfalten sollen, wie beispielsweise die Genehmigung von verbindlichen unternehmensinternen Vorschriften und von Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen, Geldbußen und sonstige Sanktionen. Sie sollte sich jedoch nicht auf die Befugnis zur Durchsetzung ihrer Entscheidungen im Hoheitsgebiet eines anderen Mitgliedstaats erstrecken, es sei denn diese erfolgt im Rahmen von gemeinsamen Maßnahmen und mit Zustimmung des betreffenden Mitgliedstaats.

- 98) Die für die Überwachung der Verarbeitung und die diesbezüglichen Entscheidungen zuständige Aufsichtsbehörde, die die Aufgaben einer solchen zentralen Kontaktstelle übernimmt, sollte die Aufsichtsbehörde des Mitgliedstaats sein, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung hat. Allerdings sollten die Verarbeitungsvorgänge einer öffentlichen Behörde oder Einrichtung nur durch die Aufsichtsbehörde oder die Aufsichtsbehörden des Mitgliedstaats überwacht werden, in dem die öffentliche Behörde oder Einrichtung ihren Sitz hat.
- 99) Obgleich diese Verordnung auch für die Tätigkeit der nationalen Gerichte gilt, sollten – damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben unangetastet bleibt – die Aufsichtsbehörden nicht für personenbezogene Daten zuständig sein, die von Gerichten in ihrer gerichtlichen Eigenschaft verarbeitet werden. Diese Ausnahme sollte allerdings streng auf rein justizielle Tätigkeiten in Gerichtsverfahren begrenzt werden und sich nicht auf andere Tätigkeiten beziehen, mit denen je nach dem nationalen Recht Richter betraut sein können.
- 100) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und Befugnisse haben, darunter, insbesondere im Fall von Beschwerden Einzelner, Untersuchungsbefugnisse sowie rechtsverbindliche Interventions-, Entscheidungs- und Sanktionsbefugnisse sowie die Befugnis, Gerichtsverfahren anzustrengen. Die Aufsichtsbehörden sollten ihre Untersuchungsbefugnisse (...) im Einklang mit dem Unionsrecht und dem einzelstaatlichen Recht ausüben. Dies betrifft vor allem das Erfordernis einer vorherigen richterlichen Genehmigung.

- 101) Jede Aufsichtsbehörde sollte Beschwerden von betroffenen Personen bearbeiten und die Angelegenheit untersuchen. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person 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.
- Ist die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, nicht zuständig, sollte die zuständige Aufsichtsbehörde im Einklang mit den Bestimmungen dieser Verordnung über Zusammenarbeit und Kohärenz eng mit der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, zusammenarbeiten. In solchen Fällen, sollte die zuständige Aufsichtsbehörde bei Maßnahmen, die rechtliche Wirkungen entfalten sollen, unter anderem bei der Verhängung von Sanktionen und Geldbußen, den Standpunkt der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde und die weiterhin befugt sein sollte, in Abstimmung mit der zuständigen Aufsichtsbehörde Untersuchungen auf dem Hoheitsgebiet ihres eigenen Mitgliedstaats durchzuführen, weitestgehend berücksichtigen.
- 102) Die Aufklärungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinunternehmen sowie kleiner und mittlerer Unternehmen, und an die betroffenen Personen richten.
- 103) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist.

- 104) Jede Aufsichtsbehörde sollte berechtigt sein, an gemeinsamen Maßnahmen von Aufsichtsbehörden teilzunehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer festgelegten Frist antworten müssen.
- 105) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenz-Verfahren) eingeführt werden, das die Aufsichtsbehörden verpflichtet, miteinander und mit der Kommission zusammenzuarbeiten. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, ihre Befugnisse in Bezug auf Verarbeitungsvorgänge auszuüben, die für eine große Anzahl von betroffenen Personen in mehreren Mitgliedstaaten wesentliche Folgen haben (...) oder die den freien Verkehr personenbezogener Daten erheblich beeinträchtigen könnten. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragen, 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.
- 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 (...) Durchsetzung der (...) Entscheidung einer Aufsichtsbehörde sein. In anderen Fällen von grenzübergreifender Relevanz können die betroffenen Aufsichtsbehörden auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen, ohne auf das Kohärenz-Verfahren zurückzugreifen.
- 110) Auf Unionsebene sollte ein Europäischer Datenschutzausschuss eingerichtet werden. Dieser ersetzt die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten gebildet werden. Die Kommission sollte an seinen Beratungen ohne Stimmrecht teilnehmen. Der Europäische Datenschutzausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Europäische Datenschutzausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.
- 111) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Grundrechtecharta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist.

- 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. Diese Einrichtungen, Organisationen oder Verbände sollten das Recht haben, unabhängig von der Beschwerde einer betroffenen Person eine eigene Beschwerde einzulegen, wenn sie Grund zu der Annahme haben, dass es zu einer Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 32 Absatz 1 gekommen ist und Artikel 32 Absatz 3 nicht zur Anwendung gelangt.
- 113) Jede natürliche oder juristische Person sollte das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde haben. Für Verfahren gegen eine Aufsichtsbehörde sollten die Gerichte des Mitgliedstaats zuständig sein, in dem die Aufsichtsbehörde ihren Sitz hat. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit relevanten Sach- und Rechtsfragen zu prüfen, einschließt.
- 114) (...)
- 115) (...)
- 116) Bei Verfahren gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter sollte es dem Kläger überlassen bleiben, ob er die Gerichte des Mitgliedstaats anruft, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder des Mitgliedstaats, in dem die betroffene Person ihren gewöhnlichen Aufenthalt 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 rechtswidrigen Verarbeitung entstehen, sollten von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter ersetzt werden, die von ihrer Haftung befreit werden können, wenn sie nachweisen, dass ihnen der Schaden nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt.
- 118a) 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. Für die Verhängung von Sanktionen und Geldbußen sollte es angemessenen Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Grundrechtecharta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.
- 119) Die Mitgliedstaaten können die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, regeln. 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. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung verwaltungsrechtlicher Sanktionen 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.
- 121) Im Recht der Mitgliedstaaten sollten die Vorschriften über die Meinungsfreiheit, auch von Journalisten, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden, insbesondere, was die allgemeinen Grundsätze, die Rechte der betroffenen Person, die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter, die Übermittlung von Daten in Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden sowie die Zusammenarbeit und die einheitliche Rechtsanwendung betrifft. 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. (...)

- 122) Für die Verarbeitung von personenbezogenen Gesundheitsdaten als besonderer Datenkategorie, die eines höheren Schutzes bedarf, lassen sich häufig berechtigte Gründe zugunsten des Einzelnen wie der Gesellschaft insgesamt anführen, insbesondere wenn es darum geht, die Kontinuität der Gesundheitsversorgung über die Landesgrenzen hinaus zu gewährleisten. Diese Verordnung sollte daher vorbehaltlich besonderer und geeigneter Garantien zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen die Bedingungen für die Verarbeitung personenbezogener Gesundheitsdaten harmonisieren. Dies schließt das Recht natürlicher Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.
- 123) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, personenbezogene Gesundheitsdaten auch ohne Einwilligung der betroffenen Person zu verarbeiten. In diesem Zusammenhang sollte der Begriff "öffentliche Gesundheit" im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates 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 und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen 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 Arbeitnehmer, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.

- 124) Die allgemeinen Grundsätze des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten sollten auch im Beschäftigungskontext gelten. Die Mitgliedstaaten sollten daher in den Grenzen dieser Verordnung die Verarbeitung personenbezogener Daten im Beschäftigungskontext gesetzlich regeln können.
- (124a) Was die Statistik betrifft, so enthält 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 <sup>8</sup> genauere Bestimmungen zur Vertraulichkeit statistischer Informationen.
- 125) Die Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen (...) Zwecken sollte, um rechtmäßig zu sein, auch anderen einschlägigen Rechtsvorschriften, beispielsweise für klinische Versuche, genügen.
- 126) (...) Die Verarbeitung von personenbezogenen Daten für wissenschaftliche Zwecke 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.

---

<sup>8</sup> ABl. L 87 vom 31.3.2009, S. 164-173.

- 127) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten gesetzlich regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen.
- 128) Im Einklang mit Artikel 17 des Vertrags über die Arbeitsweise der Europäischen Union achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht. Wendet eine Kirche in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, sollten diese Regeln weiter gelten, wenn sie mit dieser Verordnung in Einklang gebracht werden. Kirchen und religiöse Vereinigungen oder Gemeinschaften sollten verpflichtet werden, eine völlig unabhängige Datenschutzaufsicht einzurichten.

- 129) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, Rechtsakte nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union zu erlassen. Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, Rechtsakte nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union zu erlassen. Delegierte Rechtsakte sollten insbesondere erlassen werden in Bezug auf die Rechtmäßigkeit der Verarbeitung, zur Festlegung der Kriterien und Bedingungen für die Einwilligung eines Kindes, für die Verarbeitung besonderer Kategorien personenbezogener Daten, zur Beurteilung offensichtlich unverhältnismäßiger Anträge und Gebühren für die Ausübung der Rechte der betroffenen Person, zur Festlegung der Kriterien und Anforderungen im Hinblick auf die Unterrichtung der betroffenen Person sowie in Bezug auf deren Auskunftsrecht, in Bezug auf das Recht auf Vergessenwerden und auf Löschung, betreffend auf Profiling basierende Maßnahmen, zur Festlegung der Kriterien und Anforderungen betreffend die Pflichten des für die Verarbeitung Verantwortlichen und den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, in Bezug auf Auftragsverarbeiter, zur Festlegung der Kriterien und Anforderungen betreffend die Dokumentation und die Sicherheit der Verarbeitung, zur Festlegung der Kriterien und Anforderungen für die Feststellung einer Verletzung des Schutzes personenbezogener Daten und für deren Meldung bei der Aufsichtsbehörde sowie für die Umstände, unter denen anzunehmen ist, dass sich eine solche Verletzung negativ auf die betroffene Person auswirken wird, zur Festlegung der Kriterien und Bedingungen für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung erforderlich ist, zur Festlegung der Kriterien und Anforderungen für die Bestimmung hoher konkreter Risiken, die eine vorherige Zurateziehung der Aufsichtsbehörde erfordern, für die Benennung des Datenschutzbeauftragten und dessen Aufgaben, in Bezug auf Verhaltensregeln, zur Festlegung der Kriterien und Anforderungen für Zertifizierungsverfahren und für die Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften, zur Regelung der Ausnahmen für Datenübermittlungen, zur Festlegung der verwaltungsrechtlichen Sanktionen, in Bezug auf die Datenverarbeitung für Gesundheitszwecke, im Beschäftigungskontext und zu historischen, statistischen und wissenschaftlichen Zwecken (...). Es ist besonders wichtig, dass die Kommission im Rahmen ihrer Vorarbeiten auch auf Sachverständigenebene geeignete Konsultationen durchführt. Die Kommission sollte bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte dafür sorgen, dass das Europäische Parlament und der Rat die entsprechenden Dokumente gleichzeitig, rechtzeitig und in geeigneter Form erhalten.

130) Um einheitliche Bedingungen für die Anwendung dieser Verordnung sicherzustellen, sollten der Kommission Durchführungsbefugnisse übertragen werden zur Festlegung von Standardvorlagen für die Verarbeitung personenbezogener Daten von Kindern, Standardverfahren und -vorlagen für die Ausübung der Rechte der betroffenen Person, Standardvorlagen für die Unterrichtung der betroffenen Person, Standardverfahren und -vorlagen für das Auskunftsrecht und das Recht auf Datenübertragbarkeit, Standardvorlagen betreffend die Pflichten des für die Verarbeitung Verantwortlichen in Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie in Bezug auf Dokumentation, besonderen Anforderungen für die Sicherheit der Verarbeitung, Standardformat und Verfahren für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und für die Benachrichtigung der betroffenen Person, Standards und Verfahren für Datenschutz-Folgenabschätzungen, Verfahren und Vorlagen für die vorherige Genehmigung und vorherige Zurateziehung der Aufsichtsbehörde, technischen 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, Fällen der Datenweitergabe, die nicht im Einklang mit dem Unionsrecht stehen, Vorschriften für die Amtshilfe, gemeinsamen Maßnahmen und Beschlüssen im Rahmen des Kohärenzverfahrens. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren<sup>9</sup>, ausgeübt werden. Die Kommission sollte besondere Maßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen erwägen.

---

<sup>9</sup> Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

- 131) Die Standardvorlagen für die Einwilligung im Falle von Kindern, die Standardverfahren und -vorlagen für die Ausübung der Rechte der betroffenen Person, die Standardvorlagen für die Unterrichtung der betroffenen Person, die Standardverfahren und -vorlagen für das Auskunftsrecht und das Recht auf Datenübertragbarkeit, die Standardvorlagen betreffend die Pflichten des für die Verarbeitung Verantwortlichen in Bezug auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie in Bezug auf Dokumentation, die besonderen Anforderungen für die Sicherheit der Verarbeitung, das Standardformat und die Verfahren für die Meldung einer Verletzung des Schutzes von personenbezogenen Daten bei der Aufsichtsbehörde und für die Benachrichtigung der betroffenen Person, die Standards und Verfahren für Datenschutz-Folgenabschätzungen, die Verfahren und Vorlagen für die vorherige Genehmigung und vorherige Zurateziehung der Aufsichtsbehörde, die technischen Standards und Verfahren für die Zertifizierung, die Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland oder in einem Gebiet oder Verarbeitungssektor dieses Drittlands oder in einer internationalen Organisation, die Fälle der Datenweitergabe, die nicht im Einklang mit dem Unionsrecht stehen, die Vorschriften für die Amtshilfe, für gemeinsame Maßnahmen und Beschlüsse im Rahmen des Kohärenzverfahrens sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.
- 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, und sich auf Angelegenheiten beziehen, die von Aufsichtsbehörden im Rahmen des Kohärenzverfahrens mitgeteilt wurden, 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, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem Subsidiaritätsprinzip gemäß Artikel 5 des Vertrags über die Europäische Union tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht diese Verordnung nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.
- 134) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Die Genehmigungen der Aufsichtsbehörden und die Beschlüsse der Kommission auf der Grundlage der Richtlinie 95/46/EG sollten jedoch in Kraft bleiben.
- 135) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG festgelegten spezifischen Pflichten, die dasselbe Ziel verfolgen, unterliegen einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Um das Verhältnis zwischen dieser Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden.
- 136) (...)
- 137) (...)
- 138) (...) <sup>10</sup>.
- 139) (...) <sup>11</sup>

---

<sup>10</sup> Recitals 136, 137 and 138 were deleted as this proposal is not Schengen relevant. COM scrutiny reservation on deletion.

<sup>11</sup> Former recital 139 was moved up to recital 3a so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.



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 <sup>12</sup>.
2. Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
3. Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt oder verboten werden. <sup>13 14</sup>.

---

<sup>12</sup> DE scrutiny reservation: DE thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to internal market implications of the data processing operations.

<sup>13</sup> DK, FR, NL, SI scrutiny reservation. FR thought that this paragraph, which was copied from the 1995 Data Protection Directive (1995 Directive 95/46), did not make sense in the context of a Regulation as this was directly applicable.

<sup>14</sup> EE, FI, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. This is now regulated in Articles 80 and 80a of the draft Regulation.

## 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 <sup>15</sup>.
2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird
  - a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt (...),
  - b) (...),
  - c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union fallen,
  - d) durch natürliche Personen zu (...) persönlichen oder familiären Zwecken (...),
  - e) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung einer Straftat und zu diesen Zwecken <sup>16</sup> zur Aufrechterhaltung der öffentlichen Ordnung oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen staatlichen Behörden.
3. (...).

---

<sup>15</sup> HU objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording 'irrespective of the means by which personal data are processed'.

<sup>16</sup> BE reservation on the terms 'for these purposes'.

*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, diesen Personen Waren oder Dienstleistungen in der Union anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist;
  - b) der Beobachtung ihres Verhaltens dient, soweit ihr Verhalten in der Europäischen Union erfolgt <sup>17</sup>.
3. Diese Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

---

<sup>17</sup> UK reservation.

*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 (...), etwa mittels Zuordnung zu einer Kennung<sup>18</sup> wie einem Namen, 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) "pseudonymisierte Daten" personenbezogene Daten, die so verarbeitet werden, dass die Daten ohne Heranziehung 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 gewährleisten<sup>19</sup>.

---

<sup>18</sup> UK is concerned that, together with recital 24, this will lead to risk-averse approach that this is always personal data.

<sup>19</sup> BE, DE, IT, SI, PL and PT scrutiny reservation. FR and UK reservation. FR and PL queried the need for a definition of pseudonymous data. UK thought the definition was too strict, making pseudonymous data tantamount to anonymous data

- (3) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung oder das Löschen (...) Daten <sup>20</sup>;
- (3a) „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken <sup>21</sup>;
- (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 <sup>22</sup>;
- (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, können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach einzelstaatlichem oder Unionsrecht bestimmt werden;

---

<sup>20</sup> DE, FR and NL regretted that the blocking of data was not included in the list of data processing operations as this was a means especially useful in the public sector. COM indicated that the right to have the processing restricted in certain cases was provided for in Article 17(4) (restriction of data processing), even though the terminology 'blocking' was not used there. DE and FR thought the definition of Article 4(3) (erasure) should be linked to Article 17.

<sup>21</sup> RO scrutiny reservation.

<sup>22</sup> DE, FR SI, SK and UK scrutiny reservation. DE and SI thought this was completely outdated concept. COM explained that the definition had been taken over from Directive 95/46/EC and is related to the technical neutrality of the Regulation, as expressed in Article 2(1).

- (6) "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet; <sup>23</sup>
- (7) "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere, nicht mit der betroffenen Person, dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter identische Stelle, an die personenbezogene Daten weitergegeben werden; <sup>24</sup>Verwaltungsstellen und Behörden, die in Ausübung ihrer Amtshandlungen personenbezogene Daten erhalten können, gelten jedoch nicht als Empfänger <sup>25</sup>;
- (8) "Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte (...) <sup>26</sup> 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<sup>27</sup>;

<sup>23</sup> DE, DK, FR, LU and NL requested the inclusion of a definition of third party.  
<sup>24</sup> PT reservation. DE, FR, LU, NL, SI and SE regretted the deletion from the 1995 Data Protection Directive of the reference to third party disclosure and pleaded in favour of its reinstatement. COM argued that this reference was superfluous and that its deletion did not make a substantial difference.

<sup>25</sup> DE, ES, NL and UK scrutiny reservation on latter part of definition. ES, NL and UK thought it could be deleted.

<sup>26</sup> COM, CY, FR, GR, HU, IT, PL and RO reservation on the deletion of 'explicit'.

<sup>27</sup> COM, supported by LU, explained that it sought to have a similar rule as in the E-Privacy Directive, which should be extended to all types of data processing. DE scrutiny reservation questioned the very broad scope of the duty of notifying data breaches, which so far under German law was limited to sensitive cases. NL, LV and PT concurred with DE and thought this could lead to over-notification. In the meantime the scope of Articles 31 and 32 has been limited.

- (10) „genetische Daten“ personenbezogene Daten jedweder Art zu den ererbten oder erworbenen genetischen Merkmalen eines Menschen, die aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden <sup>28</sup>;
- (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 <sup>29</sup> oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten <sup>30</sup>;
- (12) „Gesundheitsdaten“ Daten, die sich auf die körperliche oder geistige Gesundheit einer Person beziehen und Informationen über ihren Gesundheitszustand enthalten <sup>31</sup>;

---

<sup>28</sup> AT, CY, FR, IT, NL and SE scrutiny reservation. Several delegations (CH, CY, DE and SE) expressed their surprise regarding the breadth of this definition, which would also cover data about a person's physical appearance. DE thought the definition should differentiate between various types of genetic data. Prüfungsvorbehalt von AT. The definition is now explained in the recital 25a.

<sup>29</sup> ES preferred 'allows'; SI suggested 'allows or confirms'

<sup>30</sup> NL, SE and AT scrutiny reservation. SI did not understand why genetic data were not included in the definition of biometric data. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. CH is of the opinion that the term 'biometric data' is too broadly defined.

<sup>31</sup> CZ, DE, DK, EE, FR and SI expressed their surprise regarding the breadth of this definition. AT, BE, DE, NL, SI and LT scrutiny reservation. COM scrutiny reservation.

(12a) "Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, mit der durch die Evaluierung persönlicher Aspekte, die sich auf eine natürliche Person beziehen, insbesondere die Analyse und Prognose von Aspekten über Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel ein persönliches Profil erstellt oder genutzt werden soll <sup>32</sup>;

(13) „Hauptniederlassung“

- im Falle des für die Verarbeitung Verantwortlichen der Ort seiner Niederlassung in der Union, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke (...) und Mittel der Verarbeitung personenbezogener Daten getroffen werden; wird über die Zwecke (...) und Mittel der Verarbeitung personenbezogener Daten nicht in der Union entschieden, ist die Hauptniederlassung der Ort, an dem die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen in der Union hauptsächlich stattfinden <sup>33</sup>;
- im Falle des Auftragsverarbeiters den Ort, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, und wenn er keine Hauptverwaltung in der Union hat, den Ort, an dem die wesentlichen Verarbeitungstätigkeiten stattfinden; <sup>34</sup>

---

<sup>32</sup> BE, RO and SE scrutiny reservation. BE, FR, LU, SI and RO would prefer reverting to the Council of Europe definition. COM reservation.

<sup>33</sup> BE, CZ DE, EE and SK scrutiny reservation: they expressed concerns about this definition, which might be difficult to apply in practice. DE thought it needed to be examined in conjunction with the one-stop-shop rules in Article 51. IE remarked this place may have no link with the place where the data are processed. DE also remarked that in the latter scenario, the Commission proposal did not determine which Member States' DPA would be competent. CZ thought the definition should be deleted.

<sup>34</sup> This definition will be revisited when discussing Chapter V.



Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, gilt die Hauptniederlassung des für die Verarbeitung verantwortlichen Unternehmens als Hauptniederlassung der Unternehmensgruppe, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt;

- (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 Verpflichtungen (...) 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 <sup>35</sup>;
- (17) „verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet <sup>36</sup>;
- (18) (...) <sup>37</sup>

---

<sup>35</sup> DE scrutiny reservation. UK scrutiny reservation on all definitions in paragraphs 10 to 16.

<sup>36</sup> DE wondered whether BCRs could also cover intra-EU data transfers.

<sup>37</sup> COM scrutiny reservation on the deletion of the definition of a child.

- (19) „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 46 eingerichtete unabhängige staatliche Stelle;
- (20) "Dienste der Informationsgesellschaft" Dienste, wie sie in Artikel 1 Absatz 2 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft definiert sind <sup>38 39 40</sup>.

---

<sup>38</sup> OJ L 204, 21.7.1998, p. 37–48.

<sup>39</sup> UK suggests adding a definition of 'competent authority' corresponding to that of the future Data Protection Directive.

<sup>40</sup> BE, DE; FR and RO suggest adding a definition of 'transfer' ('communication or availability of the data to one or several recipients'). RO suggests adding 'transfers of personal data to third countries or international organizations is a transmission of personal data object of processing or designated to be processed after transfer which ensure an adequate level of protection, whereas the adequacy of the level of protection afforded by a third country or international organization must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations'.

