Rat der
Europäischen Union

Brüssel, den 3. Oktober 2014
(OR. en)

13772/14

Interinstitutionelles Dossier:
2012/0011 (COD)

DATAPROTECT 129
JAI 730
MI 726
DRS 120
DAPIX 137
FREMP 164
COMIX 503
CODEC 1926

VERMERK

Absender:	Vorsitz
Empfänger:	Rat
Nr. Vordok.:	13212/4/14 REV 4 DATAPROTECT 109 JAI 630 MI 579 DRS 104 DAPIX 109 FREMP 148 COMIX 403 CODEC 1675
Betr.:	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) **[erste Lesung]** – Kapitel IV

1. Kapitel IV ist von der DAPIX-Gruppe im ersten Halbjahr 2013 eingehend erörtert worden. Auf der Tagung des Rates vom 6./7. Juni 2013 haben zwar alle Delegationen den irischen Vorsitz zu den sehr bedeutenden Fortschritten beglückwünscht, die hier erzielt worden sind, doch waren einige Fragen nach wie vor offen, insbesondere im Hinblick auf das Erfordernis, den Verwaltungsaufwand/die Befolgungskosten aufgrund dieser Verordnung weiter zu verringern, indem stärker auf den risikoorientierten Ansatz abgestellt wird.

2. Unter italienischem Vorsitz ist Kapitel IV in den DAPIX-Sitzungen vom 10./11. Juli und 11./12. September 2014 weiter erörtert worden. Die Delegationen haben auch schriftliche Bemerkungen übermittelt.[1] Weiterbehandelt wurde Kapitel IV in den Sitzungen der JI-Referenten vom 19., 22. and 29. September 2014 sowie auf den AStV-Tagungen vom 25. September und 1. Oktober 2014.

3. Der Vorsitz möchte den Delegationen für ihre konstruktive Mitarbeit aufrichtig danken. Nach Auffassung des Vorsitzes liegt als Ergebnis nun eine ausgewogene Überarbeitung des Kapitels IV vor.

4. Vor diesem Hintergrund ersucht der Vorsitz den Rat, eine partielle allgemeine Ausrichtung zu dem in der Anlage enthaltenen Text des Kapitels IV festzulegen, wobei von Folgendem ausgegangen wird:

   i. Die partielle allgemeine Ausrichtung wird unter der Voraussetzung festgelegt, dass nichts vereinbart ist, solange nicht alles vereinbart ist, und sie schließt künftige Änderungen am Text des Kapitels IV, die der Gesamtkohärenz der Verordnung dienen, nicht aus;

   ii. die partielle allgemeine Ausrichtung greift horizontalen Fragen nicht vor;

   iii. die partielle allgemeine Ausrichtung stellt kein Mandat für den Vorsitz dar, einen informellen Trilog mit dem Europäischen Parlament über den Text aufzunehmen.

_____

[1] Dok. 12267/2/14 REV 2 DATAPROTECT 107 JAI 625 MI 574 DRS 102 DAPIX 107 FREMP 146 COMIX 395 CODEC 1671. Die österreichische Delegation hat einen schriftlichen Beitrag verteilt: Dok. 13505/14 DATAPROTECT 124 JAI 700 MI 694 DRS 117 DAPIX 130 FREMP 159 COMIX 482 CODEC 1864.

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 müssen und nachweisen können, dass (...) die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen (...). Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die persönlichen Rechte und Freiheiten berücksichtigen.

(60a) Solche Risiken – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Datenverarbeitung hervorgehen, die zu einer physischen, materiellen oder moralischen Schädigung führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten [, einer Verletzung der (...) Pseudonymität][2] oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten oder Daten über Gesundheit oder Sexualleben oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert und prognostiziert werden, um ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft (...).

---

[2] Die in Kapitel IV enthaltene Verweisung auf die Nutzung pseudonymer Daten wird noch im Zusammenhang mit einer weiteren Diskussion über die Pseudonymisierung personenbezogener Daten zu erörtern sein.