## 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 historische, statistische oder wissenschaftliche Zwecke gilt vorbehaltlich der in Artikel 83 aufgeführten Bedingungen und Garantien nicht als unvereinbar <sup>41</sup>;
  - c) dem Verarbeitungszweck entsprechen, sachlich relevant und in Bezug auf die Zwecke, für die sie verarbeitet sein, verhältnismäßig sein (...) <sup>42</sup>;
  - 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;

---

<sup>41</sup> This is without prejudice to later agreement on the regime for historical, statistical or scientific purposes in Article 83 and on the rules on further processing for incompatible purposes in Article 6(3a).

<sup>42</sup> COM reservation on the deletion of the data minimisation principle.

- 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 (...) zu historischen, statistischen oder wissenschaftlichen Zwecken (...) gemäß Artikel 83 verarbeitet werden <sup>43</sup> (...);
  - (ee) so vereinbart 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*** <sup>44</sup>

1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
  - a) Die betroffene Person hat ihre unmissverständliche <sup>45</sup> Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben <sup>46</sup>.
  - 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.

---

<sup>43</sup> This is without prejudice to later agreement on the regime for historical, statistical or scientific purposes in Article 83.

<sup>44</sup> DE, AT, PT, SI and SK scrutiny reservation.

<sup>45</sup> COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'

<sup>46</sup> UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

- c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt <sup>47</sup>.
- d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen <sup>48</sup>.
- 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 <sup>49 50</sup>.
- f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen <sup>51</sup> des für die Verarbeitung Verantwortlichen oder eines für die Verarbeitung Verantwortlichen, an den die Daten weitergegeben werden <sup>52</sup>, 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. Dieser Unterabsatz gilt nicht für die von Behörden in Erfüllung ihrer öffentlichen Aufgaben vorgenommene Verarbeitung <sup>53 54</sup>.

---

<sup>47</sup> HU thought that this subparagraph could be merged with 6(1) (e).  
<sup>48</sup> BG and ES scrutiny reservation; UK preferred the wording of the 1995 Directive.  
<sup>49</sup> COM clarified that this was the main basis for data processing in the public sector. DE, DK, LT and UK asked what was meant by 'public interest' whether the application of this subparagraph was limited to the public sector or could also be relied upon by the private sector. FR also requested clarifications as to the reasons for departing from the text of the 1995 Directive. UK suggested reverting to the wording used in Article 7(e) of the 1995 Directive.  
<sup>50</sup> The Presidency is of the opinion that subparagraphs (d) and (e) should be inverted.  
<sup>51</sup> FR and LT scrutiny reservation.  
<sup>52</sup> BG, CZ, DE, ES, HU, IT, NL, SE and UK asked to reinstate the words 'or by a third party' from the 1995 Directive. COM, supported by FR, thought that the use of the concept '*a controller*' should allow covering most cases of a third party.  
<sup>53</sup> ES and FR scrutiny reservation. BE, DK, SI, PT and UK had suggested deleting the last sentence.  
<sup>54</sup> DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified.

2. (...)
3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e<sup>55</sup> müssen eine Rechtsgrundlage haben im
- a) Unionsrecht oder
  - b) innerstaatlichen Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.

Der Zweck der Verarbeitung wird in dieser Rechtsgrundlage festgelegt oder ist hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. Im Rahmen dieser Verordnung können der für die Verarbeitung Verantwortliche, die Verarbeitungsvorgänge und -verfahren einschließlich von Maßnahmen zur Gewährleistung einer rechtmäßigen und nach Treu und Glauben vorgenommen Verarbeitung in dieser Rechtsgrundlage aufgeführt werden. <sup>56</sup>

- 3a) Um sich zu vergewissern, ob ein Zweck der Weiterverarbeitung mit demjenigen vereinbar ist, zu dem die Daten ursprünglich erhoben wurden, berücksichtigt der für die Verarbeitung Verantwortliche u.a. <sup>57</sup>
- a) jede Verbindung zwischen den Zwecken, für die die Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;

---

<sup>55</sup> FI and SI thought (f) should be added. BE, HU and FR thought (e) should be deleted. NL proposed adding a sentence: 'The purpose of the processing referred to in point (e) must be associated with the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

<sup>56</sup> DK and DE scrutiny reservation; it was emphasised national law should not only have the possibility to specify, but also to enlarge the data protection rules of the Regulation.

<sup>57</sup> DK, FI, NL, SI and SE stressed that the list should not be exhaustive. PT wanted to add consent by the data subject as an element.

- b) den Zusammenhang, in dem die Daten erhoben wurden;
  - c) die Art der personenbezogenen Daten;
  - d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
  - e) das Vorhandensein angemessener Garantien <sup>58</sup>.
4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Weiterverarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e <sup>59</sup> genannten Gründe <sup>60 61 62</sup> zutreffen.
5. (...).

---

<sup>58</sup> BG, DE, ES and PL reservation: safeguards in themselves do not make further processing compatible.

<sup>59</sup> FR and ES thought (f) should be added.

<sup>60</sup> DE, HU, IT, NL and PT scrutiny reservation. IT and PT thought paragraph 4 could be deleted.

<sup>61</sup> BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to in recital 40. BE, supported by FR, suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

<sup>62</sup> HU thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here: 'Where personal data relating to the data subject are processed under this provision the controller shall inform the data subject according to Article 14 before the time of or within a reasonable period after the commencement of the first operation or set of operations performed upon the personal data for the purpose of further processing not compatible with the one for which the personal data have been collected.'

## Artikel 7

### **Einwilligung**

1. In den Fällen, in denen Artikel 6 Absatz 1 a zur Anwendung kommt, kann der für die Verarbeitung Verantwortliche nachweisen, dass die betroffene Person ihre unmissverständliche<sup>63</sup> Einwilligung erteilt hat.
  
- (1a) In den Fällen, in denen Artikel 9 Absatz 2 a zur Anwendung kommt, kann der für die Verarbeitung Verantwortliche nachweisen, dass die betroffene Person ihre ausdrückliche Einwilligung erteilt hat.
  
2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung so erfolgen, das 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.
  
4. (...).

---

<sup>63</sup> COM reservation related to the deletion of 'explicit' in the definition of consent.



*Artikel 8*  
**Bedingungen für die Einwilligung eines Kindes in Bezug auf  
Dienste der Informationsgesellschaft**<sup>64</sup>

1. In den Fällen, in denen Artikel 6 Absatz 1 Buchstabe a zur Anwendung kommt, ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr<sup>65</sup>, dem<sup>66</sup> direkt Dienste der Informationsgesellschaft angeboten werden, nur rechtmäßig, wenn und insoweit diese Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird.

Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um in solchen Fällen nachzuprüfen, dass eine Einwilligung erteilt oder von den Eltern oder vom Vormund des Kindes erlaubt 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<sup>67</sup>.

---

<sup>64</sup> CZ, DE, AT, SE, SI, PT and UK scrutiny reservation. CZ and SI would prefer to see this Article deleted. NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. DE, supported by NO, opined this article could have been integrated into Article 7

<sup>65</sup> Several delegations queried the expediency of setting the age of consent at 13 years: DE, FR, HU, LU, LV, RO and SI. DE, SI and RO proposed 14 years. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA).

<sup>66</sup> Several delegations (HU, FR, SE, PT) asked why the scope of this provision was restricted to the offering of information society services or wanted clarification (DE) whether it was restricted to marketing geared towards children. The Commission clarified that this provision was also intended to cover the use of social networks, insofar as this was not governed by contract law. DE thought that this should be clarified. HU and FR thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.

<sup>67</sup> DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law. SI thought the reference should be worded more broadly to 'civil law', thus encompassing also personality rights.

3. [Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 näher zu regeln (...)<sup>68</sup>.
4. Die Kommission kann Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen]<sup>69</sup>.

#### *Artikel 9*

#### ***Verarbeitung besonderer Kategorien von personenbezogenen Daten***<sup>70</sup>

1. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten und Daten über Gesundheit oder Sexualleben (...) <sup>71</sup> ist untersagt. <sup>72</sup>

---

<sup>68</sup> ES, FR and SE scrutiny reservation.

<sup>69</sup> LU reservation. ES, FR, SE and UK suggested deleting paragraphs 3 and 4.

<sup>70</sup> SE, AT and NL scrutiny reservation. DE, supported by CZ, SE and UK, criticised on the concept of special categories of data, which does not cover all sensitive data processing operations. CZ, SE and UK pleaded in favour of a risk-based approach to sensitive data. The Presidency thought there was no majority in favour of such 'open' approach. SK and RO thought the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. SK also led in favour of the inclusion of national identifier.

<sup>71</sup> The reference to criminal convictions and criminal offences has been deleted.

<sup>72</sup> EE reservation; SE scrutiny reservation UK questioned the need for special categories of data. NL thought the list of data was open to discussion, as some sensitive data like those related to the suspicion of a criminal offence, were not included. SE thought the list was at the same time too broad and too strict. SI thought the list of the 1995 Data Protection Directive should be kept. FR and AT stated that the list of special categories in the Regulation and the Directive should be identical.

2. Absatz 1 gilt nicht in folgenden Fällen:
- a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten (...) <sup>73</sup> 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 seine ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen arbeitsrechtlichen Pflichten nachkommen kann, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist <sup>74</sup>, oder
  - c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich und die betroffene Person ist aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder
  - d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Erwerbszweck im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder

---

<sup>73</sup> Deleted at the suggestion of ES: the reference to Articles 7 and 8 was superfluous.

<sup>74</sup> DE queried whether this paragraph obliged Member States to adopt specific laws on data protection regarding labour law relations; COM assured that the paragraph merely referred to a possibility to do so.

- e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat <sup>75</sup>, oder
- f) die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich <sup>76</sup>, oder
- g) die Verarbeitung ist erforderlich, um auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, aus wichtigen <sup>77</sup> Gründen des öffentlichen Interesses eine Aufgabe zu erfüllen, oder
- h) die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Artikels 81 für Gesundheitszwecke erforderlich <sup>78</sup>, oder
- i) die Verarbeitung ist vorbehaltlich der Bedingungen und Garantien des Artikels 83 für historische, statistische oder wissenschaftliche Zwecke (...) erforderlich.
- j) (...)

---

<sup>75</sup> DE, FR, SE and SI raised questions regarding the exact interpretation of the concept of manifestly made public (e.g. whether this also encompassed data implicitly made public and whether the test was an objective or a subjective one).

<sup>76</sup> DE thought it should be clarified that also courts can process sensitive data.

<sup>77</sup> ES, FR and UK scrutiny reservation on 'important'.

<sup>78</sup> Prüfungsvorbehalt von DE und SE. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.

- (2a) *die Verarbeitung von Daten über Strafurteile und Straftaten<sup>79</sup> oder damit zusammenhängende Sicherungsmaßnahmen darf nur entweder unter behördlicher Aufsicht oder aufgrund einer (...) Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung einer Aufgabe aus wichtigen Gründen des öffentlichen Interesses vorgenommen werden, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorsehen muss, zulässig ist<sup>80</sup>. Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden<sup>81</sup>.*
3. (...)

#### *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 erforderlich, ist dieser nicht verpflichtet, zur bloßen Einhaltung (...) dieser Verordnung zusätzliche Informationen einzuholen oder eine zusätzliche Verarbeitung vorzunehmen<sup>82</sup>, um die betroffene Person zu bestimmen<sup>83</sup>.

---

<sup>79</sup> EE reservation: under its constitution all criminal convictions are mandatorily public.  
<sup>80</sup> Prüfungsvorbehalt. UK queried the relationship between this paragraph and Article 2(2) (c). COM argued that the reference to civil proceedings in Article 8(5) of the 1995 Directive need not be included here, as those proceedings are as such not sensitive data. DE and SE were not convinced by this argument.  
<sup>81</sup> SE scrutiny reservation. UK reservation on last sentence.  
<sup>82</sup> BE proposal, supported by ES.  
<sup>83</sup> AT, DE, FR, HU and UK scrutiny reservation.

2. Kann der für die Verarbeitung Verantwortliche in derartigen Fällen die betroffene Person nicht bestimmen, 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 <sup>84</sup>.

---

<sup>84</sup> DK, NL, SE and SI scrutiny reservation; COM reservation. BE thought this paragraph could also be moved to a recital.

# KAPITEL III RECHTE DER BETROFFENEN PERSON <sup>85</sup>

## 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* <sup>86</sup>

1. Der für die Verarbeitung Verantwortliche trifft die erforderlichen 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 <sup>87</sup>. Die Übermittlung der Informationen erfolgt schriftlich oder gegebenenfalls in elektronischer oder anderer Form.
- 1a. Der für die Verarbeitung Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 19 <sup>88</sup>. (...)

---

<sup>85</sup> General scrutiny reservation by UK on the articles in this Chapter.

<sup>86</sup> DE, SE, SI and FI scrutiny reservation.

<sup>87</sup> COM reservation on deletion.

<sup>88</sup> SI and UK thought this paragraph should be deleted.

2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person die Informationen gemäß den Artikeln 14a und 15 und Informationen über auf Antrag gemäß den Artikeln 16 bis 19 ergriffene Maßnahmen ohne unnötige Verzögerung und spätestens innerhalb eines Monats nach Eingang des Antrags <sup>89</sup> zur Verfügung (...). Diese Frist kann aufgrund der Komplexität des Antrags und der Zahl von Anträgen erforderlichenfalls um weitere zwei Monate verlängert werden. Kommt es zu einer Fristverlängerung, 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, unterrichtet er die betroffene Person unverzüglich 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 – besonders im Fall ihrer Häufung – unverhältnismäßigen Anträgen <sup>90</sup> einer betroffenen Person kann sich der für die Verarbeitung Verantwortliche weigern, aufgrund des Antrags tätig zu werden <sup>91</sup> (...). In diesem Fall hat er den Nachweis für den offenkundig unbegründeten oder unverhältnismäßigen Charakter des Antrags zu erbringen <sup>92</sup>.

---

<sup>89</sup> UK pleaded in favour of deleting the one-month period. BG and PT thought it more simple to revert to the requirement of 'without excessive delay' under the 1995 Data Protection Directive.

<sup>90</sup> LT and PL thought the criterion of 'manifestly excessive' required further clarification, e.g. through an additional recital. COM reservation on deletion.

<sup>91</sup> NL scrutiny reservation: avoid that this gives the impression that public authority cannot refuse to consider request by citizen.

<sup>92</sup> IT scrutiny reservation.



- 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<sup>93</sup> zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind<sup>94</sup>.
5. (...)
6. (...)

*Artikel 13*

***Rechte gegenüber Empfängern***

(...)

---

<sup>93</sup> ES proposal.

<sup>94</sup> Further to UK proposal.

## ABSCHNITT 2

### INFORMATIONSPFLICHT UND AUSKUNFTSRECHT

#### *Artikel 14*

#### *Informationspflicht bei Erhebung der Daten bei der betroffenen Person* <sup>95</sup>

- 1 <sup>96</sup>. Werden personenbezogene Daten bei der betroffenen Person erhoben, 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 können gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten angegeben werden;
  - b) die Zwecke, für die die Daten verarbeitet werden (...).

---

<sup>95</sup> DE, EE, ES, NL, SE, FI, PT and UK scrutiny reservation. DE, supported by ES and NL, has asked the Commission to provide an assessment of the extra costs for the industry under this provision.

<sup>96</sup> HU thought the legal basis of the processing should be included in the list.

- 1a. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person<sup>97</sup> folgende weiteren Informationen zur Verfügung, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden,<sup>98</sup> notwendig sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten<sup>99 100</sup>.
- a) (...);
- b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen verfolgt werden;
- c) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten<sup>101</sup>;
- d) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln;

---

<sup>97</sup> DE, EE, and PL asked to insert "on request". DE, DK, NL and UK doubted whether the redraft would allow for a sufficient risk-based approach and warned against excessive administrative burdens/compliance costs. DK and UK in particular referred to the difficulty for controllers in assessing what is required under para. 1a in order to ensure fair and transparent processing. DE, EE and PL pleaded for making the obligation to provide this information contingent upon a request thereto as the controller might otherwise take a risk-averse approach and provide all the information under Article 14(1a), also in cases where not required. UK thought that many of the aspects set out in paragraph 1a of Article 14 (and paragraph 2 of Article 14a) could be left to guidance under Article 39.

<sup>98</sup> CZ suggested adding the word 'obviously'.

<sup>99</sup> FR scrutiny reservation.

<sup>100</sup> COM reservation on deletion of the words 'such as'.

<sup>101</sup> AT and DE thought that this concept was too vague (does it e.g. encompass employees of the data controller?).

- 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 (...) <sup>102</sup>,
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...);
- g) ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche mögliche Folgen die Verweigerung ihrer Bereitstellung hätte <sup>103</sup> und
- h) Hinweis auf ein Profiling der betroffenen Person gemäß Artikel 20 Absätze 1 und 3 und Angaben zum Profiling sowie zu seiner Tragweite und seinen angestrebten Auswirkungen. <sup>104</sup>*
2. (...) <sup>105</sup>
3. (...)
4. (...)
5. Die Absätze 1 und 1a finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.
6. (...)
7. (...)
8. (...)

---

<sup>102</sup> The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE.

<sup>103</sup> CZ, DE, ES and NL reservation.

<sup>104</sup> SE scrutiny reservation. At the suggestion of PL the reference to 'logic' has been deleted.

<sup>105</sup> HU reservation on the deletion of this paragraph.

**Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden** <sup>106</sup>

- 1 <sup>107</sup>. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, 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 können gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten angegeben werden;
  - b) die Zwecke, für die die Daten verarbeitet werden.
2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person folgende weiteren Informationen zur Verfügung, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen <sup>108</sup>, 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 verfolgt werden;
  - d) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

---

<sup>106</sup> DE, EE, ES, NL (§§1+2), AT, PT scrutiny reservation.

<sup>107</sup> HU thought the legal basis of the processing should be included in the list.

<sup>108</sup> ES, IT and FR doubts on the addition of the words 'and context'.

- e) das Bestehen eines Rechts auf Auskunft seitens des für die Verarbeitung Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf deren Berichtigung oder Löschung und eines Widerspruchsrechts gegen die Verarbeitung dieser Daten (...);
  - f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...);
  - g) den Ursprung der Daten, sofern diese nicht aus öffentlich zugänglichen Quellen stammen <sup>109</sup>;
  - h) *Hinweis auf ein Profiling der betroffenen Person gemäß Artikel 20 Absätze 1 und 3 und Angaben zum Profiling sowie zu seiner Tragweite und seinen angestrebten Auswirkungen.* <sup>110</sup>
3. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2 <sup>111</sup>
- a) innerhalb einer angemessenen Frist nach der Erhebung der Daten unter Berücksichtigung der spezifischen Umstände ihrer Verarbeitung oder,
  - b) falls die Weitergabe an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.

---

<sup>109</sup> COM and AT scrutiny reservation.

<sup>110</sup> PL asks for the deletion of the reference to 'logic'.

<sup>111</sup> BE proposed to add: 'possibly through an easily accessible contact person where the data subject concerned can consult his data'. This is already covered by the modified recital 46.

4. Die Absätze 1 bis 3 finden keine Anwendung, wenn und soweit
- a) die betroffene Person bereits über die Informationen verfügt oder
  - b) die Erteilung dieser Informationen – insbesondere bei der Verarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke<sup>112</sup> – sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde oder wenn die Wahrscheinlichkeit besteht, dass sie die Erreichung dieser Zwecke unmöglich macht oder ihr ernsthaft entgegensteht<sup>113</sup>; in diesen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person<sup>114</sup>, z. B. durch Verwendung pseudonymisierter Daten<sup>115</sup>, oder
  - c) die Erhebung oder Weitergabe durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt und die angemessene Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist<sup>116</sup> oder
  - d) die Daten aus öffentlich zugänglichen Quellen stammen<sup>117</sup> oder

---

<sup>112</sup> Text proposed by the Statistics Working Party in 10428/12, supported by FR, PL and UK. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into.

<sup>113</sup> COM scrutiny reservation.

<sup>114</sup> Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.

<sup>115</sup> BE, FR and IT reservation on the mentioning of pseudonymous data.

<sup>116</sup> UK thought the requirement of a legal obligation was enough and no further appropriate measures should be required.

<sup>117</sup> COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.

- e) die Daten gemäß einer Bestimmung im Unions- oder im einzelstaatlichen Recht oder aufgrund der vorrangigen berechtigten Interessen einer anderen Person vertraulich behandelt werden müssen<sup>118</sup>.
5. (...)
6. (...)

*Artikel 15*

***Auskunftsrecht der betroffenen Person***<sup>119</sup>

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen in angemessenen Abständen unentgeltlich<sup>120</sup> (...) 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<sup>121</sup>;
- b) (...)

---

<sup>118</sup> COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.

<sup>119</sup> DE, FI and SE scrutiny reservation. DE, LU and UK expressed concerns on overlaps between Articles 14 and 15.

<sup>120</sup> DE, ES, HU, IT and PL reservation on the possibility to charge a fee. DE, LV and SE thought that free access once a year should be guaranteed.

<sup>121</sup> HU thought the legal basis of the processing should be added.



- c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern <sup>122</sup>;
- d) wenn möglich die geplante <sup>123</sup> Speicherfrist;
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen oder eines Widerspruchsrechts gegen die Verarbeitung dieser Daten;
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...) <sup>124 125</sup>;
- g) wenn die Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten <sup>126</sup>;
- h) im Fall von Entscheidungen gemäß Artikel 20 Kenntnis der einer automatischen Datenverarbeitung inhärenten Logik <sup>127</sup> sowie der Tragweite der Verarbeitung und der mit ihr angestrebten Auswirkungen <sup>128</sup>.

---

<sup>122</sup> UK reservation on the reference to recipients in third countries. IT thought the concept of recipient should be clarified, inter alia by clearly excluding employees of the controller.

<sup>123</sup> ES and UK proposed adding 'where possible'; FR reservation on 'where possible' and 'envisaged'; FR emphasised the need of providing an exception to archives.

<sup>124</sup> DE thought it was too onerous to repeat this for every data subject and pointed to difficulties in ascertaining the competent DPA in its federal structure.

<sup>125</sup> IT suggestion to delete subparagraphs (e) and (f) as under Article 14 this information should already be communicated to the data subject at the moment of the collection of the data.

<sup>126</sup> SK scrutiny reservation: subparagraph (g) should be clarified.

<sup>127</sup> PL reservation on the reference to 'logic': the underlying algorithm should not be disclosed. DE reservation on reference to decisions.

<sup>128</sup> NL scrutiny reservation. CZ and FR likewise harboured doubts on its exact scope.

- 1a. Werden personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt, hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 42 im Zusammenhang mit der Übermittlung unterrichtet<sup>129</sup> zu werden<sup>130</sup>.
- 1b. Auf Antrag stellt der für die Verarbeitung Verantwortliche der betroffenen Person, ohne eine überhöhte Gebühr zu verlangen, eine Kopie der Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.
2. Werden von der betroffenen Person bereitgestellte personenbezogene Daten mit automatischen Mitteln und in einem strukturierten gängigen Format verarbeitet, stellt der für die Verarbeitung Verantwortliche der betroffenen Person auf Antrag und ohne eine überhöhte Gebühr zu verlangen<sup>131</sup> eine Kopie der betreffenden Daten in diesem Format zur Verfügung<sup>132</sup>.

---

<sup>129</sup> Further to CZ, ES and PL suggestion.

<sup>130</sup> FR and UK scrutiny reservation on links with Chapter V

<sup>131</sup> Further to ES suggestion.

<sup>132</sup> COM, ES and FR reservation: they thought this was too narrowly drafted. DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy. DE scrutiny reservation on relation to paragraph 1.

- 2a. Der Anspruch auf eine Kopie gemäß den Absätzen 1b und 2 besteht nicht, wenn eine solche nicht zur Verfügung gestellt werden kann, ohne personenbezogene Daten Dritter offenzulegen <sup>133</sup>.
3. (...)
4. (...)
5. [Die nach diesem Artikel gewährten Rechte finden keine Anwendung, wenn Daten zu rein historischen, statistischen oder wissenschaftlichen Zwecken verarbeitet werden und wenn die Bedingungen gemäß Artikel 83 Absatz 1a erfüllt sind] <sup>134</sup>.

---

<sup>133</sup> DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.

<sup>134</sup> Text proposed by the Statistics Working Party in 10428/12. Supported by BE, CZ, FR and NL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into. BE suggested adding ' and the right of access is likely to render impossible or to seriously impair the achievement of such purposes '.

## ABSCHNITT 3

### BERICHTIGUNG UND LÖSCHUNG

#### *Artikel 16*

#### ***Recht auf Berichtigung***<sup>135</sup>

1. Die betroffene Person hat das Recht <sup>136</sup>, von dem für die Verarbeitung ihrer Daten Verantwortlichen die Berichtigung unzutreffender Daten 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. [Die nach diesem Artikel gewährten Rechte finden keine Anwendung, wenn Daten zu rein historischen, statistischen oder wissenschaftlichen Zwecken verarbeitet werden und wenn die Bedingungen gemäß Artikel 83 Absatz 1a erfüllt sind]<sup>137</sup>.

---

<sup>135</sup> DE and UK scrutiny reservation.

<sup>136</sup> UK suggested to insert the qualification 'where reasonably practicable' UK also suggested inserting the qualification 'where necessary'.

<sup>137</sup> Text proposed by the Statistics Working Party in 10428/12. Supported by BE, FR and NL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will be looked into. BE, supported by PT, suggested adding 'and the right of access is likely to render impossible or to seriously impair the achievement of such purposes'

Artikel 17

**Recht auf Vergessenwerden und auf Löschung**<sup>138</sup>

1. (...) Der für die Verarbeitung Verantwortliche<sup>139</sup> ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, und die betroffene Person hat das Recht, die unverzügliche Löschung personenbezogener Daten zu verlangen, sofern einer der folgenden Gründe zutrifft:

<sup>138</sup> DE, EE, PT, SE, SI, FI and UK scrutiny reservation. EE, FR, NL, RO and SE reservation on the applicability to the public sector. Whereas some Member States have welcomed the proposal to introduce a right to be forgotten (AT, EE, FR, IE); other delegations were more sceptical as to the feasibility of introducing a right which would go beyond the right to obtain from the controller the erasure of one's own personal data ( DE, DK, ES). The difficulties flowing from the household exception (UK), to apply such right to personal data posted on social media were highlighted (BE, DE, FR), but also the impossibility to apply such right to 'paper/offline' data was stressed (EE, LU, SI). Some delegations (DE, ES) also pointed to the possible externalities of such right when applied with fraudulent intent (e.g. when applying it to the financial sector). Several delegations referred to the challenge to make data subjects active in an online environment behave responsibly (DE, LU and UK) and queried whether the creation of such a right would not be counterproductive to the realisation of this challenge, by creating unreasonable expectations as to the possibilities of erasing data (DK, LU and UK). Some delegations thought that the right to be forgotten was rather an element of the right to privacy than part of data protection and should be balanced against the right to remember and access to information sources as part of the freedom of expression (DE, ES, LU, NL, SI, PT and UK). It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LV, LU, NL, SE and SI).

<sup>139</sup> DE pointed to the difficulties in determining who is the controller in respect of data who are copied/made available by other controllers (e.g. a search engine) than the initial controller (e.g. a newspaper). AT opined that the exercise of the right to be forgotten would have take place in a gradual approach, first against the initial controller and subsequently against the 'secondary' controllers. ES referred to the problem of initial controllers that have disappeared and thought that in such cases the right to be forgotten could immediately be exercised against the 'secondary controllers' ES suggested adding in paragraph 2: ' Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof'. The Commission, however, replied that the right to be forgotten could not be exercised against journals exercising freedom of expression. According to the Commission, the indexation of personal data by search engines is a processing activity not protected by the freedom of expression.

- 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 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 <sup>140</sup>.
- e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt <sup>141</sup>.

2. (...).

---

<sup>140</sup> UK scrutiny reservation: this was overly broad.

<sup>141</sup> RO scrutiny reservation.

2a. *Hat der (...) für die Verarbeitung Verantwortliche<sup>142</sup> die personenbezogenen Daten öffentlich gemacht<sup>143</sup> und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so unternimmt er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten<sup>144</sup> (...) vertretbare Schritte<sup>145</sup>, auch technischer Art, um andere Verantwortliche<sup>146</sup>, 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<sup>147</sup>.*

---

<sup>142</sup> BE, DE and SI queried whether this also covered controllers (e.g. a search engine) other than the initial controller (e.g. a newspaper).

<sup>143</sup> ES prefers referring to 'expressly or tacitly allowing third parties access to'. IE thought it would be more realistic to oblige controllers to erase personal data which are under their control, or reasonably accessible to them in the ordinary course of business, i.e. within the control of those with whom they have contractual and business relations. BE, supported by IE and LU, also remarked that the E-Commerce Directive should be taken into account (e.g. through a reference in a recital) and asked whether this proposed liability did not violate the exemption for information society services provided in that Directive (Article 12 of Directive 2000/31/EC of 8 June 2000), but COM replied there was no contradiction. LU pointed to a risk of obliging controllers in an online context to monitor all data traffic, which would be contrary to the principle of data minimization and in breach with the prohibition in Article 15 of the E-Commerce Directive to monitor transmitted information.

<sup>144</sup> Further to NL suggestion. The Presidency hopes this can also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;

<sup>145</sup> LU queried why the reference to all reasonable steps had not been inserted in paragraph 1 as well and SE, supported by DK, suggested clarifying it in a recital. COM replied that paragraph 1 expressed a results obligation whereas paragraph 2 was only an obligation to use one's best efforts. ES thought the term should rather be 'proportionate steps'. DE, ES and BG questioned the scope of this term. ES queried whether there was a duty on controllers to act proactively with a view to possible exercise of the right to be forgotten. DE warned against the 'chilling effect' such obligation might have on the exercise of the freedom of expression.

<sup>146</sup> BE, supported by ES and FR, suggested referring to 'known' controllers (or third parties).

<sup>147</sup> BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule.

3. Die Absätze 1 und 2a gelten nicht <sup>148</sup>, soweit (...) die Verarbeitung der personenbezogenen Daten erforderlich ist
- a. zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80<sup>149</sup>;
  - b. *zur Erfüllung einer rechtlichen Verpflichtung zur Verarbeitung der personenbezogenen Daten nach Unions- oder einzelstaatlichem Recht, dem der für die Verarbeitung Verantwortliche unterliegt* <sup>150</sup>, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde <sup>151</sup>;
  - c. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81 <sup>152</sup>;

---

<sup>148</sup> DE queried whether these exceptions also applied to the abstention from further dissemination of personal data. AT and DE pointed out that Article 6 contained an absolute obligation to erase data in the cases listed in that article and considered that it was therefore illogical to provide for exception in this paragraph.

<sup>149</sup> DE and EE asked why this exception had not been extended to individuals using their own freedom of expression (e.g. an individual blogger).

<sup>150</sup> In general DE thought it was a strange legal construct to lay down exceptions to EU obligations by reference to national law. DK and SI were also critical in this regard. UK thought there should be an exception for creditworthiness and credit scoring, which is needed to facilitate responsible lending, as well as for judicial proceedings. IT suggested inserting a reference to Article 21 (1).

<sup>151</sup> AT scrutiny reservation.

<sup>152</sup> DK queried whether this exception implied that a doctor could refuse to erase a patient's personal data notwithstanding an explicit request to that end from the latter. ES and DE indicated that this related to the more general question of how to resolve differences of view between the data subject and the data controller, especially in cases where the interests of third parties were at stake. PL asked what was the relation to Article 21.



- d. für historische, statistische und wissenschaftliche Zwecke (...) gemäß Artikel 83;
  - e. (...)
  - f. (...)
  - g. zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche.
- 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 <sup>153</sup>;
  - b) der für die Verarbeitung Verantwortliche die Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche 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.

---

<sup>153</sup> FR scrutiny reservation: FR thought the cases in which this could apply, should be specified.

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 rechtlicher Ansprüche oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden <sup>154</sup>.
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 <sup>155</sup>.
5. (...)
- 5a. [Die nach diesem Artikel gewährten Rechte finden keine Anwendung, wenn Daten zu rein historischen, statistischen oder wissenschaftlichen Zwecken verarbeitet werden und wenn die Bedingungen gemäß Artikel 83 Absatz 1a erfüllt sind] <sup>156</sup>.

---

<sup>154</sup> DE , ES and SI asked who was to define the concept of public interest. DE reservation.

<sup>155</sup> DE, PT, SI and IT thought that this paragraph should be a general obligation regarding processing, not limited to the exercise of the right to be forgotten. DK likewise thought the first sentence should be moved to Article 22.

<sup>156</sup> Text proposed by the Statistics Working Party in 10428/12. Supported by ES and PL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will be looked into. BE suggested adding ' and the right of access is likely to render impossible or to seriously impair the achievement of such purposes '

*Artikel 17b*

**Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder  
Einschränkung**<sup>157</sup>

Der für die Verarbeitung Verantwortliche teilt allen Empfängern<sup>158</sup>, an die Daten weitergegeben wurden, jede Berichtigung und Löschung sowie jede Einschränkung der Verarbeitung von Daten mit, die aufgrund von Artikel 16, Artikel 17 Absatz 1 bzw. Artikel 17a vorgenommen wird, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

---

<sup>157</sup> Whilst several delegations agreed with this proposed draft and were of the opinion that it added nothing new to the existing obligations under the 1995 Directive, some delegations (DE, PL, SK and NL) pointed to the possibly far-reaching impact in view of the data multiplication since 1995, which made it necessary to clearly specify the exact obligations flowing from this proposed article. Thus, DE was opposed to a general obligation to log all the disclosures to recipients. DE also pointed out that the obligation should exclude cases where legitimate interests of the data subject would be harmed by a further communication to the recipients, that is not the case if the recipient would for the first time learn negative information about the data subject in which he has no justified interest. BE and ES asked that the concept of a 'disproportionate effort' be clarified in a recital.

<sup>158</sup> BE, supported by ES and FR, suggested referring to 'known' recipients.

Artikel 18

**Recht auf Datenübertragbarkeit**<sup>159</sup>

1. (...)
2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und erfolgt die Verarbeitung – auf Basis einer Einwilligung oder eines Vertrags – mittels eines automatisierten Verarbeitungssystems<sup>160</sup>, das durch einen Dienst der Informationsgesellschaft betrieben wird<sup>161</sup>, so hat die betroffene Person das Recht, diese Daten (...) in einer Form zurückzuziehen, die ihr eine Überführung der Daten auf ein anderes automatisiertes Verarbeitungssystem erlaubt, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.
- 2a. Das Recht gemäß Absatz 2 lässt die Rechte an geistigem Eigentum unberührt.

---

<sup>159</sup> UK reservation: while it supports the concept of data portability in principle, the UK considers it not within scope of data protection, but in consumer or competition law. Several other delegations (DK, DE, FR, IE, NL, PL and SE) also wondered whether this was not rather a rule of competition law and/or intellectual property law or how it related to these fields of law. Therefore the UK thinks this article should be deleted. DE, DK and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to/raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, SE and UK pointed to the considerable administrative burdens this article would imply. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger on-going research or the continuity of the service. Reference was also made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK). ES, FR and IE were broadly supportive of this right. SK thought that the article was unenforceable and DE referred to the difficulty/impossibility to apply this right in 'multi-data subject' cases where a single 'copy' would contain data from several data subjects, who might not necessarily agree or even be known or could not be contacted.

<sup>160</sup> DE, IT and SI scrutiny reservation; there is no definition of an 'automated processing system', which could cover almost anything.

<sup>161</sup> COM scrutiny reservation.

- [3. Die Kommission kann (...) die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten gemäß Absatz 2 festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.] <sup>162</sup>
4. [Die nach diesem Artikel gewährten Rechte finden keine Anwendung, wenn Daten zu rein historischen, statistischen oder wissenschaftlichen Zwecken verarbeitet werden und wenn die Bedingungen gemäß Artikel 83 Absatz 1a erfüllt sind.] <sup>163</sup>

---

<sup>162</sup> FR, HU, SE and UK reservation: this would better set out in the Regulation itself.

<sup>163</sup> Text proposed by the Statistics Working Party in 10428/12. Supported by BE, FR, NL and UK. At a later stage, the Commission will look into the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83.

## ABSCHNITT 4

### WIDERSPRUCHSRECHT UND PROFILING

#### *Artikel 19*

#### ***Widerspruchsrecht*** <sup>164</sup>

1. Die betroffene Person hat das Recht, aus stichhaltigen <sup>165</sup> Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstabe f (...) <sup>166</sup> erfolgt, Widerspruch einzulegen; es erfolgt keine Verarbeitung dieser Daten mehr, sofern der für die Verarbeitung Verantwortliche nicht (...) schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder (...) Rechte und (...) Freiheiten der betroffenen Person überwiegen <sup>167</sup>.

---

<sup>164</sup> DE, ES, EE, AT, SI, SK and UK scrutiny reservation.

<sup>165</sup> COM reservation.

<sup>166</sup> The reference to point (e) of Article 6(1) was deleted in view of the objections by BE, CZ, DE, DK, FR and HU. COM reservation on deletion. UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. ES and LU queried why Article 6(1) (c) was not listed here.

<sup>167</sup> SE scrutiny reservation: SE and NL queried the need to put the burden of proof on the controller regarding the existence of compelling legitimate grounds. DE and FI queried the need for new criteria, other than those from the 1995 Directive. COM stressed that the link with the 'particular situation' was made in order to avoid whimsical objections. CZ also stated that this risked making processing of data an exceptional situation due to the heavy burden of proof. NL and SE queried whether the right would also allow objecting to any processing by third parties.

- 1a. Im Falle eines Widerspruchs gemäß Absatz 1 (...) darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht weiter (...) verarbeiten <sup>168</sup>, außer zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche <sup>169</sup>.
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung <sup>170</sup> zu betreiben, hat die betroffene Person das Recht, dagegen (...) <sup>171</sup> jederzeit Widerspruch einzulegen. Die betroffene Person muss ausdrücklich (...) auf dieses Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen <sup>172</sup>.

---

<sup>168</sup> ES proposed to reformulate the last part of this paragraph as follows: 'shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise shall no longer use or otherwise process the personal data concerned'.

<sup>169</sup> UK proposed adding ' for demonstrating compliance with the obligations imposed under this instrument'. This might also cover the concern raised by DE that a controller should still be able to process data for the execution of a contract if the data were obtained further to a contractual legal basis. CZ, DK, EE, IT, SE and UK have likewise emphasised the need for allowing to demonstrate compliance. CZ and SK also referred to the possibility of further processing on other grounds.

<sup>170</sup> FR and UK under lined the need to have clarity regarding the exact content of this concept, possibly through a definition of direct marketing. DE asked which cases were covered exactly.

<sup>171</sup> The reference to 'free of charge' was deleted as this already follows from Article 12(4).

<sup>172</sup> At the request of several delegations (FR, LT, PT), COM confirmed that this paragraph was not meant to create an opt-in system and that the E-Privacy Directive would remain unaffected. DE feels there is a need to clarify the relationship between Article 19(2) on the one hand and Article 6(1)(f) and Article 6(4) on the other. It can be concluded from the right to object that direct marketing without consent is possible on the basis of a weighing of interests. On the other hand, Article 6(1)(f) no longer refers to the interests of third parties and Article 6(4) also no longer refers to Article 6(1)(f) in regard to data processing which changes the original purpose. DE is therefore of the opinion that this also needs to be clarified in view of online advertising and Directive 2002/58/EC and Article 89 of the Proposal for a Regulation.

- 2a. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so erfolgt keine Verarbeitung der personenbezogenen Daten für diese Zwecke mehr.
3. (...)
4. [Die nach diesem Artikel gewährten Rechte finden keine Anwendung auf personenbezogene Daten, die zu rein historischen, statistischen oder wissenschaftlichen Zwecken verarbeitet werden, wenn die Bedingungen gemäß Artikel 83 Absatz 1a erfüllt sind<sup>173</sup>].

---

<sup>173</sup> Text proposed by the Statistics Working Party in 10428/12. Supported by FR, and DK PL was opposed to this exception. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into.



*Artikel 20*  
***Profiling***<sup>174</sup>

1. Jede betroffene Person hat das Recht, nicht einer allein auf Profiling basierenden Entscheidung unterworfen zu werden, *die ihr gegenüber rechtliche Wirkung entfaltet* oder sie erheblich beeinträchtigt<sup>175</sup>, sofern die Verarbeitung der Daten nicht
  - a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen vorgenommen wird (...) und geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, beispielsweise durch deren Recht auf direkten persönlichen Kontakt zu dem für die Verarbeitung Verantwortlichen, auf Äußerung ihres Standpunkts und auf Anfechtung der Entscheidung<sup>176</sup> oder

---

<sup>174</sup> DE, ES, FR, AT, PL, SE and UK scrutiny reservation. COM reservation: COM is of the opinion that that the level of data protection in the current draft of this article is below that of Directive 95/46. DE thinks this provision must take account of two aspects, namely, whether and under what conditions a profile (= the linking of data which permits statements to be made about a data subject's personality) may be created and further processed, and, secondly, under what conditions a purely automated measure based on that profile is permissible if the measure is to the particular disadvantage of the data subject. It appears expedient to include two different rules in this regard. According to DE Article 20 only covers the second aspect and DE would like to see a rule included on profiling in regard to procedures for calculating the probability of specific behaviour (cf. Article 28b of the German Federal Data Protection Act, which requires that a scientifically recognized mathematical/statistical procedure be used which is demonstrably essential as regards the probability of the specific behaviour).

<sup>175</sup> DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there are also cases of automated data processing which actually were aimed at increasing the level of data protection (e.g. in case of children that are automatically excluded from certain advertising).

<sup>176</sup> NL had proposed to use the wording 'and arrangements allowing him to put his point of view, inspired by Article 15 of Directive 95/46. BE suggested adding this for each case referred in paragraph 2.

- b) (...) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt, gestattet ist und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person enthalten oder
- c) mit ausdrücklicher Einwilligung der betroffenen Person (...) erfolgt.
2. (...)
3. Profiling (...) darf sich nicht auf die in Artikel 9 Absatz 1 genannten besonderen Kategorien personenbezogener Daten stützen, sofern nicht Artikel 9 Absatz 2 gilt und geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person getroffen wurden<sup>177</sup>.
4. (...)
5. (...)

---

<sup>177</sup> BE, FR, IT, PL, PT, AT, SE and UK reservation FR and AT reservation on the compatibility with the E-Privacy Directive. BE would prefer to reinstate the term 'solely based', but FR and DE had previously pointed out that 'not ... solely' could empty this prohibition of its meaning by allowing sensitive data to be profiled together with other non-sensitive personal data. DE would prefer to insert a reference to a the use of pseudonymous data.

## ABSCHNITT 5 BESCHRÄNKUNGEN

### *Artikel 21*

#### **Beschränkungen**<sup>178</sup>

1. Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung der Daten Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß Artikel 5 Buchstaben a bis e<sup>179</sup> und Artikel 12 bis 20 sowie Artikel 32 beschränkt werden, sofern eine solche Beschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist<sup>180</sup>

---

<sup>178</sup> SI and UK scrutiny reservation. SE and UK wondered why paragraph 2 of Article 13 of the 1995 Data Protection Directive had not been copied here. IT and NL also referred to the importance of having the possibility to provide derogations for statistical purposes. DE, supported by DK, HU, RO, PT and SI, stated that para. 1 should not only permit restrictions of the rights of data subjects but also their extension. For example, Article 20(2)(b) requires that Member States lay down 'suitable measures to safeguard the data subject's legitimate interests', which, when they take on the form of extended rights of access to information as provided for under German law in the case of profiling to assess creditworthiness (credit scoring), go beyond the Proposal for a Regulation. With an eye to Article 6(3), the Member States also need flexibility especially in the public sector or in the health sector when it comes to laying down and framing specific rules (esp. in regard to earmarking, the nature of the data and the recipient) and enacting stricter rules. DE and EE thought the derogations should distinguish between the private and the public sector.

<sup>179</sup> BE, DE, HU, FI, FR, LU, AT and PL thought that the reference to Article 5 should be deleted, as the principles of Article 5 should never be derogated from. IE and UK opposed this; with IE citing the example of 'unfair' data collection by insurance companies which might be necessary to rebut false damage claims. UK asked for clarification as to why Articles 6-10 are not covered by the exemption.

<sup>180</sup> PL deemed such list not appropriate in the context of a Regulation. IT remarked that this demonstrated the impossibility of full harmonisation. GR and LU thought that it needed to be ensured that the exceptions would be interpreted and applied in a restrictive manner.

- aa) zum Schutz der nationalen Sicherheit;
- ab) zur Landesverteidigung;
- a) zum Schutz der öffentlichen Sicherheit;
- b) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten und in diesem Zusammenhang zur Aufrechterhaltung der öffentlichen Ordnung oder zur Vollstreckung strafrechtlicher Sanktionen;
- c) zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats <sup>181</sup>, insbesondere eines wichtigen <sup>182</sup> wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa <sup>183</sup> im Währungs-, Haushalts- und Steuerbereich, und zum Schutz der Marktstabilität und Marktintegrität;
- 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 a, b, c und d genannten Zwecke verbunden sind;
- f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

---

<sup>181</sup> DE, IT, LT scrutiny reservation as to the broad character of this exemption. SE thought it should be moved to a separate subparagraph.

<sup>182</sup> DK and UK scrutiny reservation on the adjective 'important'.

<sup>183</sup> BE and FR suggested adding 'public health' and 'social security'. The Commission's argued that 'public health' was already covered by point (f).

2. Jede Legislativmaßnahme im Sinne des Absatzes 1 muss 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 sowie den geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung und der Risiken für die Rechte und Freiheiten der betroffenen Personen enthalten.

**KAPITEL IV**

**FÜR DIE VERARBEITUNG VERANTWORTLICHER UND  
AUFTRAGSVERARBEITER <sup>184</sup>**

**ABSCHNITT 1**

**ALLGEMEINE PFLICHTEN**

*Artikel 22*

**Pflichten des für die Verarbeitung Verantwortlichen <sup>185</sup>**

1. Der für die Verarbeitung Verantwortliche stellt unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung und der Risiken für die Rechte und Freiheiten der betroffenen Personen <sup>186</sup> durch geeignete (...) Maßnahmen sicher und kann den Nachweis dafür erbringen, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden <sup>187</sup>.