(60b) *Eintrittswahrscheinlichkeit und Schwere des Risikos sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes*[3] *Risiko der Beeinträchtigung der persönlichen Rechte und Freiheiten (...).*

(60c) Anleitungen, wie der für die Verarbeitung Verantwortliche [oder Auftragsverarbeiter] geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Europäischen Datenschutzausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Europäische Datenschutzausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können. (…)

61) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden persönlichen Rechte und Freiheiten ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der für die Verarbeitung Verantwortliche interne Strategien festlegen und geeignete Maßnahmen ergreifen, die insbesondere dem Grundsatz des Datenschutzes durch Technik *(data protection by design)* und durch datenschutzfreundliche Voreinstellungen *(data protection by default)* Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, (...) personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Datenverarbeitung zu überwachen, und der für die Verarbeitung Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Auslegung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherstellen, dass die für die Verarbeitung Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

---

[3] Die Verwendung des Ausdrucks "besonderes" wurde von BE, CZ, ES und UK in Frage gestellt, nach deren Auffassung darin nicht die Schwere des Risikos im Falle des "hohen" Risikos zum Ausdruck kommt.

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

63) Jeder für die Verarbeitung Verantwortliche ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf in der Union ansässige betroffene Personen beziehen und dazu dienen, diesen Personen Waren oder Dienstleistungen anzubieten oder deren Verhalten in der Union zu beobachten, (...) sollte einen Vertreter benennen müssen, es sei denn, (...) *die von ihm ausgeführte Verarbeitung erfolgt* **vereinzelt** *und bringt unter Berücksichtigung ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke* **wahrscheinlich** k*ein Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich* **oder** bei dem für die Verarbeitung Verantwortlichen handelt es sich um eine Behörde oder öffentliche Einrichtung (...). Der Vertreter sollte im Namen des für die Verarbeitung Verantwortlichen tätig werden und den Aufsichtsbehörden als Ansprechpartner dienen. Der für die Verarbeitung Verantwortliche sollte den Vertreter ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln. Die Benennung eines solchen Vertreters berührt nicht die Verantwortung und Haftung des für die Verarbeitung Verantwortlichen nach Maßgabe dieser Verordnung. Der Vertreter sollte seine Aufgaben entsprechend dem Mandat des für die Verarbeitung Verantwortlichen ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des für die Verarbeitung Verantwortlichen sollte der bestellte Vertreter Durchsetzungsmaßnahmen unterworfen werden.

(63a) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des für die Verarbeitung Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein für die Verarbeitung Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. (...) Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des für die Verarbeitung Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats erfolgen, der den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind.

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden oder Bestandteil einer im Rahmen des Zertifizierungsverfahrens erteilten Zertifizierung sind. Nach Beendigung der Verarbeitung im Namen des für die Verarbeitung Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten zurückgeben oder löschen, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er unterliegt, eine Verpflichtung zur Speicherung der Daten besteht.

64) (…)

65) Zum Nachweis der Einhaltung dieser Verordnung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter Aufzeichnungen über alle Kategorien von Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder für die Verarbeitung Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Verlangen die entsprechenden Aufzeichnungen vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Unterlagen kontrolliert werden können.

66) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen (...) Risiken ermitteln und Maßnahmen zu ihrer Eindämmung ergreifen. Diese Maßnahmen müssen unter Berücksichtigung der verfügbaren Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. (…). Bei der Bewertung des Datensicherheitsrisikos sollten die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Weitergabe von beziehungsweise unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder moralischen Schaden führen könnte.

66a) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen, besser eingehalten wird, sollte der für die Verarbeitung Verantwortliche [oder Auftragsverarbeiter] für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche (...) geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der für die Verarbeitung Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

67) Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen (...) physischen, materiellen oder moralischen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung (...) ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, [Verletzung der (...) Pseudonymität,] Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile. (…). Deshalb sollte der für die Verarbeitung Verantwortliche nach Bekanntwerden einer (...) Verletzung des Schutzes personenbezogener Daten, die einen (...) physischen, materiellen oder moralischen Schaden nach sich ziehen kann, die Aufsichtsbehörde ohne 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 Rechte und Freiheiten durch die Datenschutzverletzung erheblich beeinträchtigt werden könnten, sollten ohne unangemessene Verzögerung benachrichtigt werden, damit sie die erforderlichen Vorkehrungen treffen können. (…). Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger negativer Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden (z.B. Strafverfolgungsbehörden) erteilten Weisungen erfolgen. (...) Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste sie sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen der Datensicherheit zu ergreifen.

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

(68a) Die Benachrichtigung der betroffenen Person von der Verletzung des Schutzes personenbezogener Daten sollte nicht erforderlich sein, wenn der für die Verarbeitung Verantwortliche geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Zu diesen technischen Sicherheitsvorkehrungen sollte zählen, dass die betreffenden Daten für alle Personen, die nicht zum Zugriff auf sie befugt sind, unverständlich gemacht werden, insbesondere durch Verschlüsselung der personenbezogenen Daten (...).