---

<sup>184</sup> DK, PT, SI and UK scrutiny reservation on the entire chapter. BE stated that it was of the opinion that the proposed rules, while doing away with the general notification obligation on controllers, did not reduce the overall administrative burden/compliance costs for controllers. The Commission disagreed with this. DE, DK, NL, PT and UK were not convinced by the figures provided by COM according to which the reduction of administrative burdens outbalanced any additional burdens flowing from the proposed Regulation. FR referred to the impact this article should have on members of the professions (*professions libérales*) who collect sensitive data as part of their work (e.g. health professionals)

<sup>185</sup> DE scrutiny reservation. UK thought this Article could be deleted as it overlaps with existing obligations. UK thought it focuses too much on procedures rather than on outcomes. DE, LT and PT deplored that Article 22 does not contain an exception for SMEs. BE remarked that anyone who puts a photo on social media might be considered as a controller. SK proposed introducing a new concept of 'entitled person' in Article 4, together with obligations for the controller and processor to instruct their 'entitled persons' who come into contact with personal data about rights and obligations under this regulation as well as laying down responsibility for their infringement.

<sup>186</sup> Several delegations stressed that the risk concept should be further detailed: DE, ES, HU, NL, PT, FI and RO. DE, ES and SE pointed out a description or definition of low risk was missing.

<sup>187</sup> BE and UK referred to the danger in maintaining such a vaguely worded obligation, applicable to all controllers, non-compliance of which is liable to sanctions.

2. (...) <sup>188</sup>
- 2a. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht <sup>189</sup>, beinhalten die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den für die Verarbeitung Verantwortlichen <sup>190</sup>.
- 2b. Der für die Verarbeitung Verantwortliche kann den Nachweis für die Erfüllung seiner Pflichten durch die Einhaltung von Verhaltenskodizes gemäß Artikel 38 oder ein Zertifizierungsverfahren gemäß Artikel 39 erbringen <sup>191</sup>.
3. (...)
4. (...)

---

<sup>188</sup> PL asked for the reinstatement of this paragraph.

<sup>189</sup> HU and PL thought this wording allowed too much leeway to controllers. AT thought that in particular for the respects to time limits and the reference to the proportionality was problematic.

<sup>190</sup> UK thought this was too complicated. ES thought the concept of 'appropriate data protection policies' was too vague.

<sup>191</sup> Reference to auditors deleted in view of the remarks made by CZ, ES and IT.

Artikel 23

**Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen** <sup>192</sup>

1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten sowie der Risiken, die aufgrund der Art, des Umfangs und des Zwecks der Verarbeitung für die Rechte und Freiheiten der betroffenen Personen bestehen, der Verarbeitungstätigkeit und ihren Zielen angemessene technische und organisatorische Maßnahmen – einschließlich der Verwendung pseudonymisierter Daten – durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und dass die Rechte der betroffenen Personen gewahrt werden. <sup>193</sup>
  
2. Der für die Verarbeitung Verantwortliche wendet geeignete Maßnahmen an, die sicherstellen, dass durch Voreinstellung grundsätzlich nur (...) personenbezogene Daten verarbeitet werden, die gemessen an den spezifischen Zwecken der Verarbeitung (...) nicht unverhältnismäßig <sup>194</sup> sind; (...) dies gilt für den Umfang der erhobenen Daten, 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 <sup>195</sup>.

---

<sup>192</sup> DE scrutiny reservation; UK reservation: UK thought this should not be set out in the Regulation. FR scrutiny reservation: FR and LT sought clarification on the scope of the data protection by design and by default and on why the processor was not included. DE and MT thought that more emphasis should be put on pseudonymising and anonymising data. DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. It also thought data protection by design and by default should be more used in response to risky data processing operations. ES thought that the term 'non-excessive data processing' was preferable to 'data protection by design'. FR also queried the exact meaning of the terms used in the title.

<sup>193</sup> NL stated this paragraph added little in terms of legal obligations compared to other articles in the draft regulation. It might be moved to a recital.

<sup>194</sup> ES proposed to replace 'necessary' by 'not excessive in quantity'.

<sup>195</sup> DE, IT and SE reservation; DE and UK queried the exact meaning of the last sentence for social media. SE thought this would be better moved to the recitals. BE and FR asked what this added to the principle of data minimisation contained in Article 5. AT thought the second sentence should be retained.



- 2a. Der für die Verarbeitung Verantwortliche kann die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen mittels eines Zertifizierungsverfahrens gemäß Artikel 39 nachweisen.
3. (...)
4. (...)

*Artikel 24*

***Gemeinsam für die Verarbeitung Verantwortliche*** <sup>196</sup>

1. (...) Gemeinsam für die Verarbeitung Verantwortliche 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, <sup>197</sup> 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.

<sup>196</sup> EE scrutiny reservation. SI and UK reservation: UK thought this provision should be deleted. UK and ES thought this article does not take sufficiently account of cloud computing. CZ, DE and NL expressed grave doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings. CZ and DE thought this article should contain a safeguard against outsourcing of responsibility. FR thought the allocation of liability between the controller and the processor is very vague. DE and LT emphasised that it would be in the interest of the data subject to have clear rules and thought the article should therefore be clarified. Other delegations (DK, EE, SE, SI and UK) warned against potential legal conflicts on the allocation of the liability. SE thought that the allocating respective liability between public authorities should be done by legislation. SI scrutiny reservation.

<sup>197</sup> BE proposed adding: 'The arrangement shall duly reflect the joint controllers' respective effective roles vis-à-vis data subjects. The arrangement shall designate the supervisory authority in accordance with Article 51. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.' ES suggested adding ' For this agreement to be valid in relation to data subjects, it must be documented and must have been brought to their attention beforehand; otherwise, the aforementioned rights may be exercised in full before any of the controllers, and it shall be incumbent on them to ensure precise compliance with the legally established benefits.' SK also pleaded in favour of informing data subjects of any arrangements between several controllers.

2. Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen der vorliegenden Verordnung bei und gegenüber jedem einzelnen der für die Verarbeitung Verantwortlichen<sup>198</sup> geltend machen, sofern sie nicht in transparenter Form darüber informiert worden ist, welcher der gemeinsam Verantwortlichen zuständig ist.

*Artikel 25*

***Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen<sup>199</sup>***

1. In den Fällen gemäß Artikel 3 Absatz 2 benennt der für die Verarbeitung Verantwortliche schriftlich einen Vertreter in der Union<sup>200</sup>.
2. Diese Pflicht gilt nicht für

---

<sup>198</sup> DE, FR and LT emphasised that it would be in the interest of the data subject to have clear rules which allow it to address its requests to all controllers concerned. Potential language problems in case of controllers established in different Member States were also highlighted. ES indicated that such arrangements can never be to the detriment of the data subject's rights and its proposal for paragraph 2 seeks to take account of the concerns.

<sup>199</sup> DE, GR and UK scrutiny reservation. Several delegations (DE, NL, SE) expressed doubts as to whether the tool of obliging controllers not established in the EU to appoint representatives was the right one to ensure the application of EU data protection law to the offering of services and goods in the EU, in view, inter alia, of the low success of this tool under the 1995 data protection directive. CZ and UK also questioned the enforceability of this provision and thought it should be considered alongside Article 3(2). BE, DE FR, IT, PL and UK argued that, if such obligation were to be imposed, the Regulation, Article 79(6)(f) of which provides a mandatory fine for failure to appoint a representative, should clearly allocate duties and tasks to the representative. Reference was also made to the lack of clarity regarding possible sanctions in case of non-designation of a representative. FR also thought the representative's contact details should mandatorily be communicated to the DPA and referred specifically to the potentially problematic case of non-EU air carriers which, often in cooperation with EU carriers, offered flights to EU residents and might not have a representative in the Union.

<sup>200</sup> SI reservation.

- a) für die Verarbeitung Verantwortliche, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz im Sinne von Artikel 41 bietet <sup>201</sup>; oder
- b) Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zwecke besondere Risiken für die Rechte und Freiheiten der betroffenen Personen birgt <sup>202</sup>; oder
- c) Behörden oder öffentliche Einrichtungen <sup>203</sup>.
- d) (...) <sup>204</sup>

---

<sup>201</sup> BE, DE, IT, NL, PL and SK reservation: they thought this indent should be deleted. At the request of several delegations, COM confirmed that this indent also covered the Safe Harbour Agreement. It also pointed out that under Article 41(2)(1) of its proposal having effective and enforceable rights was precisely one of the determining elements to be taken into account in the case of an adequacy decision.

<sup>202</sup> BE, DE, ES, FR, FI, GR, IT, LT, LV, PL, PT and SK remarked that the SME-criterion in itself, while being relevant, could not be sufficient to determine the applicability of the obligation to appoint a representative. The risk inherent in data processing operations should be more important and this text proposal seeks to incorporate this element. DE remarked that the proposed criterion itself would exclude 99.8 % of all enterprises in third countries from the scope of this obligation. FR thought that the risk-criterion should be described in a uniform manner throughout the Regulation

<sup>203</sup> SI thought this should be drafted more broadly so as to encompass any body which exercised sovereign governmental powers. LT scrutiny reservation.

<sup>204</sup> DE and SK thought that this scenario was not covered by Article 3(2). There appears to be no more need for this subparagraph now in view of the revised recital 23

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 <sup>205</sup>.
- 3a. Der Vertreter wird durch den für die Verarbeitung Verantwortlichen beauftragt<sup>206</sup>, 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 der vorliegenden 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.

---

<sup>205</sup> DE pointed out that paragraph 3 leaves it entirely up to businesses offering EU-wide internet services where they appoint a representative within the EU; it thought that this should be done in accordance with the rule on supervisory jurisdiction in the cases referred to in Article 3(2). At any rate, the supervisory authority in that Member State in which the representative is appointed should have jurisdiction.

<sup>206</sup> BE proposed to state 'is liable'.

*Artikel 26*  
***Auftragsverarbeiter***<sup>207</sup>

1. (...) <sup>208</sup> Der für die Verarbeitung Verantwortliche arbeitet nur mit Auftragsverarbeitern, die hinreichende Garantien <sup>209</sup> dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt (...) <sup>210 211</sup>
- 1a. Der Nachweis für das Vorliegen hinreichender Garantien gemäß Absatz 1 kann durch die Einhaltung von Verhaltenskodizes gemäß Artikel 38 oder ein Zertifizierungsverfahren gemäß Artikel 39 erbracht werden.

---

<sup>207</sup> CZ reservation: this article should be deleted. Several delegations (DE, EE, FR IT, LU, NL, SI, SK and UK) pointed to the difficulties in distinguishing the roles of controllers and processors, in particular in the context of cloud computing, where the controller often can not exercise (full) control over the way in which the processor handles the data and thought the proposed provision did not reflect the realities of cloud computing. DE thought the provision needed to be re-examined to see to what extent it is applicable to and meaningful for existing and emerging procedures and services in the health sector, in particular the processing of pseudonymised data or data rendered unintelligible and the administration of medical file systems under the patient's control ('Google health', 'health vault').

<sup>208</sup> DE proposed starting the sentence by stating that the controller shall be responsible for ensuring compliance with data protection rules.

<sup>209</sup> DK and FR thought the 'sufficient guarantees' should be detailed.

<sup>210</sup> The latter part of the article was deleted as it added nothing substantial: IE, NL and SE. DE thought it could be put in a separate sentence.

<sup>211</sup> Some delegations thought it should be explicitly stated that the rights of the data subject and the right to compensation for damages must be asserted against the controller

2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags, in dem dessen Inhalt und Geltungsdauer, der Charakter und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen angegeben werden, oder auf der Grundlage eines anderen rechtlichen Akts <sup>212</sup>, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter
- a) die personenbezogenen Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeitet <sup>213</sup>, sofern er nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dies dem für die Verarbeitung Verantwortlichen mit, sofern eine entsprechende Mitteilung nicht rechtlich unzulässig ist;
  - b) (...)
  - c) alle gemäß Artikel 30 erforderlichen Maßnahmen ergreift;
  - d) die Bedingungen für die Inanspruchnahme eines weiteren Auftragsverarbeiters (...) festlegt <sup>214</sup>;
  - e) soweit es angesichts der Art der Verarbeitung (...) möglich ist <sup>215</sup>, den für die Verarbeitung Verantwortlichen dabei unterstützt, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

---

<sup>212</sup> FR wanted to know what was meant by an ‘other legal act’.

<sup>213</sup> DE wondered whether this requirement was feasible in the context of social media.

<sup>214</sup> UK thought this overlapped with other parts of the Regulation (Article 26,(2)(a) and 30). BE thought the requirement should be deleted and DE thought it should at least have been limited to establishment of contractual relationships. AT and SK scrutiny reservation: SK thought there were many questions surrounding the relation with this 'secondary' processor.

<sup>215</sup> FR thought this was unclear and should possibly be replaced by a reference to risk. IT thought different types of risk could be referred to here.

- f) festlegt, in welchem Umfang der für die Verarbeitung Verantwortliche bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten zu unterstützen ist;
- g) die personenbezogenen Daten nach Beendigung der Verarbeitung, die in dem Vertrag oder dem sonstigen rechtlichen Akt angegeben ist, zurückgibt <sup>216</sup>, 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 <sup>217</sup> zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt.
3. Der in Absatz 2 genannte Vertrag ist schriftlich oder in einem elektronischen oder einem anderen ohne technische Vermittlung nicht lesbaren Format, das in ein lesbares Format umgewandelt werden kann, abzufassen.
4. (...)
5. (...) <sup>218</sup>

---

<sup>216</sup> Drafting amended in order to accommodate. FR, ES and NL request that there should be an obligation to return the data.

<sup>217</sup> DE referred to 'the principal's rights of supervision and the contractor's corresponding rights of tolerance and involvement', for instance rights of entry, certified auditor's obligations to report periodically.

<sup>218</sup> COM reservation on deletion.

Artikel 27

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

(...) <sup>219</sup>

Artikel 28

**Aufzeichnungen <sup>220</sup> zu den Kategorien von Vorgängen zur Verarbeitung personenbezogener Daten** <sup>221</sup>

1. Alle für die Verarbeitung Verantwortlichen (...) <sup>222</sup> und gegebenenfalls ihre Vertreter führen eine Aufzeichnung zu allen Kategorien von Vorgängen zur Verarbeitung personenbezogener Daten, die ihrer Zuständigkeit unterliegen <sup>223</sup>.

<sup>224</sup>Diese Aufzeichnung enthält folgende Angaben:

---

<sup>219</sup> ES, FR, SI and UK stated that it is difficult to see what is the added value of this Article as compared to Article 26, §2(b). As for employees of the controller, the latter will always be liable for any data protection violations carried out by the former. All confidentiality duties have now been moved to Article 30.

<sup>220</sup> Further to UK proposal the term 'document' has been replaced by the more technologically neutral term 'record'. PL and SK suggested to specify that the documents/records could be kept 'in paper or electronically', but the Presidency prefers to keep the wording technologically neutral.

<sup>221</sup> AT and SI scrutiny reservation. UK stated that it thought that the administrative burden caused by this Article nullified the benefits if the proposed abolition of the notification obligation. DE, LU, NL and SE shared these concerns.

<sup>222</sup> Several delegations (BE, DE) thought the processor should not have cumulative obligations with the controller. ES and UK pointed out that the impact of cloud computing needed further reflection.

<sup>223</sup> FR thought it should be specified for how long the documentation needed to be kept.

<sup>224</sup> ES proposed to insert a sentence along the following lines: 'Controllers that do not have a data protection officer or sufficient certificate in force, shall have the legally established documentation form with regard to all processing operations carried out under their responsibility'. NL thought the keeping of documentation should be made conditional upon a prior risk assessment: 'Where a data protection impact assessment as provided for in Article 33 indicates the processing operation presents a high degree of risk, referred to in Article 33'. RO is also in favour of a less prescriptive list.



- 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 legitimen Interesses, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet <sup>225</sup>;
  - 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 in ein Drittland oder an eine internationale Organisation (...) <sup>226</sup>;
  - g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien.
  - h) (...)
- 2a. Jeder Auftragsverarbeiter <sup>227</sup> führt eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Vorgängen zur Verarbeitung personenbezogener Daten, die Folgendes enthält:

---

<sup>225</sup> UK suggested deleting it, as it overlaps with Article 6(1)(f).

<sup>226</sup> UK reservation.

<sup>227</sup> UK thinks this article should not apply to processor(s) at all, as all their processing activities are carried out under the responsibility of the controller.

- 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 Verarbeitungsvorgänge, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden;
  - d) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation.
- 3a. Die in den Absätzen 1 und 2a genannten Aufzeichnungen sind schriftlich oder in einem elektronischen oder einem anderen ohne technische Vermittlung nicht lesbaren Format, das in ein lesbares Format umgewandelt werden kann, zu führen.
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 <sup>228</sup>.
4. Die in den Absätzen 1 und 2a genannten Pflichten gelten nicht für:
- a) (...) <sup>229</sup>

---

<sup>228</sup> SI wondered why the data subject was not mentioned here. COM stated this information of the data subject is covered by the general principles. FI proposed to insert an exception in case the controller is subject to a professional secrecy duty, but this is already covered by Article 84 of the regulation.

<sup>229</sup> COM reservation on deletion.

- b) Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zwecke besondere Risiken für die Rechte und Freiheiten der betroffenen Personen birgt <sup>230</sup>; oder
- c) Kategorien von Verarbeitungsvorgängen, die <sup>231</sup> aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zwecke aller Wahrscheinlichkeit nach nicht mit konkreten Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden sind.
5. (...)
6. (...)

*Artikel 29*

***Zusammenarbeit mit der Aufsichtsbehörde***

(...) <sup>232</sup>

---

<sup>230</sup> Many delegations criticised the appropriateness of this criterion: AT, BE, DE, DK, ES, FR, GR, IT, LT, LU, NL, MT, PT, and SE. At the suggestion of BE, the criterion was narrowed in the same way as in Article 25(2)(b).

<sup>231</sup> Proposal inspired by Article 18(2) of the Data Protection Directive, in order to take account of delegations that thought that the proposed exceptions were not well-founded and that risk-based exceptions would be preferable. FR thinks that the risk-based approach cannot lead to exemption of certain types of processing operations

<sup>232</sup> PT and ES scrutiny reservation on deletion.

## ABSCHNITT 2 DATENSICHERHEIT

### *Artikel 30*

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

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter<sup>233</sup> treffen unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten sowie angesichts des Charakters, der Umstände, der Tragweite und der Zwecke der Verarbeitung und der Risiken für die Rechte und Freiheiten der betroffenen Personen technische und organisatorische Maßnahmen, einschließlich der Verwendung pseudonymisierter Daten, die geeignet sind, ein diesen Risiken angemessenes Schutzniveau zu gewährleisten.
2. (...)
- 2a. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können die Erfüllung der in Absatz 1 genannten Anforderungen durch die Einhaltung von Verhaltenskodizes gemäß Artikel 38 oder ein Zertifizierungsverfahren gemäß Artikel 39 nachweisen.

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, sofern sie keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedstaatlichen Recht erwachsenden Pflichten unterliegen.
3. (...)
4. (...)

---

<sup>233</sup> Several delegations thought that the controller should have the main responsibility (NO, NL, RO, UK).

Artikel 31

**Meldung von Verletzungen des Schutzes personenbezogener Daten an die  
Aufsichtsbehörde**<sup>234</sup>

1. Bei einer Verletzung des Schutzes personenbezogener Daten, die eine schwere Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen wahrscheinlich macht<sup>235</sup>, benachrichtigt der für die Verarbeitung Verantwortliche die gemäß Artikel 51 zuständige Aufsichtsbehörde 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<sup>236</sup> nicht erforderlich ist.
2. (...) Der Auftragsverarbeiter alarmiert und informiert den für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung nach Feststellung einer Verletzung des Schutzes personenbezogener Daten<sup>237 238</sup>.

---

<sup>234</sup> AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

<sup>235</sup> BE suggested adding: ‘or creates a risk for the data subjects’.

<sup>236</sup> BE thought that also point (a) of Article 32(3) should be added here.

<sup>237</sup> The Commission highlighted the importance of this obligation, in particular in the context of cloud computing. UK thought this should be moved to Article 26.

<sup>238</sup> DE remarked that in view of the Commission proposal of 7 February 2013 for a Directive concerning measures to ensure a high level of network and information security across the Union (COM(2013) 48 final), it should be checked whether in certain cases the authority competent for network and information security should also be notified.

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 Kategorien und der 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 negativer 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 unangemessene 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 <sup>239</sup>. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. (...).
5. (...)
- [6. Die Kommission kann das Standardformat für derartige Meldungen an die Aufsichtsbehörde, die Verfahrensvorschriften für die vorgeschriebene Meldung sowie Form und Modalitäten der in Absatz 4 genannten Dokumentation einschließlich der Fristen für die Löschung der darin enthaltenen Informationen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen] <sup>240</sup>.

---

<sup>239</sup> AT, LU and FR queried what was the retention period for this documentation. IT proposed to insert a reference to the estimated severity of the remedial action taken.

<sup>240</sup> BE, DE, IT, LT, RO and UK pleaded for the deletion of paragraph 6.

Artikel 32

**Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person** <sup>241</sup>

1. Besteht die Wahrscheinlichkeit, dass (...) durch die Verletzung des Schutzes personenbezogener Daten die Rechte und Freiheiten der betroffenen Person erheblich beeinträchtigt werden <sup>242</sup>, benachrichtigt der für die Verarbeitung Verantwortliche (...) <sup>243</sup> die betroffene Person <sup>244</sup> ohne unangemessene Verzögerung von der Verletzung.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt <sup>245</sup> die Art der Verletzung des Schutzes personenbezogener Daten und umfasst 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

---

<sup>241</sup> AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded. NL thought there should be an exception for statistical data processing. FR thought that the possible application to public/private archives required further scrutiny.

<sup>242</sup> BE and SK scrutiny reservation. BE suggested adding: ‘or creates a risk for the data subjects’.

<sup>243</sup> The Presidency agrees with AT, PT and SE that there is no valid reason why the data subject should always be informed after the DPA. Therefore this part has been deleted. DE however proposed to start this paragraph by stating: ‘As soon as appropriate measures have been taken to render the data secure or where such measures were not taken without undue delay and there is no longer a risk for the criminal prosecution’

<sup>244</sup> PL suggested specifying this could be done either in paper or electronic form.

<sup>245</sup> DE proposed adding “in generally comprehensible terms”, but this is already covered by Article 12.



- a. der für die Verarbeitung Verantwortliche (...) <sup>246</sup> geeignete technische 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 <sup>247</sup>, etwa durch Verschlüsselung oder Verwendung pseudonymisierter Daten <sup>248</sup> <sup>249</sup>; oder
  - b. der für die Verarbeitung Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr erheblich beeinträchtigt werden; 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. (...)

---

<sup>246</sup> NL and FR criticised the subjective criterion of satisfying to the satisfaction of the DPA. More generally, NL opined that there was danger of the data protection authority would obtain company secrets from the data controller which the DPA might be obliged to disclose under access to document legislation.

<sup>247</sup> BE proposed 'have the purpose'.

<sup>248</sup> AT, FR, IT and PT reservation on reference to pseudonymised data. The Presidency has proposed a new recital 68a to accompany this text.

<sup>249</sup> MT and UK thought this exception should also be inserted to Article 31. The Presidency considers that there might be cases where it still might be useful to inform the DPA.

- [6. Die Kommission kann das Format für die in Absatz 1 genannte Benachrichtigung der betroffenen Person und die für die Benachrichtigung geltenden Verfahrensvorschriften festlegen. Die betreffenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen] <sup>250</sup>.

---

<sup>250</sup> BE, CZ, DK, DE, ES, PL and UK pleaded for the deletion of paragraph 6.