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

70) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat doch keineswegs in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, *ihrer Umstände* und ihrer Zwecke (...) wahrscheinlich ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen. Bei diesen Arten von Verarbeitungsvorgängen kann es sich um solche handeln, bei denen insbesondere neue Technologien eingesetzt werden oder die neuartig sind und bei denen der für die Verarbeitung Verantwortliche zuvor keine Datenschutz-Folgenabschätzung durchgeführt hat oder die in Anbetracht der seit der ursprünglichen Verarbeitung vergangenen Zeit notwendig geworden sind.[4]

[4] BE lehnt den Zeitbezug im letzten Teil des Satzes ab.

70a) In derartigen Fällen sollte der für die Verarbeitung Verantwortliche (...) vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, *der Umstände und* der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden und die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

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

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

73) Datenschutz-Folgeabschätzungen können von einer Behörde oder öffentlichen Einrichtung durchgeführt werden, sofern eine solche Folgenabschätzung nicht schon anlässlich des Erlasses des Gesetzes erfolgt ist, auf dessen Grundlage die Behörde oder Einrichtung ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt.

74) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ungeachtet geplanter Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen (...), und ist der für die Verarbeitung Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten von Datenverarbeitungen und einem bestimmtem Umfang und einer bestimmten Häufigkeit der Verarbeitung verbunden, die für die betroffenen Personen auch eine (...) Schädigung oder eine (...) Beeinträchtigung ihrer Rechte und Freiheiten mit sich bringen können. Sie sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Datenverarbeitung gemäß Artikel 33 durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die persönlichen Rechte und Freiheiten geplanten Maßnahmen.

(74a) Der Auftragsverarbeiter sollte erforderlichenfalls den für die Verarbeitung Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.

(74b) Eine Konsultation der Aufsichtsbehörde sollte auch während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften, in denen eine (...) Verarbeitung personenbezogener Daten vorgesehen ist, erfolgen, um die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.

75) In Fällen, in denen die Verarbeitung im öffentlichen Sektor oder durch ein privates Großunternehmen erfolgt oder in denen die Kerntätigkeit eines Unternehmens ungeachtet seiner Größe Verarbeitungsvorgänge einschließt, die einer regelmäßigen und systematischen Überwachung bedürfen, kann der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet der Datenschutzvorschriften und -verfahren verfügt, unterstützt werden. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich um Angestellte des für die Verarbeitung Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

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

76a) Bei der Ausarbeitung oder bei der Änderung oder Erweiterung solcher Verhaltensregeln sollten Verbände und oder andere Vereinigungen, die bestimmte Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, die einschlägigen interessierten Kreise, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.

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

KAPITEL IV

FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER[5]

ABSCHNITT 1
ALLGEMEINE PFLICHTEN

Artikel 22

Pflichten des für die Verarbeitung Verantwortlichen

(1) Der für die Verarbeitung Verantwortliche (...) führt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete Maßnahmen durch und muss den Nachweis dafür erbringen können, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden.

(2) (…)

(2a) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht[6], müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den für die Verarbeitung Verantwortlichen umfassen.

(2b) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 38 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des für die Verarbeitung Verantwortlichen nachzuweisen.

(3) (…)

(4) (…)

---

5 Prüfungsvorbehalt von SI und UK zum gesamten Kapitel. BE, DE, NL und UK sind von den von der KOM vorgelegten Zahlen nicht überzeugt, nach denen zusätzliche Verwaltungslasten und Befolgungskosten, die sich aus der vorgeschlagenen Verordnung ergeben, durch die Verringerung der Verwaltungslast aufgrund der Streichung der allgemeinen Meldepflicht der für die Verarbeitung Verantwortlichen ausgeglichen werden.

6 Nach Auffassung von HU, RO und PL räumt diese Formulierung den für die Verarbeitung Verantwortlichen zu viel Ermessensspielraum ein. AT ist der Auffassung, dass die Bezugnahme auf die Verhältnismäßigkeit insbesondere in Bezug auf die Einhaltung von Fristen problematisch ist.

Artikel 23

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

(1) (...) Die für die Verarbeitung Verantwortlichen treffen unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten und der *Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung* sowie der Schwere und Eintrittswahrscheinlichkeit dieser Risiken für die Rechte und Freiheiten natürlicher Personen der Verarbeitungstätigkeit und ihren Zielen angemessene technische und organisatorische Maßnahmen [einschließlich Minimierung und Pseudonymisierung[7]], durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und dass die Rechte (...) der betroffenen Personen (...) geschützt werden.

(2) Der für die Verarbeitung Verantwortliche wendet geeignete Maßnahmen an, die sicherstellen, dass durch Voreinstellung grundsätzlich nur (...) personenbezogene Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung (...) erforderlich[8] sind; (...) dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Besteht der Zweck der Verarbeitung nicht darin, der Öffentlichkeit Informationen zur Verfügung zu stellen, müssen diese Verfahren durch Voreinstellung sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne menschliches Eingreifen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

2a. Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 39 *kann als Faktor herangezogen werden,* um die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen nachzuweisen.

(3) (…)

(4) (…)

---

7 DE ist der Auffassung, dass im Hinblick auf Artikel 5 Buchstabe c der Grundsatz der Datensparsamkeit und -vermeidung sowie die Anonymisierung und Pseudonymisierung als wichtige Optionen für die Umsetzung aufgelistet werden sollten. Diese Debatte muss jedoch im Zusammenhang mit Beratungen zur Pseudonymisierung personenbezogener Daten geführt werden.

8 CZ würde "nicht unverhältnismäßig" bevorzugen. Dieser Begriff kann später im Zusammenhang mit den Beratungen zur Formulierung des Artikels 5 Absatz 1 Buchstabe c wieder geändert werden.

Artikel 24

Gemeinsam für die Verarbeitung Verantwortliche[9]

(1) Legen zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung personenbezogener Daten fest, so sind sie gemeinsam für die Verarbeitung Verantwortliche. (...) Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die (...) Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 14 und 14a nachkommt, sofern und soweit die jeweiligen Aufgaben der für die Verarbeitung Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die für die Verarbeitung Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung wird angegeben, welcher der gemeinsam für die Verarbeitung Verantwortlichen als einzige Anlaufstelle für die betroffenen Personen handeln soll, wenn es um die Ausübung ihrer Rechte geht.

(2) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der für die Verarbeitung Verantwortlichen geltend machen.

(3) Die Vereinbarung spiegelt die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam für die Verarbeitung Verantwortlichen gegenüber betroffenen Personen gebührend wider und der Kern der Vereinbarung wird den betroffenen Personen zur Verfügung gestellt. Absatz 2 gilt nicht, wenn die betroffene Person in transparenter und eindeutiger Form darüber informiert wurde, welcher der gemeinsam für die Verarbeitung Verantwortlichen zuständig ist, es sei denn, eine solche Vereinbarung – soweit es sich nicht um eine durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegte Vereinbarung handelt – ist im Hinblick auf die Rechte der betroffenen Person unbillig (...).

---

9 Vorbehalt SI; die Delegation warnt vor möglichen Rechtsstreitigkeiten in Bezug auf die Zuweisung der Haftung und ihrer Auffassung nach sollte dieser Artikel daher im Zusammenhang mit künftigen Beratungen zum Kapitel VIII noch weiter geprüft werden. Ferner ist FR der Auffassung, dass die Zuweisung der Haftung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter sehr wage ist, und CZ äußert Bedenken zur Durchsetzbarkeit dieser Bestimmung im privaten Sektor außerhalb von Vereinbarungen in einer Unternehmensgruppe und ist der Auffassung, dass ein Schutz gegen die Übertragung der Haftung vorgesehen werden sollte.

Artikel 25

Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen

(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der für die Verarbeitung Verantwortliche schriftlich einen Vertreter in der Union.

(2) Diese Pflicht gilt nicht für

(a) (…); oder

(b) eine Verarbeitung, die **gelegentlich**[10] erfolgt **und** *unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung (...) voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt;* oder

(c) Behörden oder öffentliche Einrichtungen;

(d) (…)

(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, ansässig sind.

(3a) Der Vertreter wird durch den für die Verarbeitung Verantwortlichen beauftragt, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.

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

[10] Vorbehalt von HU, SE und UK.

Artikel 26

Auftragsverarbeiter

(1) (…).[11] Der für die Verarbeitung Verantwortliche arbeitet nur mit Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt (...).

(1a) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch. Im letzteren Fall sollte der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen immer über jede vorgesehene Änderung in Bezug auf die Hinzufügung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch der für die Verarbeitung Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einwand zu erheben[12].

(1b) (…)[13].