### ABSCHNITT 3

## DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE GENEHMIGUNG

#### *Artikel 33*

#### *Datenschutz-Folgenabschätzung*<sup>251</sup>

1. Bei Verarbeitungsvorgängen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zwecke konkrete<sup>252</sup> Risiken für die Rechte und Freiheiten betroffener Personen bergen<sup>253</sup>, führt der für die Verarbeitung Verantwortliche (...) <sup>254</sup> vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. (...) <sup>255</sup>.
2. Konkrete Risiken gemäß Absatz 1 bestehen (...) bei folgenden Verarbeitungsvorgängen:

---

<sup>251</sup> ES, HU and UK scrutiny reservation; FR thought that the possible application to public/private archives required further scrutiny.

<sup>252</sup> ES thought that such assessment should not be required in all cases and wanted to restrict the scope of the Article. ES, FR, LU, PT, RO, SK, SI and UK warned against the considerable administrative burdens flowing from the proposed obligation.

<sup>253</sup> BE scrutiny reservation.

<sup>254</sup> Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deletion.

<sup>255</sup> ES had proposed exempting certified processing operations. BE, CZ, EE and had proposed exempting a controller who had appointed a DPO.

- a) systematische und umfassende Auswertung persönlicher Aspekte natürlicher Personen, (...) die sich auf Profiling gründet und die ihrerseits als Grundlage für Entscheidungen<sup>256</sup> dient, welche Rechtswirkung gegenüber betroffenen Personen entfalten oder erhebliche Auswirkungen für diese mit sich bringen<sup>257</sup>;
- b) Verarbeitung von Daten, aus denen die Rasse oder die ethnische Herkunft, politische Überzeugungen, die Religionszugehörigkeit oder Weltanschauung oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie Verarbeitung von genetischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über Strafurteile und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen, wenn die Daten in großem Umfang im Hinblick auf Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen<sup>258</sup>;
- c) *weiträumige* Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen (...) <sup>259</sup>;

---

<sup>256</sup> BE proposed to replace this by wording similar to that used for profiling in Article 20: 'decision which produces adverse legal effects concerning this natural person or significant adverse effects concerning this natural person'. DE and NL also thought the drafting could be improved.

<sup>257</sup> FR thought profiling measures might need to be covered by this Article, but the Presidency thinks this type of processing is largely covered by paragraph 2(a).

<sup>258</sup> DE proposed referring to 'particularly sensitive personal information, in particular special categories of personal data under Article 9(1), data on children, genetic data or biometric data'. FR and IT are also supportive of the inclusion on sensitive data.

<sup>259</sup> BE, FR, SK and IT asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale'. DE proposed the following text: 'processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where legitimate expectations are not met, for example owing to the context of the processing operation'.

- d) Verarbeitung personenbezogener Daten in umfangreichen Verarbeitungssystemen, die (...) genetische Daten oder biometrische Daten enthalten <sup>260</sup>;
- e) sonstige Verarbeitungsvorgänge, die nach Einschätzung der zuständigen Aufsichtsbehörde konkrete Risiken für die Rechte und Freiheiten der betroffenen Personen bergen <sup>261</sup>.
- 2a. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsarten, für die gemäß Absatz 2 Buchstabe e eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss. <sup>262</sup>
- 2b. Vor Festlegung der Liste wendet die Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 57 an, wenn die Liste, auf die in Absatz 2a Bezug genommen wird, Verarbeitungsvorgänge beinhaltet, die mit dem Angebot von Waren oder Dienstleistungen für Personen in mehreren Mitgliedstaaten oder der Beobachtung des Verhaltens dieser Personen im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten. <sup>263</sup>

---

<sup>260</sup> COM reservation on deletion of reference to children. DE proposed ‘processing operations which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons’.

<sup>261</sup> BE and DE reservation: in favour of deleting this subparagraph. NL and PL thought a role could be given to the EDPB in order to determine high-risk operations.

<sup>262</sup> New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

<sup>263</sup> New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

3. Die Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung; sie enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen <sup>264</sup>, 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 <sup>265</sup>. <sup>266</sup>
4. (...) <sup>267</sup>
5. Falls es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde oder um eine öffentliche Einrichtung <sup>268</sup> handelt und 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, gelten die Absätze 1 bis 3 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen <sup>269</sup>.
6. (...)
7. (...)

---

<sup>264</sup> DE suggests adding ' also in view of Article 30'.

<sup>265</sup> NL proposes to specify this reference and refer to Articles 30, 31, 32 and 35.

<sup>266</sup> DE and FR scrutiny reservation. DE referred to Article 23 (b) of the 2008 Data Protection Framework Decision, which requires prior consultation of the DPA where 'the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.'

<sup>267</sup> The Presidency agrees with those delegations (BE, FR) that indicated that this was a completely impractical obligation. NL and COM were in favour of maintaining it.

<sup>268</sup> BE proposed replacing the criterion of a controller being a public body by 'data are processed for the public interest'.

<sup>269</sup> IT scrutiny reservation. DK, IT and COM think the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

Artikel 34

**Vorherige (...) Konsultation** <sup>270</sup>

1. (...)
2. Der für die Verarbeitung Verantwortliche (...) <sup>271</sup> zieht vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate (...), wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 33 hervorgeht, dass die Verarbeitung hohe konkrete Risiken birgt <sup>272 273</sup>.  
  
(...)

---

<sup>270</sup> ES, HU and UK scrutiny reservation; DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. The Presidency has revised the wording of recital 74 with a view to clarifying the scope of the obligation.

<sup>271</sup> Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deleting processor.

<sup>272</sup> FR and SE scrutiny reservation on the concept of a high degree of specific risks. It was pointed out that such assessments might be time-consuming. IT thought there should be scope for consulting the DPA in other cases as well.

<sup>273</sup> DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

3. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 2 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, unterbreitet sie dem für die Verarbeitung der Daten Verantwortlichen spätestens sechs Wochen nach dem Antrag auf Konsultation geeignete Empfehlungen (...) <sup>274</sup>. Diese Frist kann angesichts der Komplexität der geplanten Verarbeitung um einen weiteren Monat 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 <sup>275</sup>.
4. (...)
5. (...) <sup>276</sup>
6. Der für die Verarbeitung Verantwortliche (...) stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 2 auf Verlangen die Datenschutz-Folgenabschätzung gemäß Artikel 33 sowie alle sonstigen von ihr angeforderten Informationen (...) zur Verfügung. <sup>277</sup>

---

<sup>274</sup> Drafting amended in order to take account of the concern expressed by several delegations that a sanctioning power for DPAs would be difficult to reconcile with (1) the duty on controllers to make prior consultation under the previous paragraph (DE, DK, NL, SE, SI) and (2) the freedom of expression (NL, PL, SI).

<sup>275</sup> ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing. The Presidency thinks that any discussion regarding differentiating the DPA powers should take place under Article 53.

<sup>276</sup> IT reservation on the deletion of paragraphs 4 and 5.

<sup>277</sup> DE thought this paragraph should be deleted.



7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung <sup>278</sup> von Vorschlägen für Rechts- oder Verwaltungsvorschriften zu Rate, die die Verarbeitung personenbezogener Daten vorsehen und die aufgrund der Art, des Umfangs oder der Zwecke der Verarbeitung bestimmte Kategorien von betroffenen Personen erheblich <sup>279</sup> beeinträchtigen können.
- 7a. Unbeschadet 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 <sup>280</sup>.
8. (...)
9. (...)

---

<sup>278</sup> CZ wanted clarification that this obligation does not apply to private member's bills.

<sup>279</sup> COM reservation, in particular regarding regulatory measures: this threshold is not present in the 1995 Directive.

<sup>280</sup> DK, NL, PL, SE scrutiny reservation.

## 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 – <sup>281</sup> einen Datenschutzbeauftragten benennen (...) <sup>282</sup>.
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 Struktur und 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 einschlägigen Verfahrensweisen besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben <sup>283</sup>(...).
6. (...)

---

<sup>281</sup> Made optional further to decision by the Council. DE and AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself. COM reservation on optional nature and deletion of points a) to c). UK thinks paragraphs 5 to 8 could be deleted.

<sup>282</sup> PL suggested adding ‘The controller or the processor may appoint one or more deputy data protection officers. Deputy data protection officer must fulfil conditions stipulated in art. 35 point 5 of this Regulation’

<sup>283</sup> PL suggested adding a reference to the absence of a criminal record as a condition.

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 zu ziehen.
11. (...)

#### *Artikel 36*

#### ***Stellung des Datenschutzbeauftragten*** <sup>284</sup>

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.

---

<sup>284</sup> UK thought articles 36 and 37 could be deleted in a pure risk-based approach.

3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben unabhängig handeln kann<sup>285</sup> und keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. 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<sup>286</sup>.

#### *Artikel 37*

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

1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter betraut den Datenschutzbeauftragten mit (...) folgenden Aufgaben:
  - a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die personenbezogene Daten verarbeiten, über ihre aus dieser Verordnung erwachsenden Pflichten (...);
  - b) Überwachung der Einhaltung dieser Verordnung und der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Aufklärung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

---

<sup>285</sup> DE, EE, ES, LV and NL pointed out that the requirement of independence was not the same for DPOs as for DPAs.

<sup>286</sup> Moved from Article 35 (6). DE was opposed to this as these requirements were irrelevant to the functional independence of the DPO. FR demanded further clarifications. UK also thought this was too prescriptive. Presidency endeavoured to redraft this paragraph in order to make it less prescriptive. AT thought the redraft did not sufficiently take account of the situation of external DPOs.

- c) (...)
- d) (...)
- e) (...)
- f) (...)
- 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<sup>287</sup>.

2. (...)

---

<sup>287</sup> FR suggested adding an obligation to draft an annual report on his activities, but the Presidency wonders whether this is not too heavy an obligation.

## ABSCHNITT 5

### VERHALTENSREGELN UND ZERTIFIZIERUNG <sup>288</sup>

#### *Artikel 38*

#### *Verhaltensregeln* <sup>289 290</sup>

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 Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten <sup>291</sup>, können Verhaltensregeln ausarbeiten oder ändern oder ergänzen, damit die Anwendung von Bestimmungen dieser Richtlinie 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;

---

<sup>288</sup> COM scrutiny reservation on Section 5.

<sup>289</sup> AT, DK, FI, SK and PL scrutiny reservation. DE, FR and SI stated that this article should not apply to the public sector.

<sup>290</sup> Several delegations thought more incentives should be made to apply to the use of codes of conduct: BE, DE, DK, LV, SE, SI, UK. Several delegations thought that hortatory language was being used in §1 (SI, PT), §1c (NL, SI, FR)

<sup>291</sup> LU pleaded in favour of extending this to multinational companies established in various Member states.

- (bb) Verwendung pseudonymisierter Daten <sup>292</sup>;
- 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 Mitteilung solcher Verletzungen an betroffene Personen;
- f) Datenübermittlung in Drittländer oder an internationale Organisationen <sup>293</sup>.

---

<sup>292</sup> FR scrutiny reservation.

<sup>293</sup> NL queried whether this also covered the transfer to processors in 3rd countries.

- 1b. Die Verhaltensregeln enthalten Mechanismen zu ihrer Überwachung und zur Sicherstellung ihrer Einhaltung durch die für die Verarbeitung Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, unbeschadet der Pflichten und Befugnisse der Aufsichtsbehörde, die nach Artikel 51 zuständig ist.
2. Verbände und andere Einrichtungen 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 nimmt <sup>294</sup> zu der Frage Stellung, ob der Entwurf der Verhaltensregeln beziehungsweise die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind.
- 2a. Wird durch die Stellungnahme nach Absatz 2 bestätigt, dass die Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind, und beziehen sich die Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so verzeichnet die Aufsichtsbehörde die Verhaltensregeln und veröffentlicht die Einzelheiten der Verhaltensregeln.
- 2b. Beziehen sich die Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die Aufsichtsbehörde sie nach dem Verfahren gemäß Artikel 57 dem Europäischen Datenschutzausschuss vor, der zu der Frage Stellung nehmen kann, ob der Entwurf der Verhaltensregeln beziehungsweise die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind.
3. Wird durch die Stellungnahme nach Absatz 2b bestätigt, dass die Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind, so übermittelt der Europäische Datenschutzausschuss seine Stellungnahme der Kommission <sup>295</sup> (...).

---

<sup>294</sup> Further to CY, FR, IT, LU, LV and PT suggestion.

<sup>295</sup> DE, IE, ES, PT also remarked that the DPAs should be involved; to that end paragraph 2a has been inserted. EE, ES and UK thought that the Commission need not be involved.



4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln allgemeine Gültigkeit in der Union <sup>296</sup> besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.
5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden <sup>297</sup>.

*Artikel 38a*

**Überwachung (...) der Verhaltensregeln** <sup>298</sup>

1. Unbeschadet der Pflichten und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 38 von einer (...) Stelle durchgeführt werden <sup>299</sup>, die über das geeignete Fachwissen hinsichtlich der Verhaltensregeln verfügt und 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 der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

<sup>296</sup> CZ, EE and FR queried what was the legal status of such approved codes of conduct and in particular their binding nature.

<sup>297</sup> BG suggests deleting paragraph 4; ES suggests deleting paragraphs 4 and 5.

<sup>298</sup> AT, DE, DK, NL, LU, FI, IT, PT and UK scrutiny reservation.

<sup>299</sup> CZ, DK, EE, LV, PT and UK are opposed to giving this role to such separate bodies. Concerns were raised, *inter alia*, on the administrative burden involved in the setting up of such bodies. The Presidency stresses that codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

- b. sie Verfahren aufgestellt 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 aufgestellt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;
- d. sie (...) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
3. Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 57 an den Europäischen Datenschutzausschuss.
4. Unbeschadet der Bestimmungen 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 darüber, aus welchen Gründen sie ergriffen werden.

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 <sup>300</sup>.
6. Dieser Artikel gilt nicht für die Verarbeitung personenbezogener Daten durch Behörden oder öffentliche Einrichtungen.

### *Artikel 39*

### ***Zertifizierung*** <sup>301</sup>

1. Die Mitgliedstaaten, der Europäische Datenschutzausschuss und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und –zeichen, die dazu dienen, nachzuweisen, dass für die Verarbeitung Verantwortliche oder Auftragsverarbeiter diese Verordnung einhalten. Den besonderen Bedürfnissen von Kleinst-, Klein- und mittleren Unternehmen wird Rechnung getragen.

(...)

---

<sup>300</sup> BE proposed adding: 'An infringement of a code of conduct shall not in itself constitute an infringement of this Regulation, unless the Commission has, pursuant to paragraph 4 of Article 38, decided the code has general validity within the European Union.' The Presidency thinks that this proposal should be revisited in the wider context of the discussions on sanctions.

<sup>301</sup> AT, DK, EE, FR, FI , IT , PT and UK scrutiny reservation. ES, SI and UK thought further incentives should be provided for using certification mechanism. FR thought the terminology used was unclear and that the DPA should be in a position to check compliance with certified data protection policies; the Presidency will try to do this in Article 53.

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 Pflichten und Befugnisse der Aufsichtsbehörde, die gemäß Artikel 51 zuständig ist.
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Stelle gemäß Artikel 39a Absatz 1 alle Informationen und den Zugang zu seinen Verarbeitungstätigkeiten, die bzw. der für die Durchführung des Zertifizierungsverfahrens erforderlich sind, zur Verfügung. (...)
4. Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter erteilte Zertifizierung wird von der Stelle gemäß Artikel 39a Absatz 1 oder der zuständigen Aufsichtsbehörde regelmäßig überprüft. Sie wird widerrufen, wenn die Anforderungen der Zertifizierung nicht oder nicht mehr erfüllt sind.

*Artikel 39a*

**Zertifizierungsstelle und -verfahren**<sup>302</sup>

1. Unbeschadet der Pflichten und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 kann die Zertifizierung und deren regelmäßige Überprüfung von einer Zertifizierungsstelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt und von der Aufsichtsbehörde, die gemäß Artikel 51 zuständig ist, akkreditiert wurde.
2. Die Stelle gemäß Absatz 1 kann zu diesem Zweck akkreditiert werden, wenn
  - a. sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

---

<sup>302</sup> AT, DK, EE, FR, IT and PT scrutiny reservation.

- b. sie Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzsiegel und –zeichen aufgestellt hat;
  - c. sie Verfahren und Strukturen aufgestellt 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 Aufsichtsbehörden übermitteln den Entwurf der Kriterien für die Akkreditierung der Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 57 an den Europäischen Datenschutzausschuss.
4. Die Stelle gemäß 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 zugrunde liegt, verantwortlich.
- 4a. Unbeschadet der Bestimmungen des Kapitels VIII kann die Stelle gemäß Absatz 1 vorbehaltlich angemessener Garantien die Zertifizierung widerrufen, wenn die Zertifizierung unsachgemäß verwendet wird oder wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die Anforderungen der Zertifizierung nicht oder nicht mehr erfüllt.
5. Die Stelle gemäß Absatz 1 teilt der zuständigen Aufsichtsbehörde Einzelheiten zu erteilten und widerrufenen Zertifizierungen und die Gründe für den Widerruf einer Zertifizierung mit.
6. Die Aufsichtsbehörde veröffentlicht die Zertifizierungskriterien und die Einzelheiten der Zertifizierung in leicht zugänglicher Form.

- 6a. 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.
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen festzulegen, die für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind [einschließlich der Bedingungen für die Erteilung und den Widerruf der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung und der Anforderungen für ein standardisiertes "Europäisches Datenschutzsiegel" in der Union und in Drittländern].
8. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen <sup>303</sup>.

---

<sup>303</sup> DE pleaded in favour of deleting the last two paragraphs. ES thought that this should not be left exclusively to the Commission.

# KAPITEL V

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN <sup>304</sup>

### *Artikel 40*

#### *Allgemeine Grundsätze der Datenübermittlung* <sup>305</sup>

(...) <sup>306</sup>.

---

<sup>304</sup> FR reservation. In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, CZ, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (EE, FR, PL). FR requested that a grandfather clause be inserted preserving international agreements concluded by Member States.

<sup>305</sup> COM scrutiny reservation, in particular regards onward transfers.

<sup>306</sup> The Presidency agrees with GR, SE, NL and UK that this article has no added value to the rest of the Chapter V and has therefore deleted it., BE, supported by FI and NL, thought that the requirements regarding onward transfer need not be mentioned here, as these were at any rate subsumed under the adequacy requirement. FR thought the requirement of prior originator consent to onward transfer should be expressed in a different manner. ES was opposed to putting the processor and controller on the same footing.

Artikel 41

**Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses** <sup>307</sup>

1. Eine Übermittlung personenbezogener Daten an einen oder mehrere Empfänger in einem Drittland oder einer internationalen Organisation darf vorgenommen werden, wenn die Kommission <sup>308</sup> festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor <sup>309</sup> dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner besonderen <sup>310</sup> Genehmigung.
2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt <sup>311</sup> die Kommission <sup>312</sup><sup>313</sup> insbesondere
  - a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte <sup>314</sup> und Grundfreiheiten, die (...) in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation geltenden Vorschriften, Datenschutzbestimmungen und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland beziehungsweise eine andere internationale Organisation sowie die Existenz wirksamer und durchsetzbarer <sup>315</sup> Rechte der betroffenen Person und wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen (...), deren personenbezogene Daten übermittelt werden <sup>316</sup> <sup>317</sup>;

<sup>307</sup> AT, LU and FR expressed their support for maintaining the adequacy procedure. Some delegations raised concerns on the time taken up by adequacy procedures. LV thought a separate paragraph setting.

<sup>308</sup> CZ and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data. UK had considerable doubts on the feasibility of the list in paragraph 2.

<sup>309</sup> IT, SK and AT scrutiny reservation.

<sup>310</sup> ES proposal.

<sup>311</sup> PL proposal. IT thought the list should not be exhaustive and therefore proposed adding 'in particular'.

<sup>312</sup> NL thought a preponderant role should be given to the EDPB in assessing these elements. COM indicated that this could be done in the articles dealing with the EDPB competences and that at any rate the Member States were involved in the adequacy procedure.

<sup>313</sup> CZ and IT asked for involvement of the EDPB.

<sup>314</sup> GR, AT and SK thought a reference to human rights should be inserted.

<sup>315</sup> ES proposal.

<sup>316</sup> Deleted further to CZ and FI remark that no distinction should be made between EU citizens.

<sup>317</sup> COM scrutiny reservation.



- b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger <sup>318</sup> Aufsichtsbehörden <sup>319</sup> in dem betreffenden Drittland, oder denen eine internationale Organisation untersteht und die für die Einhaltung der Datenschutzvorschriften, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind, und
- c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation <sup>320</sup> in Bezug auf den Schutz personenbezogener Daten eingegangenen internationalen Verpflichtungen <sup>321</sup> <sup>322</sup> ,

---

<sup>318</sup> Further to FDE and BE proposal.

<sup>319</sup> CZ and NL queried how strict this independence would need to be assessed.

<sup>320</sup> CH and NL remarked that many of these elements need to be formulated less broadly. FR thought the criteria should be more focused on implementation.

<sup>321</sup> CZ proposal. COM had clarified that this was mainly the CoE Convention No 108.

<sup>322</sup> DE proposed adding ' participation in a suitable international data protection system established in third countries or a territory or a processing sector' and that the list of checks in Article 42(2) should include a new component consisting of the participation of third States or international organisations in international data-protection systems (e.g. APEC and ECOWAS). It also suggested referring to 'ways of ensuring consistent interpretation and application of the data-protection provisions under Articles 55 et seq'.

3. Nach der Bewertung der Angemessenheit<sup>323</sup> des Schutzniveaus kann die Kommission durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. In jedem Durchführungsrechtsakt werden der territoriale und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben. Der Durchführungsrechtsakt wird im Einklang mit dem Überprüfungsverfahren<sup>324</sup> aus Artikel 87 Absatz 2 angenommen.<sup>325</sup>
- 3a) *Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission geändert, ersetzt oder aufgehoben werden<sup>326</sup>.*
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 gefassten Beschlüsse.

---

<sup>323</sup> DE proposal. CZ and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data.

<sup>324</sup> BE and LU queried whether Member States would initiate such procedure.

<sup>325</sup> DE queried the follow-up to such decisions and warned against the danger that third countries benefiting from an adequacy decision might not continue to offer the same level of data protection. COM indicated there was monitoring of third countries for which an adequacy decision was taken.

<sup>326</sup> Moved from paragraph 8. CZ and AT thought an absolute time period should be set. NL, PT and SI thought this paragraph 8 was superfluous or at least unclear. If maintained it should be moved to the end of the Regulation.

5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 mehr<sup>327</sup> bietet, und erforderlichenfalls derartige Beschlüsse ohne rückwirkende Kraft widerrufen, ändern oder aussetzen. Die Durchführungsrechtsakte werden im Einklang mit dem Überprüfungsverfahren aus Artikel 87 Absatz 2 oder in äußerst dringlichen Fällen nach dem Verfahren des Artikels 87 Absatz 3 angenommen. <sup>328</sup>
  
6. (...) Übermittlungen personenbezogener Daten an das betreffende Drittland beziehungsweise an das Gebiet oder (...) den Verarbeitungssektor in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 42 bis 44 werden durch einen Beschluss nach Absatz 5 (...) nicht berührt. Die Kommission nimmt zu geeigneter Zeit Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation auf, um Abhilfe für die Situation, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat, zu schaffen. <sup>329</sup>
  
7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren von Drittländern und aller internationalen Organisationen, zu denen Beschlüsse gemäß den Absätzen 3 und 5 gefasst wurden.
  
8. (...) <sup>330</sup>

---

<sup>327</sup> COM reservation on the deletion of its possibility to adopt negative adequacy decisions.

<sup>328</sup> BE, DE, FI, IT, LU and FR asked for the deletion of paragraph 5.

<sup>329</sup> BE, DE, FR, FI, IT, LU and CZ asked for the deletion of paragraph 6.

<sup>330</sup> Move to paragraph 3a.

Artikel 42

***Datenübermittlung auf der Grundlage geeigneter Garantien*** <sup>331</sup>

1. Hat die Kommission keinen Beschluss nach Artikel 41 erlassen, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an einen oder mehrere Empfänger in einem Drittland oder an eine internationale Organisation übermitteln, sofern der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter *in einem rechtsverbindlichen Instrument* geeignete Garantien <sup>332</sup> zum Schutz personenbezogener Daten vorgesehen hat.
  
2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere <sup>333</sup> bestehen in
  - a) verbindlichen unternehmensinternen Vorschriften gemäß Artikel 43, oder
  - b) Standarddatenschutzklauseln, die (...) von der Kommission <sup>334</sup> gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen werden, oder
  - c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommenen Standarddatenschutzklauseln, die von der Kommission nach dem Prüfverfahren des Artikels 87 Absatz 2 angenommen wurden <sup>335</sup>, oder

---

<sup>331</sup> Several delegations (BE, CH, IT) queried whether this article (in particular paragraphs 2 (a + b) and 5) could also be applied to public authorities. UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of these procedures regarding data flows in the context of cloud computing was also questioned.

<sup>332</sup> SK scrutiny reservation.

<sup>333</sup> COM emphasised the non-exhaustive nature of this list, clarifying that also other types of agreements could be envisaged.

<sup>334</sup> FR reservation.

<sup>335</sup> DE proposal.

- d) Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger der Daten <sup>336</sup> vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden, oder
- e) genehmigten Verhaltensregeln gemäß Artikel 38 <sup>337</sup>, oder
- f) einem Zertifizierungsverfahren nach Maßgabe von Artikel 39. <sup>338</sup>, <sup>339</sup>
3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, b und c genannten *unternehmensinternen Vorschriften und Standarddatenschutzklauseln* erfolgen, bedürfen keiner besonderen Genehmigung.
4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d <sup>340</sup> (...) <sup>341</sup> genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter <sup>342</sup> die vorherige Genehmigung der zuständigen Aufsichtsbehörde (...) ein.
5. <sup>343</sup> Wenn trots der diesbezüglichen Bestimmung in Absatz 1 keine geeigneten Garantien für den Schutz personenbezogener Daten in einem rechtsverbindlichen Instrument vorgesehen werden, holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, wenn es sich dabei um eine Behörde oder öffentliche Stelle handelt, bei der zuständigen Aufsichtsbehörde die vorherige Genehmigung für jede Übermittlung oder Kategorie von Übermittlungen oder für die Aufnahme von entsprechenden Bestimmungen in die Verwaltungsvereinbarungen ein, die die Grundlage für eine solche Übermittlung bilden (...).

<sup>336</sup> BE proposed referring to a sub-processor.

<sup>337</sup> COM scrutiny reservation.

<sup>338</sup> NL proposed adding a reference to 'mutual binding obligations of professional secrecy or existing sectoral legislation which offers special protection to the interests of data subject between the controller or processor and the recipient of the data in the third country, territory or processing sector thereof or international organisation'.

<sup>339</sup> COM scrutiny reservation.

<sup>340</sup> BE proposed adding a reference point (e). CH thought this paragraph should not be applicable to public authorities.

<sup>341</sup> ES suggested inserting a reference to the absence of a DPO or certifications.

<sup>342</sup> BE suggested deleting the reference to the processor.

<sup>343</sup> BE and GR want to limit the scope of this paragraph to public authorities. IT on the contrary could not see how it could be applied by public authorities.

- 5a. Falls die Datenübermittlung nach Absatz 4<sup>344</sup> im Zusammenhang mit Verarbeitungstätigkeiten steht, welche betroffene Personen in mehreren Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.
- 5b. *Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben so lange in Kraft, bis sie von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden.*<sup>345</sup>
6. (...) <sup>346</sup>.

---

<sup>344</sup> COM scrutiny reservation.

<sup>345</sup> UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. It was thought that this was contrary to the principle of accountability. The question as to the fate of existing MOUs and international conventions was also raised. AT, PL, GR, SI and BG voiced concerns regarding the possibility to transfer personal data in the absence of a legally binding instrument. FR scrutiny reservation on the terms 'administrative arrangements' and 'substantially affect the free movement of personal data'. BE also thought this paragraph needed clarification.

<sup>346</sup> Subsumed under paragraphs 4 and 5.

Artikel 43

***Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner  
Vorschriften***<sup>347</sup>

1. Die zuständige Aufsichtsbehörde genehmigt<sup>348</sup> nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens *verbindliche unternehmensinterne Vorschriften*, sofern diese
  - a) rechtsverbindlich sind, für alle betreffenden<sup>349</sup> Mitglieder der Unternehmensgruppe oder der Unternehmensgruppen, die eine gemeinsame wirtschaftliche Tätigkeit ausüben, gelten und von diesen Mitgliedern angewendet werden<sup>350 351 352</sup>;
  - b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen<sup>353</sup>;
  - c) die in Absatz 2 festgelegten Anforderungen erfüllen.

---

<sup>347</sup> Several delegations supported this innovative legal technique: BE, CZ, DE, FR, FI, IT, LU, NL, PT and PL. NL thought it should be given a wider scope. NL and GR pleaded in favour of covering data flows in the context of cloud computing and ES thought more flexibility should be provided in this way. SI thought it should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied.

<sup>348</sup> DE and UK expressed concerns on the lengthiness and cost of such approval procedures. The question was raised which DPAs should be involved in the approval of such BCRs in the consistency mechanism.

<sup>349</sup> DE proposal.

<sup>350</sup> Further to GR proposed to insert a reference to 'alliances'. BE proposed to refer to sub-processors; ES proposed to insert a reference (in paragraph 1(a) as well as in (2)(f)(h)(i) and (k) to 'business partners'.

<sup>351</sup> ES thought subparagraph (a) could be simplified by stating that BCRs all binding to all involved.

<sup>352</sup> COM has a scrutiny reservation on 'group of enterprises engaged in a joint economic activity' extending the scope beyond one group of undertakings and how this would work in practice.

<sup>353</sup> FI proposed referring to BCRs and BE suggested a reference to effective administrative and judicial redress.

2. die verbindlichen unternehmensinternen Vorschriften nach Absatz 1 enthalten mindestens <sup>354</sup> folgende Angaben:
- a) Struktur und Kontaktdaten der betreffenden <sup>355</sup> Unternehmensgruppe und jedes ihrer Mitglieder <sup>356</sup>;
  - 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 Vorschriften;
  - d) die Anwendung der allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, auch in Bezug auf die Zwecke der Weiterverarbeitung <sup>357</sup>, die Datenqualität, die Rechtsgrundlage für die Verarbeitung, die Verarbeitung besonderer Kategorien von personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese unternehmensinternen Vorschriften gebundene Stellen (...);
  - e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten <sup>358</sup> und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner Profilerstellung (...) nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

---

<sup>354</sup> FR pleaded in favour of deleting the words 'at least'. IT is opposed to the deletion thereof.

<sup>355</sup> BE proposals.

<sup>356</sup> BE proposal; BE also proposed a reference to sub-processors.

<sup>357</sup> NL proposal.

<sup>358</sup> FI proposal.



- 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 Vorschriften; 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 Artikel 14 und 14a über die verbindlichen unternehmensinternen Vorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;
- h) die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;
- (hh) die Beschwerdeverfahren;
- i) die innerhalb der (...) Gruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften <sup>359</sup>;
- 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.

---

<sup>359</sup> NL proposed referring to auditing as an example.

- [3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.]<sup>360</sup>
4. Die Kommission kann das Format und Verfahren für den auf elektronischem Wege erfolgenden Informationsaustausch über verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

*Artikel 44*

***Ausnahmen für Sonderfälle***<sup>361</sup>

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 vorliegt noch geeignete Garantien nach Artikel 42<sup>362</sup> bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen<sup>363</sup> personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur zulässig, wenn

---

<sup>360</sup> CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives.

<sup>361</sup> EE, FR and NL reservation. UK thought that in reality these 'derogation' would become the main basis for international data transfers. It also opined that by their nature (many of) these derogations should not be called as such because the data transfers for which they allow are both justified and necessary.

<sup>362</sup> BE and LU proposed adding a reference to BCRs.

<sup>363</sup> FR and PL scrutiny reservation on the term 'set of transfers'.

- a) die betroffene Person in die vorgeschlagene Datenübermittlung eingewilligt hat, nachdem sie über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführter Datenübermittlungen informiert wurde, oder
- b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist, oder
- c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist, oder
- d) die Übermittlung aus *wichtigen* Gründen des öffentlichen Interesses notwendig ist <sup>364</sup>; *dabei muss es sich um ein öffentliches Interesse handeln, das im Unionsrecht oder im innerstaatlichen Recht des Mitgliedstaates, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt <sup>365</sup> ist*, oder
- e) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist <sup>366</sup>, 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 <sup>367</sup>, oder

---

<sup>364</sup> DE remarked that the effects of (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties. FR and IT reservation on the (subjective) use of the concept of public interest. It thought that also here it should be clarified that this ground cannot justify massive and structural transfers of data. LU proposed deleting the word 'important'.

<sup>365</sup> According to DE the word "exist" should make it clear that it is the public interest of the EU Member State being referred to, and not that of the third state.

<sup>366</sup> PL requested clarification on this subparagraph.

<sup>367</sup> In the view of the Presidency this also covers public health emergency situations.

- [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 <sup>368</sup>,] <sup>369</sup>oder
- h) die nicht in großem Maßstab oder häufig <sup>370</sup> erfolgende Übermittlung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter wahrgenommen wird <sup>371</sup>, erforderlich ist und falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und *erforderlichenfalls* auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat <sup>372</sup>. <sup>373</sup>
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.]

<sup>368</sup> FI requested clarification of this subparagraph.

<sup>369</sup> The Presidency will request the Commission to explain the purpose of this provision.

<sup>370</sup> NL proposal. DE and SK also thought the terms 'frequent or massive' are unclear. UK thought this qualification should be deleted.

<sup>371</sup> FR requests clarification concerning the concept of "legitimate interest(s)" and would like the balance of Directive 95/46 to be preserved. It scrutiny reservation. AT, PT and PL are opposed to this subparagraph and plead in favour of its deletion.

<sup>372</sup> IT suggested deleting the words 'where necessary'.

<sup>373</sup> DE proposed adding another exemption in cases where the competent supervisory authority has granted prior authorisation. DE is of the opinion: public entities should be exempted from this provision, because they are already checked by a state authority, which is itself subject to supervision and involved in procedures of mutual administrative and legal assistance.

3. (...)
4. Absatz 1 Buchstaben a, b und c <sup>374</sup> gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.
5. (...) <sup>375</sup>
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die in Absatz 1 Buchstabe h dieses Artikels genannten geeigneten Garantien in der Dokumentation gemäß Artikel 28 (...) <sup>376</sup>.
- [6a 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 aufgekündigt werden.] <sup>377</sup>
7. (...) <sup>378</sup>.

---

<sup>374</sup> COM scrutiny reservation on deleting (h).

<sup>375</sup> Moved to paragraph (1)(d). DE and NL proposed adding the possibility of Member State law preventing a transfer of data outside the EU.

<sup>376</sup> GR reservation: GR suggested deleting this paragraph in view of the administrative burden it entailed for controllers. IT wanted to clarify the notification took place before the transfer.

<sup>377</sup> COM enters reservation based on strong legal doubts on the legality of such proposal. COM recalls recital 79 which states that ‘This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subject.’

<sup>378</sup> Deleted further to reservation by BE, CZ, CY, ES, FR, FI, SE and UK.

Artikel 45

**Internationale Zusammenarbeit zum Schutz personenbezogener Daten** <sup>379</sup>

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) gegenseitigen Leistung internationaler 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 <sup>380</sup>,
  - c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zur Förderung der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,
  - d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten.
2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen, einschließlich deren Aufsichtsbehörden, insbesondere wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese einen angemessenen Schutz bieten <sup>381</sup>.

---

<sup>379</sup> PL thought (part of) Article 45 could be inserted into the preamble. UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI.

<sup>380</sup> AT and FO thought this subparagraph was unclear and required clarification.

<sup>381</sup> NL schlug vor, diesen Buchstaben zu streichen.

# KAPITEL VI

## UNABHÄNGIGE AUFSICHTSBEHÖRDEN

### ABSCHNITT 1

#### UNABHÄNGIGKEIT

##### *Artikel 46*

##### *Aufsichtsbehörde*<sup>382</sup>

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 (...) <sup>383</sup>. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden mit der Kommission sowie der Aufsichtsbehörden untereinander <sup>384</sup>.
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 <sup>385</sup>.

---

<sup>382</sup> At the request of IT, COM clarified that this DPA could be the same as the one designated/set up under the future Data Protection Directive. ES asked for clarification that a DPA may be composed of more members, but the presidency thinks this is already sufficiently clear from the current text.

<sup>383</sup> UK sought reassurance that the supervisory authority could also be given a wider remit, such as ensuring the freedom of information.

<sup>384</sup> UK thought there was no reason to mention this duty of co-operation here.

<sup>385</sup> De suggested deleting the bracketed part of the text

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 <sup>386</sup>.

*Artikel 47*

***Unabhängigkeit***

1. Jede Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben <sup>387</sup> und bei der Ausübung ihrer Befugnisse völlig <sup>388</sup> unabhängig.
2. Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse weder direkter noch indirekter Beeinflussung von außen.
3. (...)
4. (...) <sup>389</sup>
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 <sup>390</sup>.

---

<sup>386</sup> This paragraph could be moved to the final provisions.

<sup>387</sup> Prüfungsvorbehalt von EL.

<sup>388</sup> EE and SI suggested deleting the word 'completely'.

<sup>389</sup> COM scrutiny reservation on deletion of paragraphs 3 and 4.

<sup>390</sup> This paragraph was criticised for being too prescriptive (FR, SE) and too vague (LV).



6. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde über eigenes Personal verfügt, das der Leitung des Mitglieds oder der Mitglieder<sup>391</sup> der Aufsichtsbehörde (...) untersteht.
7. Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Die Mitgliedstaaten sorgen dafür, dass jede Aufsichtsbehörde über eigene jährliche Haushaltspläne verfügt, die veröffentlicht werden.

*Artikel 48*

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

1. Die Mitgliedstaaten tragen dafür Sorge, dass das Mitglied oder die Mitglieder<sup>392</sup> jeder Aufsichtsbehörde entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des betreffenden Mitgliedstaats ernannt werden<sup>393</sup>.
2. Das Mitglied oder die Mitglieder verfügen über die für die Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde (...) <sup>394</sup>.
3. (...)
4. (...).
5. (...) <sup>395</sup>

---

<sup>391</sup> DE, LV, NO, PT and UK questioned who were to be considered as members of the DPA and argued that the regulation should allow different models. IT thought EU resources could also be considered.

<sup>392</sup> DE, LV, NO, PT and UK questioned would were to be considered as members of the DPA and argued that the regulation should allow different models.

<sup>393</sup> Several delegations (FR, SE, SI and UK) thought that other modes of appointment should be allowed for. LU thought this should not be governed by the Regulation.

<sup>394</sup> As several delegations (DE, ES, SE) thought that also the appointment of persons with prior data protection experience should be allowed for, this requirement has been deleted. CZ indicated that independence should not be a requirement for appointment, but for the functioning of DPA members.

<sup>395</sup> The Presidency agrees with those delegations (BE, CZ, FR, LU, NL, NO, PT, SE, SK, UK) that are of the opinion that paragraphs 4 and 5 interfere too much with national law. CZ, NO, SE and the Presidency also see no need for paragraph 3. COM scrutiny reservation on deletion of paragraphs 3 to 5.

Artikel 49

**Errichtung der Aufsichtsbehörde** <sup>396</sup>

1. Jeder Mitgliedstaat regelt durch Gesetz
  - a) die Errichtung jeder Aufsichtsbehörde (...),
  - b) (...),
  - 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 <sup>397</sup> 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 <sup>398</sup>;
  - e) ob, und wenn ja, wie oft <sup>399</sup> das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiedervernannt werden können,

---

<sup>396</sup> DE and FR queried which was the leeway given to Member States by this article as compared to the rules flowing from the previous Articles from the Regulation. Several delegations (FR, GR, SE, SI UK) thought that some of these rules, in particular those spelled out in subparagraphs (c) and (d) were too detailed.

<sup>397</sup> DE proposed adding a maximum term of eight years.

<sup>398</sup> The last part of this point might need to be moved to the final provisions.

<sup>399</sup> DE proposal. IT likewise thought a maximum term should be set

- f) die (...) Bedingungen für die Einstellung des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde sowie die Regelungen für die Beendigung des Beschäftigungsverhältnisses <sup>400</sup>,
- g) (...).
2. Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht während ihrer Amts- beziehungsweise Dienstzeit und 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 bewahren. <sup>401 402</sup>

*Artikel 50*

***Berufsgeheimnis*** <sup>403</sup>

(...)

---

<sup>400</sup> SE thought that subparagraphs (b), (c) and (f) should be deleted or substantially redrafted as they were too detailed.

<sup>401</sup> BE proposed adding an additional paragraph on the need to distinguish investigating and sanctioning powers, but the presidency deem that this is dealt with by the general safeguard clause in Article 53.5. The same goes for the DE proposal for adding language concerning the duty to report an offence under national law and the privilege against self-incrimination.

<sup>402</sup> COM scrutiny reservation on adding the provision on professional secrecy to Article 49, which concerns rules on the establishment of supervisory authorities.

<sup>403</sup> UK pointed out that also transparency concerns should be taken into account. Many delegations (CZ, DE, FR, FI; GR, IT, SE, SI, UK) raised practical questions as to the scope and the exact implications of this article. All thought that the rules on professional secrecy should be left to national law and hence the Presidency has followed the suggestion by CZ and SI and moved this to Article 49. COM scrutiny reservation on moving this provision to Article 49; should remain a separate provision.

## ABSCHNITT 2

### ZUSTÄNDIGKEIT<sup>404</sup>, AUFGABEN UND BEFUGNISSE

#### *Artikel 51*

#### ***Zuständigkeit***<sup>405</sup>

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<sup>406, 407</sup>.

---

<sup>404</sup> GR thought it would be better to refer to jurisdiction rather than competence.

<sup>405</sup> Some delegations (BG, CY, DE, GR, NL and LU) supported the principle of the main-establishment rule (aka as the one-stop-shop principle), but had many questions of understanding as to its practical implementation. Other delegations (BE, CZ, ES, FR, IT, AT, PT, RO and SI) had a more critical attitude and entered a reservation. One of the main questions was whether the allocation of competence to the DPA of the main establishment was exclusive and whether it also implied a rule of applicable law (DE, ES). A practical question was that of the language regime which would govern the co-operation between the DPAs and the communication with the controllers and the data protection. All delegations seemed to agree that at any rate the establishment of such a rule could not lead to the exercise of investigative powers by the DPA of one authority in the territory of another Member State.

<sup>406</sup> At the request of several delegations, COM indicated that the main-establishment rule under this paragraph would not apply to controllers established outside the EU. In the view of the Commission, this constituted an incentive for non-EU controllers to establish themselves in the EU in order to avail themselves of the benefit of the main establishment rule. PL rightly pointed out that there was a need to specify the criterion on the basis of which the competent DPA would be established in such cases and the Presidency has endeavoured to do so by adding a sentence.

<sup>407</sup> Some Member States questioned the interaction between paragraphs 1 and 2 and requested more clarity on which was to be the competent Member State: DE, SE. The Presidency has endeavoured to redraft paragraph 1 so as to clarify that this paragraph sets out the principle of the territoriality of supervision, from which the main-establishment rule in paragraph 2 derogates. The new drafting of § 1 also implies that for controllers established outside the EU, the competent DPA will be that of the Member State where the data subjects resides. IT thought the latter rule should also be applied regarding processing of personal data by controllers/processors established within the EU.

2. Findet die Verarbeitung personenbezogener Daten in mehreren Mitgliedstaaten statt, wobei der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, so ist die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, für Maßnahmen zuständig, die durch die Erfüllung der Aufgaben gemäß Artikel 52 Absatz 1 Buchstaben hb und i und in Ausübung der Befugnisse nach Artikel 53 Absatz 1 Buchstaben a bis h sowie nach den Artikeln 79 und 79a hinsichtlich der Verarbeitungstätigkeit des für die Verarbeitung Verantwortlichen oder des Verarbeiters in allen betroffenen Mitgliedstaaten Rechtswirkungen erzeugen sollen.
- 2a. Die Aufsichtsbehörde der Hauptniederlassung arbeitet gemäß Kapitel VII dieser Verordnung mit anderen Aufsichtsbehörden und insbesondere mit der Aufsichtsbehörde, bei der eine Beschwerde eingelegt wurde, zusammen.
- 2b. Absatz 2 gilt nicht für Behörden und öffentliche Stellen <sup>408</sup>.
3. Die Aufsichtsbehörden sind nicht zuständig für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen <sup>409</sup>.

---

<sup>408</sup> Further to LU proposal.

<sup>409</sup> FR, HU, UK scrutiny reservation.

*Artikel 52*  
***Aufgaben*** <sup>410</sup>

1. Jede Aufsichtsbehörde muss zumindest <sup>411</sup>
- aa) (...) *die Öffentlichkeit über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;*
- ab) *die für die Verarbeitung Verantwortlichen, und der Auftragsverarbeiter über die ihnen aus dieser Verordnung entstehenden Verpflichtungen aufklären;*
- (ac) *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;*
- a) die Anwendung dieser Verordnung überwachen und durchsetzen,
- b) sich mit Beschwerden <sup>412</sup> einer betroffenen Person oder einer Stelle, einer Organisation oder <sup>413</sup> 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<sup>414</sup>, vor allem, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,

---

<sup>410</sup> IT scrutiny reservation.

<sup>411</sup> Addition suggested by the Presidency in order to clarify that Member States may allocate other tasks to DPAs.

<sup>412</sup> IT scrutiny reservation on the term complaint; UK thought the emphasis should be on complaint-resolution.

<sup>413</sup> Alignment with the text of Article 73.

<sup>414</sup> IT suggested fixing a 10-weeks period for dealing with the complaint.

- c) Information mit anderen Aufsichtsbehörden austauschen und Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten,
- d) Untersuchungen über die Anwendung dieser Verordnung entweder auf eigene Initiative oder (...) auf Ersuchen einer anderen Aufsichtsbehörde oder einer anderen Behörde durchführen (...),
- e) relevante Entwicklungen verfolgen, soweit als sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere der Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,
- f) Konsultationsersuchen der Organe und Einrichtungen der Mitgliedstaaten, einschließlich derjenigen nach Artikel 34 Absatz 7, im Hinblick auf Rechts- und Verwaltungsmaßnahmen Folge leisten, die den Schutz der Rechte und Freiheiten der natürlichen Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand haben <sup>415</sup>,
- (fa) eine Liste der Verarbeitungsarten erstellen und veröffentlichen, für die gemäß Artikel 33 Absatz 2a eine Datenschutz-Folgenabschätzung durchzuführen ist <sup>416</sup>,
- g) Beratung in Bezug auf die in Artikel 34 Absatz 3 genannten Verarbeitungsvorgänge leisten und die Verarbeitung im Sinne des Artikels 34 Absatz 7a genehmigen,
- (ga) die Ausarbeitung von Verhaltensregeln gemäß Artikel 38 fördern;

---

<sup>415</sup> CZ, ES, MT and LT reservation on this measure, which they considered as an interference with the legislative process. Other delegations (CH, DE, FI, LU, SI) did not have problems with this obligation, which already existed under the data protection Directive 46/95

<sup>416</sup> Further to BE proposal.

- (gb) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen anregen,
  - (gc) die nach Artikel 39 Buchstabe 4 erteilten Zertifizierungen regelmäßig überprüfen,
  - h) zu den Entwürfen von Verhaltensregeln gemäß Artikel 38 Absatz 2 Stellung nehmen,
  - (ha) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 38a und einer Zertifizierungsstelle gemäß Artikel 39a vornehmen<sup>417</sup>;
  - (hb) Vertragsklauseln im Sinne des Artikels 42 Absatz 2 Buchstabe d genehmigen,
  - i) verbindliche unternehmensinterne Vorschriften gemäß Artikel 43 genehmigen,
  - j) Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses leisten.
2. (...) <sup>418</sup>
  3. (...) <sup>419</sup>
  4. Für die in Absatz 1 Buchstabe b genannten Beschwerden stellt jede Aufsichtsbehörde ein Beschwerdeformular zur Verfügung, das elektronisch oder auf anderem Wege ausgefüllt werden kann.
  5. Die Leistungen jeder Aufsichtsbehörde sind für die betroffene Person und für den Datenschutzbeauftragten<sup>420</sup> kostenlos.

---

<sup>417</sup> Further to DE proposal.

<sup>418</sup> Moved to paragraph 1.

<sup>419</sup> Moved to paragraph 1.

<sup>420</sup> DE proposal.



6. Bei offenkundig unbegründeten oder – besonders im Fall ihrer Häufung – unverhältnismäßigen Anträgen kann sich die Aufsichtsbehörde weigern, aufgrund des<sup>421</sup> Antrags tätig zu werden (...) <sup>422</sup>. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offensichtlich unbegründeten oder unverhältnismäßigen Charakter des Antrags <sup>423</sup>.

*Artikel 53*

***Befugnisse***<sup>424</sup>

1. Jeder Mitgliedstaat regelt durch Gesetz, dass <sup>425</sup> seine Aufsichtsbehörde mindestens<sup>426</sup> über die Befugnis verfügt <sup>427</sup>,

---

<sup>421</sup> DE proposal.

<sup>422</sup> PL scrutiny reservation. EE pointed out that under its constitution this required an act of parliament. NL also thought this should be left to Member States.

<sup>423</sup> DE reservation: this can be left to general rules.

<sup>424</sup> Several Member States (DE, FR) stated that it was unacceptable that the supervisory authority would be able to exercise these powers vis-à-vis public authorities.

<sup>425</sup> Suggested amendment in order to allay the concern from Member States (FR, NL) that they should be able to specify in their national law, as has been the case under the 1995 Data Protection Directive, the exact scope of, conditions and guarantees for the exercise of these powers.

<sup>426</sup> Further to BG suggestion to make this an indicative list. RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules.

<sup>427</sup> A distinction must be drawn between powers with regard to public and non-public bodies. Direct powers of instruction in respect of public bodies subject to supervisory and judicial control, which might therefore lead to conflicts, would be problematic for Germany. Moreover, consideration also needs to be given to the delimitation between this proposal and the proposal for a Directive on police and judicial affairs, which accords fewer powers to the supervisory authorities in some respects.

- a) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter auf einen behaupteten Verstoß gegen diese Verordnung hinzuweisen und ihn gegebenenfalls anzuweisen, diesem Verstoß in einer bestimmten Weise abzuhelpen <sup>428</sup>,
- b) den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
- ba) Datenschutzüberprüfungen durchzuführen,
- c) den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
- d) sicherzustellen, dass die Bestimmungen über die vorherige Zurateziehung in Artikel 34 Absatz 2 und die Bestimmungen über die vorherigen Genehmigungen in Artikel 34 Absatz 7a und in Artikel 42 Absatz 2 Buchstabe d und Absatz 5 eingehalten werden,
- e) einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
- (ea) einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter zu tadeln, wenn sie mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen haben,
- (eb) einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

---

<sup>428</sup> BE suggested adding the power to oblige the controller to communicate the personal data breach to the data subject.

- f) die Berichtigung, Vernichtung oder Löschung (...) von Daten (...) <sup>429</sup> anzuordnen, und solche Maßnahmen Empfängern, an die diese Daten gemäß Artikel 17 und 17b weitergegeben wurden, mitzuteilen,
- g) die Verarbeitung vorübergehend oder endgültig zu verbieten,
- h) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen,
- i) Stellungnahmen zu allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten abzugeben,
- j) (...) <sup>430</sup>.

2. Jede Aufsichtsbehörde (...) ist befugt, vom für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter Folgendes zu verlangen:

- a) Zugriff auf alle personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind,
- b) Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte <sup>431</sup>.

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

---

<sup>429</sup> Deleted further to DE suggestion as the breach of the Regulation is obvious here.

<sup>430</sup> Deleted in view of the constitutional and other problems raised by some Member States (NL, IT, PT) and the fact that there is already an information under Article 54. ES suggested inserting a reference to the carrying out of audit plans or audit plans.

<sup>431</sup> The requirement of reasonable grounds has been deleted here as the procedural requirements will be set out under national law to which the new paragraph 5 refers.

3. Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Klage einzureichen oder zu erheben <sup>432</sup>, damit diese Verordnung durchgeführt wird.
4. Jede Aufsichtsbehörde ist befugt, zusätzlich zu den in Absatz 1 Buchstaben e bis h vorgesehenen Maßnahmen oder an deren Stelle je nach den Umständen jedes einzelnen Falls Geldbußen gemäß Artikel 79 und 79a zu verhängen <sup>433</sup>.
5. Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel unterliegt angemessenen Verfahrensgarantien in Übereinstimmung mit dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren <sup>434</sup>.

---

<sup>432</sup> CZ, DE and FR reservation on proposed DPA power to engage in legal proceedings.

<sup>433</sup> BE scrutiny reservation. DE reservation: deletion.

<sup>434</sup> New paragraph, partially inspired by the last sentence of paragraph 2. The additional language is proposed by the Presidency in order to clarify that these powers will be exercised under the national law of the Member States, which needs to provide for the necessary guarantees for the rights of the defence. The reference to national law will allow Member States to apply their procedural rules (cf. remarks by BE, DE, ES). This should also allow to take into account any concerns regarding self-incrimination.

*Artikel 54*  
***Tätigkeitsbericht***

Jede Aufsichtsbehörde erstellt einen Jahresbericht <sup>435</sup> über ihre Tätigkeit. Der Bericht wird der Regierung <sup>436</sup> und dem nationalen Parlament vorgelegt und der Öffentlichkeit, der Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

---

<sup>435</sup> This article does not detract from the possibility for Member States to provide under national law that other, extraordinary reports may also be conveyed to the parliament and the government. However, the Presidency agrees with SI that there no need to oblige Member States to do so, certainly as there is a risk of an 'overkill' of reports.

<sup>436</sup> SE proposal; ES suggested adding 'other authorities designated under national law'.

**KAPITEL VII**  
**ZUSAMMENARBEIT UND KOHÄRENZ**

**ABSCHNITT 1**  
**ZUSAMMENARBEIT**

*Artikel 54a*

**Zusammenarbeit bei Beschwerden**

1. Wird bei einer anderen als der nach Artikel 51 zuständigen Aufsichtsbehörde eine Beschwerde eingelegt, so trifft die zuständige Aufsichtsbehörde bei Eingang der Beschwerde im Benehmen mit der Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, geeignete Maßnahmen.
  
2. Bei der Ausübung der Befugnisse gemäß Artikel 51 Absatz 2 trägt die zuständige Aufsichtsbehörde den Auffassungen der Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, weitestgehend Rechnung.

*Artikel 55*  
*Amtshilfe*<sup>437</sup>

1. Die Aufsichtsbehörden übermitteln einander zweckdienliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Zurateziehung, um Vornahme von Nachprüfungen und Untersuchungen. Dies gilt insbesondere, wenn die Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, nicht die Aufsichtsbehörde der Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters ist. Die Amtshilfe bezieht sich auch auf die Bereitstellung von Informationen über Untersuchungen in Fällen, in denen Personen in mehreren Mitgliedstaaten voraussichtlich von Verarbeitungsvorgängen des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters betroffen sind.

---

<sup>437</sup> SI and SE scrutiny reservation. Several delegations indicated further clarity was required on the concept of mutual assistance: DE, NL, FR, ES, NL, PL and UK pleaded for more flexibility. COM stated this was a specification of the rules already contained in CoE Convention No. 108. EE pleaded for much more detailed rules on mutual assistance, as is already the case in civil and criminal law.

2. Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats <sup>438</sup> nach Eingang des Ersuchens nachzukommen. Dazu können insbesondere auch die Übermittlung zweckdienlicher Informationen über die Durchführung einer Untersuchung oder Durchsetzungsmaßnahmen gehören, um die Aussetzung oder das Verbot von Verarbeitungsvorgängen zu erwirken, die gegen diese Verordnung verstoßen.
3. Das Amtshilfeersuchen enthält alle erforderlichen Informationen <sup>439</sup>, darunter Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für die sie angefordert wurden.
4. <sup>440</sup> Die Aufsichtsbehörde, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn
  - a) sie für den Gegenstand des Ersuchens nicht zuständig ist <sup>441</sup> 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 die Beschwerde eingeht, unterliegt.

---

<sup>438</sup> SE remarked that this timeline might be unrealistic in some cases. COM indicated that it was only a deadline for replying, but that §5 allowed longer periods for executing the assistance requested ES on the other hand suggested reducing it to 15 days.

<sup>439</sup> EE scrutiny reservation.

<sup>440</sup> SE indicated further scrutiny was required as to whether other grounds of refusal were required.

<sup>441</sup> Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI.



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 <sup>442</sup>.
6. Die Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, 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 <sup>443</sup> einer anderen Aufsichtsbehörde die Informationen gemäß Absatz 5 <sup>444</sup>, so kann die ersuchende Aufsichtsbehörde einstweilige Maßnahmen im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 51 Absatz 1 ergreifen und die Angelegenheit dem Europäischen Datenschutzausschuss und der Kommission gemäß dem Kohärenzverfahren des Artikels 57 vorlegen <sup>445</sup>.

---

<sup>442</sup> Further to IT remark

<sup>443</sup> Further to DE and GR suggestion.

<sup>444</sup> SE suggestion.

<sup>445</sup> EE, FR, RO and UK reservation. FR asked whether this referred to the urgency procedure of Article 61.

9. Die Aufsichtsbehörde legt die Gültigkeitsdauer dieser einstweiligen Maßnahme fest, die drei Monate nicht übersteigen darf. Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission 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. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen <sup>446</sup>.

#### *Artikel 56*

#### ***Gemeinsame Maßnahmen der Aufsichtsbehörden*** <sup>447</sup>

1. (...) Die Aufsichtsbehörden können<sup>448</sup> gegebenenfalls gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen (...) durchführen, an denen (...) Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.

---

<sup>446</sup> DE, IT and EE reservation. EE questioned whether implementing acts where necessary for this purpose .

<sup>447</sup> EE and PT scrutiny reservation. Several delegations (DE, LV, NL, SE) supported the idea of joint operations, but thought more details needed to clarified. DE and EE referred to a criminal law model of a joint investigation team. Other Member States (LU, PL) indicated they were not convinced of the added value of joint investigations.

<sup>448</sup> LU proposal.

2. In Fällen, in denen die Verarbeitungsvorgänge voraussichtlich auf eine erhebliche Anzahl von <sup>449</sup> betroffenen Personen in mehreren Mitgliedstaaten <sup>450</sup> nachteilige Auswirkungen haben werden <sup>451</sup>, 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 der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Untersuchungsbefugnisse nach dem Recht 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. (...) <sup>452</sup> <sup>453</sup>
4. (...)

---

<sup>449</sup> LU proposal. COM reservation.

<sup>450</sup> At the request of several delegations, COM indicated that this phrase was the criterion which could trigger the establishment of a joint operation.

<sup>451</sup> LU and SI suggestion.

<sup>452</sup> SI and GR suggestion.

<sup>453</sup> DE and COM scrutiny reservation.

5. Ist eine gemeinsame Maßnahme geplant und kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 zweiter Satz 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 und die Kommission gemäß dem Kohärenzverfahren nach Artikel 57 unverzüglich von dieser Maßnahmen und ihren Gründen für deren Erlass in Kenntnis.

## ABSCHNITT 2

### KOHÄRENZ <sup>454</sup>

#### *Artikel 57*

#### ***Kohärenzverfahren***

1. Zu dem in Artikel 46 Absatz 1a genannten Zweck arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und mit der Kommission zusammen <sup>455</sup>.
2. *Bevor die zuständige Aufsichtsbehörde eine Maßnahme nach Absatz 3 erlässt, übermittelt sie die geplante Maßnahme dem Europäischen Datenschutzausschuss und der Kommission <sup>456</sup>.*
3. *Die in Absatz 2 genannte Verpflichtung gilt für eine geplante Maßnahme, die (...)*

---

<sup>454</sup> SI scrutiny reservation. BE reservation on the time required for a consistency mechanism procedure. DE parliamentary reservation and ES reservation on the role of COM in the consistency mechanism.

<sup>455</sup> DE thought that supervisory authorities of third countries for which there is an adequacy decision should be involved in the consistency mechanism; if third countries participated in the consistency mechanism, they would be bound by uniform implementation and interpretation.

<sup>456</sup> IT proposed limiting this to cases where a coordination mechanism implemented by the lead authority does not result a solution acceptable to all supervisory authorities concerned.

- a) für die Ausübung der Befugnisse der Aufsichtsbehörde nach Artikel 53 Absatz 1 Buchstaben b, c, eb, f, g und h oder auf die Verhängung einer verwaltungsrechtlichen Sanktion gemäß den Artikeln 79 und 79a<sup>457</sup> bestimmt ist und sich auf Verarbeitungstätigkeiten bezieht, die für eine große Zahl von<sup>458</sup> betroffenen Personen in mehreren Mitgliedstaaten wesentliche Folgen haben; oder
- b) *den freien Verkehr personenbezogener Daten in der Union wesentlich beeinträchtigen kann<sup>459 460</sup>;*
- c) *der Annahme einer Liste der Verarbeitungsvorgänge dient, die der Anforderung einer Datenschutz-Folgenabschätzung gemäß Artikel 33 Absatz 2b unterliegen oder*
- ca) eine Angelegenheit gemäß Artikel 38 Absatz 2b und damit die Frage, ob ein Entwurf von Verhaltensregeln oder eine Änderung oder Ergänzung von Verhaltensregeln mit dieser Verordnung in Einklang steht, betrifft oder
- (cb) der Billigung der Kriterien für die Akkreditierung einer Einrichtung gemäß Artikel 38a Absatz 3 oder einer Zertifizierungseinrichtung gemäß Artikel 39a Absatz 3 dient;
- d) *der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 42 Absatz 2 Buchstabe c dient oder*

---

<sup>457</sup> IT suggested adding the sanctioning power under Article 79.

<sup>458</sup> LU proposed adding ‘a significant number’. PL and SE also thought the involvement of the EDPB should be confined to cases where the DPAs cannot agree among each others and referred in particular to paragraph 2(a). COM scrutiny reservation.

<sup>459</sup> IT scrutiny reservation.

<sup>460</sup> DE proposed combining (a) and (b) and thereby reducing the cases in which the consistency mechanism would need to be applied.

- 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.*
4. *Jede betroffene<sup>461</sup> Aufsichtsbehörde und der Europäische Datenschutzausschuss können beantragen, dass eine Angelegenheit nach Absatz 3 im Rahmen des Kohärenzverfahrens behandelt wird, insbesondere, wenn eine Aufsichtsbehörde die in Absatz 3 genannte geplante Maßnahme nicht vorlegt oder den Verpflichtungen zur Amtshilfe gemäß Artikel 55 oder zu gemeinsamen Maßnahmen gemäß Artikel 56 <sup>462</sup>nicht nachkommt.*
5. *Um die ordnungsgemäße und kohärente Anwendung dieser Verordnung sicherzustellen, kann die Kommission beantragen, dass eine Angelegenheit nach Absatz 3 im Rahmen des Kohärenzverfahrens behandelt wird <sup>463</sup>.*
6. *Die Aufsichtsbehörden und die Kommission übermitteln dem Europäischen Datenschutzausschuss<sup>464</sup> auf elektronischem Wege unter Verwendung eines standardisierten Formats zweckdienliche Informationen, darunter je nach Fall eine kurze Darstellung des Sachverhalts, die geplante Maßnahme, (...) die Gründe, warum eine solche Maßnahme ergriffen werden muss, und die Ansichten anderer betroffener Aufsichtsbehörden.*

---

<sup>461</sup> BE, IT, SE SI and PL thought the scope of this paragraph should be limited so as to limit the number of cases. BE suggested deleting this paragraph

<sup>462</sup> LU proposed restricting this to cases where the coordination mechanism implemented by the competent authority did not allow for a solution to be reached; ES referred to cases where the other authorities did not agree with the proposal of the competent(/lead) authority.

<sup>463</sup> BE and DE asked for the deletion of this paragraph.

<sup>464</sup> DE proposal.

7. *Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet unverzüglich<sup>465</sup> auf elektronischem Wege unter Verwendung eines standardisierten Formats die Mitglieder des Datenschutzausschusses und die Kommission über zweckdienliche Informationen, die ihm zugegangen sind. Soweit erforderlich stellt der Vorsitz des Europäischen Datenschutzausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung.*

*Artikel 58*

***Stellungnahme des Europäischen Datenschutzausschusses***

1. (...)
2. (...)
3. (...)
4. (...)
5. (...)
6. (...)<sup>466</sup>
7. Der Europäische Datenschutzausschuss gibt eine Stellungnahme zu Angelegenheiten ab, die ihm im Rahmen des Kohärenzverfahrens nach Artikel 57 vorgelegt wurden, sofern er nicht bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat<sup>467</sup>.

---

<sup>465</sup> GR and IT suggestion.

<sup>466</sup> Paragraphs 1 to 6 have been moved to Article 57.

<sup>467</sup> ES suggested deleting the possibility for one DPA requesting an opinion from the EDPB, but keeping this possibility for the Commission.



- 7a. Die Stellungnahme wird binnen eines Monats <sup>468</sup> mit einfacher Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen, es sei denn, eine Aufsichtsbehörde des Mitgliedstaats, in dem eine Beschwerde erhoben worden ist, verlangt eine eingehendere Prüfung der Stellungnahme. In diesem Fall wird die Stellungnahme mit Zweidrittelmehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen <sup>469</sup>.
- 7b. Nimmt der Europäische Datenschutzausschuss innerhalb der Frist nach Absatz 7a keine Stellungnahme an, so kann die Aufsichtsbehörde nach Artikel 57 Absatz 2 ihre geplante Maßnahme erlassen <sup>470</sup>.
- 7c. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet je nach Fall die in Artikel 57 Absatz 2 oder 4 genannte Aufsichtsbehörde und die Kommission (...) unverzüglich über die Stellungnahme und veröffentlicht sie.
8. Die in Artikel 57 Absatz 2 genannte Aufsichtsbehörde (...) tragen der Stellungnahme des Europäischen Datenschutzausschusses so weit wie möglich<sup>471</sup> Rechnung und teilen dessen Vorsitz (...) binnen zwei Wochen nach Eingang der Stellungnahme elektronisch unter Verwendung eines standardisierten Formats mit, ob sie die geplante Maßnahme beibehält oder ändert; gegebenenfalls übermittelt sie die geänderte geplante Maßnahme.
9. Beabsichtigt die betroffene Aufsichtsbehörde nicht, der Stellungnahme zu folgen, so unterrichtet sie den Vorsitz des Europäischen Datenschutzausschusses und die Kommission innerhalb der Frist nach Absatz 8 und erläutert ihre Weigerung, der Stellungnahme zu folgen <sup>472</sup>.

---

<sup>468</sup> BE and GR proposed two months.

<sup>469</sup> DE proposed providing a mechanism for consultation of stakeholders.

<sup>470</sup> Further to LU proposal.

<sup>471</sup> Further to IT suggestion.

<sup>472</sup> Further to DE proposal.

*Artikel 59*

***Stellungnahme der Kommission*** <sup>473</sup>

(...)

*Artikel 60*

***Aussetzung einer geplanten Maßnahme*** <sup>474</sup>

(...)

---

<sup>473</sup> Deleted in accordance with the request from BE, CZ, DE, ES, FR, SE and UK. PT and PL scrutiny reservation. COM reservation on deletion.

<sup>474</sup> Deleted at the suggestion of BE, CZ, DE, FR, IT, SE and UK. PT scrutiny reservation. COM reservation on deletion.

Artikel 61

**Dringlichkeitsverfahren** <sup>475</sup>

1. Unter außergewöhnlichen Umständen *kann die zuständige* Aufsichtsbehörde abweichend vom Kohärenzverfahren nach Artikel 57 sofort einstweilige Maßnahmen gemäß Artikel 53 Absatz 1 Buchstaben b,c,eb,f, g und h <sup>476</sup>mit festgelegter Geltungsdauer treffen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um Rechte und Freiheiten von betroffenen Personen, (...) zu schützen (...). Die Aufsichtsbehörde setzt den Europäischen Datenschutzausschuss und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis <sup>477</sup>.
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 des Europäischen Datenschutzausschusses ersuchen.
3. Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme ersuchen, wenn die zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine geeignete Maßnahme getroffen hat, um die Rechte und Freiheiten von betroffenen Personen zu schützen.

---

<sup>475</sup> COM explained that the urgency procedure was an essential part of the consistency mechanism. The existence of an urgency procedure was welcomed by several delegations (DE, ES, IT, NL), but also gave rise to many questions. There was lack of clarity surrounding the criteria which could warrant the taking of provisional measures (DE, FR, PT), in particular by another DPA. The need to respect certain procedural guarantees (e.g. giving notice to the data controller) prior to the taking of provisional measures was emphasised by FR.

<sup>476</sup> COM scrutiny reservation.

<sup>477</sup> The conditions under which the EDPB needed to be informed also gave rise to questions (GR, ES). Com stated the obligation only existed in cross-border cases

4. Abweichend von Artikel 58 Absatz 7a wird die Stellungnahme im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen mit einfacher Mehrheit der Mitglieder des Europäischen Datenschutzausschusses angenommen.

*Artikel 62<sup>478</sup>*

***Durchführungsrechtsakte***

1. Die Kommission kann zu folgenden Zwecken Durchführungsrechtsakte mit allgemeiner Geltung erlassen:
- a) Gewährleistung der ordnungsgemäßen und einheitlichen Anwendung dieser Verordnung (...) im Hinblick auf Angelegenheiten, die ihr gemäß Artikel 57 Absatz 3 Buchstabe b von einer Aufsichtsbehörde übermittelt wurden (...),
  - 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 6 und 7 sowie Artikel 58 Absatz 5.

Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

---

<sup>478</sup> COM reservation.

2. In hinreichend begründeten Fällen äußerster Dringlichkeit im Zusammenhang mit den Interessen betroffener Personen gemäß Absatz 1 Buchstabe a erlässt die Kommission gemäß dem Verfahren von Artikel 87 Absatz 3 sofort geltende Durchführungsrechtsakte. Diese gelten für einen Zeitraum von höchstens 12 Monaten.
3. Unabhängig davon, ob die Kommission eine Maßnahme nach Maßgabe dieses Abschnitts erlassen hat, kann sie auf der Grundlage der Verträge andere Maßnahmen erlassen.

*Artikel 63*

***Durchsetzung***<sup>479</sup>

1. Für die Zwecke dieser Verordnung ist eine (...) Maßnahme einer Aufsichtsbehörde eines Mitgliedstaats, die mit den Anforderungen dieses Abschnitts in Einklang steht, in allen anderen betroffenen Mitgliedstaaten durchsetzbar.
2. (...) <sup>480</sup>

---

<sup>479</sup> EE and SI reservation.

<sup>480</sup> COM scrutiny reservation on deletion.

### ABSCHNITT 3

## EUROPÄISCHER DATENSCHUTZAUSSCHUSS <sup>481</sup>

#### *Artikel 64*

#### *Europäischer Datenschutzausschuss* <sup>482</sup>

1. Hiermit wird ein Europäischer Datenschutzausschuss eingerichtet.
2. Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten <sup>483</sup>.
3. Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Richtlinie erlassenen Vorschriften zuständig, so wird der Leiter einer dieser Aufsichtsbehörden zum gemeinsamen Vertreter ernannt.
4. Die Kommission <sup>484</sup> ist berechtigt, an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen und bestimmt einen Vertreter ohne Stimmrecht. Der Vorsitz des Europäischen Datenschutzausschusses unterrichtet die Kommission unverzüglich von allen Tätigkeiten des Europäischen Datenschutzausschusses.

---

<sup>481</sup> Several Member States (BE, DE, IT, PT) pleaded in favour of granting the EDPB the power to take legally binding decisions in the context of the consistency mechanism and do away with the proposed Commission power to intervene. It was argued that the DPAs should have the same independence vis-à-vis the Commission, as vis-à-vis the Member States' authorities. COM argued that it was legally impossible under the T(F)EU to confer such powers on the EDPB. ES was also opposed to granting the EDPB the power to take legally binding decisions.

<sup>482</sup> The term 'Board' seems inappropriate and could be replaced by Committee

<sup>483</sup> NO pleaded in favour of the participation of the associated States. COM replied that the modalities for such participation were provided for in the association agreement.

<sup>484</sup> It pleaded in favour of also including the Council and the Parliament.

*Artikel 65*

***Unabhängigkeit***

1. Der Europäische Datenschutzausschuss handelt bei der Ausführung seiner Aufgaben 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 Ausführung seiner Aufgaben weder um Weisung noch nimmt er Weisungen entgegen.

*Article 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 <sup>485</sup>:
  - a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, darunter auch etwaige Vorschläge zur Änderung dieser Verordnung;
  - b) von sich aus, auf Antrag eines seiner Mitglieder <sup>486</sup> oder auf Ersuchen der Kommission <sup>487</sup> vorgenommene Prüfung von die Anwendung dieser Verordnung betreffenden Fragen und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren (...) zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;

---

<sup>485</sup> DE suggested adding the provision of an opinion on the level of data protection in third countries or international organisations

<sup>486</sup> FR suggested that controllers be added here. However a controller can always ask 'its' DPA to submit a certain issue to the DPA.

<sup>487</sup> Some Member States (IT, DE) thought that, if Commission requests were included here, a similar possibility for the Council and the Parliament should be provided.

- ba) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 53 Absatz 1 Buchstaben e bis h und die Festsetzung von Geldbußen gemäß den Arikeln 79 und 79a;
- c) Überprüfung der praktischen Anwendung der unter den Buchstabe 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) Abgabe einer Stellungnahme für die Kommission zum Schutzniveau in Drittländern oder internationalen Organisationen;
- d) Abgabe von Stellungnahmen zu geplanten Maßnahmen von Aufsichtsbehörden gemäß dem in Artikel 57 genannten Kohärenzverfahren (...);
- 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 –verfahren mit Datenschutzaufsichtsbehörden in aller Welt.



2. Die Kommission kann, wenn sie den Europäischen Datenschutzausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist für die Erteilung eines solchen Rates setzen.
3. Der Europäische Datenschutzausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken an die Kommission und an den in Artikel 87 genannten Ausschuss weiter und veröffentlicht sie.
4. Die Kommission setzt den Europäischen Datenschutzausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die vom Europäischen Datenschutzausschuss herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Praktiken ergriffen hat.

#### *Artikel 67*

#### ***Berichterstattung***

1. Der Europäische Datenschutzausschuss informiert die Kommission in regelmäßigen Abständen (...) über die Ergebnisse seiner Tätigkeiten.
2. *Er erstellt einen jährlichen Bericht über (...) den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union und gegebenenfalls in Drittländern und internationalen Organisationen. 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.

*Artikel 68*

***Verfahrensweise***

1. Der Europäische Datenschutzausschuss trifft seine Beschlüsse mit einfacher Mehrheit seiner Mitglieder, es sei denn, dass gemäß Artikel 58 Absatz 7a eine Zweidrittelmehrheit erforderlich ist.
2. Der Europäische Datenschutzausschuss gibt sich eine Geschäftsordnung und legt seine Arbeitsweise fest. (...) <sup>488</sup>.

*Artikel 69*

***Vorsitz***

1. Der Europäische Datenschutzausschuss wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und zwei stellvertretende Vorsitzende (...) <sup>489</sup>
2. Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre einmalige Wiederwahl ist zulässig <sup>490</sup>.

---

<sup>488</sup> DE thought that the majorities by which further decisions shall be taken should be established by the EDPB itself

<sup>489</sup> COM reservation on deletion.

<sup>490</sup> Further to BE proposal. NL thought that also the case where a chair or a deputy chairperson ceases to be a member of the European Data Protection Board[/Committee], should be addressed by the Regulation. However, this may be left to national law of the Member state concerned. COM scrutiny reservation.

*Artikel 70*  
***Aufgaben des Vorsitzes***

1. Der Vorsitz hat folgende Aufgaben:
  - a) Einberufung der Sitzungen des Europäischen Datenschutzausschusses und Erstellung der Tagesordnungen;
  - 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 erhält ein Sekretariat. Dieses wird vom Europäischen Datenschutzbeauftragten gestellt <sup>491</sup>.
2. Das Sekretariat leistet dem Europäischen Datenschutzausschuss unter Leitung von dessen Vorsitz analytische, administrative und logistische Unterstützung.

---

<sup>491</sup> DE reservation on entrusting the EDPS with the EDPB secretariat. The risk of conflicts of interest of EDPS staff was also raised.

3. Das Sekretariat ist insbesondere verantwortlich für
- a) das Tagesgeschäft des Europäischen Datenschutzausschusses;
  - b) die Kommunikation zwischen den Mitgliedern des Europäischen Datenschutzausschusses, seinem Vorsitz und der Kommission sowie die Kommunikation mit anderen Organen und mit der Öffentlichkeit;
  - c) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation;
  - d) die Übersetzung sachdienlicher Informationen;
  - e) die Vor- und Nachbereitung der Sitzungen des Europäischen Datenschutzausschusses;
  - f) Vorbereitung, Entwurf und Veröffentlichung von Stellungnahmen und sonstigen vom Europäischen Datenschutzausschuss angenommenen Dokumenten.

*Artikel 72*

***Vertraulichkeit***<sup>492</sup>

- 1. Die Beratungen des Europäischen Datenschutzausschusses sind vertraulich.
- 2. Der Zugang zu den Mitgliedern des Europäischen Datenschutzausschusses, Sachverständigen und den Vertretern von Dritten vorgelegten Dokumenten wird durch die Verordnung (EG) Nr. 1049/2001 geregelt.

---

<sup>492</sup> DE, EE, ES, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this.

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

## KAPITEL VIII

### RECHTSBEHELFE, HAFTUNG UND SANKTIONEN <sup>493</sup>

#### *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 einzigsten Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.
2. In dem in Absatz 1 genannten Fall hat die betroffene Person das Recht, eine Einrichtung, eine Organisationen oder eine Vereinigung, die *nach dem Recht eines Mitgliedstaats gegründet ist* und zu deren Zielen der Schutz der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten gehört, zu beauftragen, in deren Namen Beschwerde zu erheben (...).
3. Unabhängig von dem Auftrag oder der Beschwerde einer betroffenen Person haben Einrichtungen, Organisationen oder Vereinigungen im Sinne des Absatzes 2 das Recht auf Beschwerde bei der zuständigen <sup>494</sup> Aufsichtsbehörde, wenn sie der begründeten Ansicht sind, dass der Schutz personenbezogener Daten gemäß Artikel 32 Absatz 1 verletzt wurde und Artikel 32 Absatz 3 keine Anwendung findet. <sup>495</sup>

---

<sup>493</sup> FR and EE scrutiny reservation.

<sup>494</sup> COM reservation on limitation to competent supervisory authority.

<sup>495</sup> BE reservation.

Artikel 74

***Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde*** <sup>496</sup>

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 Entscheidung einer Aufsichtsbehörde.
2. Eine betroffene Person hat unbeschadet eines anderweitigen administrativen oder außergerichtlichen Rechtsbehelfs das Recht auf einen gerichtlichen Rechtsbehelf, (...) wenn die Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 73 erhobenen Beschwerde in Kenntnis gesetzt hat.
3. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.
4. (...)
5. (...) <sup>497</sup>

Artikel 75

***Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter*** <sup>498</sup>

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.

---

<sup>496</sup> SI reservation.

<sup>497</sup> COM reservation on deletion of paragraphs 4 and 5.

<sup>498</sup> SI scrutiny reservation.

2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.
3. (...)
4. (...)

*Article 76*<sup>499</sup>

**Vertretung von betroffenen Personen**

1. Eine betroffene Person hat das Recht, eine Einrichtung, Organisation oder Vereinigung im Sinne des Artikels 73 Absatz 2 zu beauftragen, die in Artikel 74 und 75 genannten Rechte in ihrem Namen (...) wahrzunehmen.<sup>500</sup>
2. (...)
3. (...)
4. (...)
5. (...) <sup>501</sup>

---

<sup>499</sup> EE, PT and SI scrutiny reservation.

<sup>500</sup> DE parliamentary reservation; BE reservation.

<sup>501</sup> COM scrutiny reservation on deletion of paragraphs 3 to 5.



*Artikel 77*

***Haftung und Recht auf Schadenersatz***

1. Jede Person, der wegen einer Verarbeitung, die nicht mit dieser Verordnung zu vereinbaren ist, ein Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.
2. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter gesamtschuldnerisch für den gesamten Schaden; dies gilt unbeschadet des Artikels 24 Absatz 2..
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.

*Artikel 78*

***Sanktionen***

(...) <sup>502</sup>

---

<sup>502</sup> This Article was moved to Article 79b.

Artikel 79

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde ist befugt, gemäß diesem Artikel Geldbußen für Verstöße gegen diese Verordnung zu verhängen.  
Diese Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstatt von Maßnahmen nach Artikel 53 Absatz 1 verhängt.
2. Die gemäß Artikel 79a verhängten Geldbußen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.
  - 2a. Die Höhe der Geldbuße wird im Einzelfall unter gebührender Berücksichtigung folgender Elemente festgesetzt:
    - a) der Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung;
    - b) des vorsätzlichen oder fahrlässigen Charakters des Verstoßes,
    - c) der Zahl der betroffenen Personen, für die der Verstoß Folgen hatte, und des Ausmaßes des ihnen entstandenen Schadens;
    - d) der von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
    - e) des Grads 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) jedes früheren Verstoßes des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters;

- (g) der finanziellen Lage des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters, einschließlich der unmittelbar oder mittelbar durch den Verstoß erworbenen finanziellen Vorteile oder vermiedenen Verluste;
- h) der 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) des Umfangs der Zusammenarbeit mit der Aufsichtsbehörde während der Untersuchung des Verstoßes;
- j) der Einhaltung von genehmigten Verhaltensregeln oder genehmigten Zertifizierungsverfahren;
- k) ob ein Datenschutzbeauftragter benannt wurde;
- l) ob der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine öffentliche Behörde oder eine öffentliche Einrichtung ist;
- (m) jegliche anderen erschwerenden oder mildernden Umstände, die für den Einzelfall gelten.

3. (...) <sup>503</sup>

[3a. Ist gemäß Artikel 25 von einem für die Verarbeitung Verantwortlichen ein Vertreter benannt worden, so können unbeschadet aller Verfahren, die gegen den für die Verarbeitung Verantwortlichen eingeleitet werden können, Geldbußen gegen den Vertreter verhängt werden.]

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.

---

<sup>503</sup> COM reservation on deletion; linked to reservation on Article 79a.

4. Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel unterliegt angemessenen Verfahrensgarantien in Übereinstimmung mit dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren.

Artikel 79a

Geldbußen<sup>504</sup>

1. Die Aufsichtsbehörde kann eine Geldbuße, die [...] EUR oder im Fall eines Unternehmens [...] % seines gesamten (...) Jahresumsatzes 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 eine Gebühr (...) verlangt.
2. Die Aufsichtsbehörde kann eine Geldbuße, die [...] EUR oder im Fall eines Unternehmens [...] % seines gesamten (...) Jahresumsatzes nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig
- (c) der betroffenen Person die Auskünfte gemäß (...) den Artikeln 14 und 14a nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise erteilt;

---

<sup>504</sup> COM reservation on replacing ‘shall’ by ‘may’ and the deletion of amounts and percentages in paragraphs 1, 2 and 3.

- (d) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt, personenbezogene Daten nicht gemäß Artikel 16 berichtet oder die Rechte und Verpflichtungen gemäß den Artikeln 17, 17a, 17b, 19 oder 19 nicht wahrt bzw. einhält;
  - (e) (...);
  - (f) (...);
  - (g) die jeweilige Verantwortung der gemeinsam für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt hat;
  - (h) die Dokumentation gemäß Artikel 28 und Artikel 31 Absatz 4 nicht oder nicht hinreichend gewährleistet;
  - (i) (...)
3. Die Aufsichtsbehörde kann eine Geldbuße, die [...] EUR oder im Fall eines Unternehmens [...] % seines gesamten (...) Jahresumsatzes nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig
- a) personenbezogene Daten ohne oder ohne ausreichende 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 (...) Profiling nicht beachtet;
  - e) (...) 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;
  - f) unter Verstoß gegen Artikel 25 keinen Vertreter benennt;

- (g) unter Verstoß gegen Artikel 26 (...) personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;
- h) 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 oder nicht rechtzeitig oder nicht vollständig von einer solchen Verletzung benachrichtigt;
- i) unter Verstoß gegen Artikel 33 keine Datenschutz-Folgenabschätzung vornimmt oder personenbezogene Daten unter Verstoß gegen Artikel 34 ohne vorherige Zurateziehung der Aufsichtsbehörde verarbeitet;
- k) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht oder die in den Artikeln 38a und 39a festgelegten Bedingungen und Verfahren nicht einhält;
- (l) unter Verstoß gegen die Artikel 40 bis 44 eine Datenübermittlung an einen Empfänger in einem Drittland oder an eine internationale Organisation vornimmt oder anordnet;
- (m) einer Anweisung oder einem vorübergehenden oder endgültigen Verarbeitungsverbot oder einer Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1 nicht Folge leistet oder unter Verstoß gegen Artikel 53 Absatz 2 keinen Zugang gewährt.
- (n) (...)
- (o) (...)

4. [Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Höchstbeträge der in den Absätzen 1, 2 und 3 genannten Geldbußen unter Berücksichtigung der in Artikel 79 Absatz 2a aufgeführten Kriterien an die währungsspezifischen Entwicklungen anzupassen.]

*Artikel 79b*  
**Sanktionen**<sup>505</sup>

1. *Bei nicht in Artikel 79a genannten Verstößen gegen Bestimmungen dieser Verordnung 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.*

---

<sup>505</sup> This corresponds to Article 78 of the Commission proposal.

**KAPITEL IX**  
**VORSCHRIFTEN FÜR BESONDERE**  
**DATENVERARBEITUNGSSITUATIONEN**

*Artikel 80*

***Verarbeitung personenbezogener Daten und freie Meinungsäußerung***

1. In den Rechtsvorschriften der Mitgliedstaaten (...) wird das Recht auf den Schutz der Privatsphäre gemäß dieser Verordnung mit dem Recht auf die Freiheit der Meinungsäußerung, einschließlich der Verarbeitung personenbezogener Daten zu journalistischen Zwecke und zu künstlerischen oder literarischen Zwecken, in Einklang gebracht.
2. (...)

*Artikel 80a*

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

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



*Artikel 80b*

**Verarbeitung einer nationalen Kennziffer**

Die Mitgliedstaaten können bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. <sup>506</sup>

*Artikel 81*

**Verarbeitung personenbezogener Gesundheitsdaten**

1. Die Verarbeitung personenbezogener Gesundheitsdaten erfolgt in den Grenzen dieser Verordnung nach Maßgabe von Artikel 9 Absatz 2 Buchstabe h auf der Grundlage des Unionsrechts oder des Rechts des jeweiligen Mitgliedstaats, das geeignete, besondere Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht; sie muss notwendig sein
  - a) für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten, sofern die Verarbeitung dieser Daten durch dem Berufsgeheimnis unterliegendes ärztliches Personal erfolgt oder durch sonstige Personen, die nach dem Recht eines Mitgliedstaats, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, einer entsprechenden Geheimhaltungspflicht unterliegen oder
  - b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit unter anderem zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards unter anderem für Arzneimittel oder Medizinprodukte oder

---

<sup>506</sup> BE suggestion based on Article 8(7) of the 1995 Directive. COM reservation.

- c) aus anderen Gründen des öffentlichen Interesses in Bereichen wie der sozialen Sicherheit, insbesondere um die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Krankenversicherungsleistungen sicherzustellen.
2. Die Verarbeitung personenbezogener Gesundheitsdaten, die zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung unter anderem zur Erstellung von Patientenregistern zur Verbesserung der Diagnose sowie zur Unterscheidung zwischen ähnlichen Krankheitsarten und zur Vorbereitung von Studien zu Therapiezwecken erforderlich ist, unterliegt den Bedingungen und Garantien gemäß Artikel 83.
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit im Sinne des Absatzes 1 Buchstabe b näher auszuführen und um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.

## *Artikel 82*

### ***Datenverarbeitung im Beschäftigungskontext***

1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung per Gesetz die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext unter anderem 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 Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses regeln.

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 Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten für die in Absatz 1 genannten Zwecke festzulegen.

### *Artikel 83*

#### ***Datenverarbeitung zu historischen, statistischen oder wissenschaftlichen (...) Zwecken***

1. Personenbezogene Daten dürfen nur dann zu historischen, statistischen oder wissenschaftlichen (...) Zwecken verarbeitet werden, wenn
  - a) diese Zwecke nicht auf andere Weise durch die Verarbeitung von Daten erfüllt werden können, die eine Bestimmung der betroffenen Person nicht oder nicht mehr ermöglichen;
  - b) Daten, die die Zuordnung von Informationen zu einer bestimmten oder bestimmbar betroffenen Person ermöglichen, von den übrigen Informationen getrennt aufbewahrt werden, sofern diese Zwecke in dieser Weise erfüllt werden können.
- 1a. Die Bestimmungen und die Ausnahmen für historische, statistische und wissenschaftliche Zwecke in den Grenzen dieser Verordnung gelten nur unter der Voraussetzung, dass
  - a) die Daten über eine bestimmte Person nicht zur Unterstützung von Maßnahmen oder Entscheidungen gegenüber dieser Person verarbeitet werden,

b) die Daten nicht in einer Weise verarbeitet werden, durch die einer Person ein erheblicher Schaden oder eine erhebliche Beeinträchtigung zugefügt wird oder wahrscheinlich zugefügt wird <sup>507</sup>.

2. Personenbezogene Daten, die für historische, statistische oder wissenschaftliche (...) Zwecke verarbeitet werden, dürfen (...) nur dann veröffentlicht oder auf andere Weise öffentlich bekannt gemacht werden, wenn

a) die betroffene Person nach Maßgabe von Artikel 7 ihre Einwilligung erteilt hat,

b) die Veröffentlichung personenbezogener Daten für die Darstellung von Forschungsergebnissen oder zur Unterstützung der Forschung notwendig ist, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person diese Interessen nicht überwiegen oder

c) die betroffene Person die Daten veröffentlicht hat <sup>508</sup>.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verarbeitung personenbezogener Daten für die Zwecke der Absätze 1 und 2, etwaige erforderliche Beschränkungen der Rechte der betroffenen Person auf Unterrichtung und Auskunft sowie die unter diesen Umständen geltenden Bedingungen und Garantien für die Rechte der betroffenen Person festzulegen.

---

<sup>507</sup> Text proposed by the Statistics Working Party in 10428/12. COM reservation.

<sup>508</sup> NO thinks it is unclear whether the researcher according to paragraph 2 will need a new and separate legal ground for publishing material that has been collected for research purposes, even if the initial legal basis for processing specifically mentions publishing.

*Article 84*

**Geheimhaltungspflichten**

1. Die Mitgliedstaaten können in den Grenzen dieser Verordnung die Untersuchungsbefugnisse der Aufsichtsbehörden im Sinne des Artikels 53 Absatz 2 gegenüber den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeitern, die nach einzelstaatlichem Recht oder nach von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, 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, 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, richten eine unabhängige Datenschutzaufsicht im Sinne des Kapitels VI ein.

**KAPITEL X**  
**DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE** <sup>509</sup>

*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 8 Absatz 3, Artikel 9 (...), Artikel 39a Absatz 7, [Artikel 43 Absatz 3], (...), Artikel 79a Absatz 4, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 wird der Kommission auf unbestimmte Zeit ab Inkrafttreten dieser Verordnung übertragen.
3. Die Befugnisübertragung gemäß (...) Artikel 8 Absatz 3, (...) Artikel 39a Absatz 7, [Artikel 43 Absatz 3], (...), Artikel 79a Absatz 4, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. 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.

---

<sup>509</sup> COM reservation on the deletion of empowerments for delegated acts or implementing acts.

5. Ein delegierter Rechtsakt der gemäß (...) Artikel 8 Absatz 3, Artikel 9 Absatz 3, (...) Artikel 39a Absatz 7, [Artikel 43 Absatz 3], (...), Artikel 79a Absatz 4, Artikel 81 Absatz 3, Artikel 82 Absatz 3 und Artikel 83 Absatz 3 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um 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/EC***

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

*Artikel 89*

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

1. Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.
2. Artikel 1 Absatz 2 der Richtlinie 2002/58/EG wird gestrichen.



*Artikel 90*

***Bewertung***

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig einen Bericht zur Bewertung und Überprüfung dieser Verordnung vor. Der erste Bericht wird spätestens vier Jahre nach Inkrafttreten dieser Verordnung vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Die Kommission legt geeignete Vorschläge zur Änderung dieser Verordnung und zur Anpassung anderer Rechtsinstrumente vor, die sich insbesondere unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen können. Die Berichte werden veröffentlicht.

*Artikel 91*

***Inkrafttreten und Anwendung***

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

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

Geschehen zu Brüssel am

*Im Namen des Europäischen Parlaments*      *Im Namen des Rates*

*Der Präsident*

*Der Präsident*