(2) Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines rechtlichen Akts **nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats**, der den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien von betroffenen Personen (...) und die Rechte des Auftragsverarbeiters festgelegt sind und insbesondere vorgesehen ist, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeitet, sofern er nicht durch das Unionsrecht oder das Recht des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem für die Verarbeitung Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung der Daten mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

---

11 Der Vorsitz schlägt vor, in Artikel 5 Absatz 2 die Formulierung "auch wenn personenbezogene Daten in seinem Namen von einem Auftragsverarbeiter verarbeitet werden" zu ergänzen. Diesbezüglich können auch weitere Beratungen im Rahmen künftiger Beratungen zur Haftung im Zusammenhang mit Kapitel VIII notwendig werden.

12 LU und FI haben Bedenken, dass dies einen unzulässigen Eingriff in die Vertragsfreiheit darstellen könnte.

13 Mehrere Delegationen (CZ, AT, LU) weisen auf die Notwendigkeit einer Angleichung an die Bestimmungen des Artikels 77 hin. Beratungen zur Ausübung der Rechte der betroffenen Personen sollte im Zusammenhang mit Kapitel VIII erfolgen.

b) (…)

c) alle gemäß Artikel 30 erforderlichen Maßnahmen ergreift;

d) die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters (...) einhält, wie etwa die Anforderung, dass der für die Verarbeitung Verantwortliche diese zuvor ausdrücklich genehmigt haben muss;

e) angesichts der Art der Verarbeitung (...) den für die Verarbeitung Verantwortlichen dabei unterstützt, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) (…) den für die Verarbeitung Verantwortlichen bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;

g) die personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen, die in dem Vertrag oder dem sonstigen rechtlichen Akt angegeben sind, zurückgibt bzw. löscht – nach Wahl des für die Verarbeitung Verantwortlichen –, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der Daten besteht;

h) dem für die Verarbeitung Verantwortlichen (...) alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen, die vom für die Verarbeitung Verantwortlichen durchgeführt werden, ermöglicht und dazu beiträgt.

Der Auftragsverarbeiter informiert den für die Verarbeitung Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(2a) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des für die Verarbeitung Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter *im Wege eines Vertrags oder eines anderen rechtlichen Akts nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats* [14] dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen rechtlichen Akt zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 2 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die entsprechenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(2aa) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 oder eines *genehmigten Zertifizierungsverfahrens gemäß Artikel 39*[15] *durch den Auftragsverarbeiter* kann als Faktor herangezogen werden, *um hinreichende Garantien im Sinne der Absätze 1 und 2a* nachzuweisen.

(2ab) Unbeschadet eines individuellen Vertrags zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder der andere rechtliche Akt im Sinne der Absätze 2 und 2a ganz oder teilweise auf den in den Absätzen 2b und 2c genannten Standardvertragsklauseln oder aber auf Standardvertragsklauseln beruhen, die Bestandteil einer dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 39 und 39a erteilten Zertifizierung sind.

---

14 HU schlägt zur näheren Bestimmung dieser Bezugnahme auf das Unionsrecht oder das Recht des Mitgliedstaats vor, die Formulierung "durch den dieser weitere Auftragsverarbeiter an den ersten Auftragsverarbeiter gebunden ist" hinzuzufügen.

15 Vorbehalt von FR; SK schlägt vor zu präzisieren, dass der Auftragsverarbeiter bei Nichterfüllung der Datenschutzpflichten durch den weiteren Auftragsverarbeiter im Rahmen eines solchen Vertrags oder anderen rechtlichen Akts weiterhin in vollem Umfang gegenüber dem für die Verarbeitung Verantwortlichen für die Leistung der Pflichten des weiteren Auftragsverarbeiters haftet. Wird es dem Auftragsverarbeiter ermöglicht, Unteraufträge zu vergeben, ohne den Unterauftragsverarbeiter zu einem Vertragsverhältnis mit dem für die Verarbeitung Verantwortlichen zu verpflichten, so sollte für den für die Verarbeitung Verantwortlichen ausreichend Rechtssicherheit in Bezug auf die Haftung gewährleistet werden. Der Grundsatz der Haftung des Hauptauftragsverarbeiters für jegliche Verstöße durch den Unterauftragsverarbeiter ist in der Klausel 11 der Standardvertragsklauseln 2010/87 und in den unternehmensinternen Datenschutzvorschriften für Auftragsverarbeiter festgelegt und ist damit der derzeitige Standard. SK schlägt außerdem vor, die Bezugnahme auf Artikel 69 zu streichen.

(2b) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 2 und 2a genannten Fragen festlegen[16].

(2c) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 57 Standardvertragsklauseln zur Regelung der in den Absätzen 2 und 2a genannten Fragen festlegen.

3. Der Vertrag oder der andere rechtliche Akt im Sinne der Absätze 2 und 2a ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

4. (…)

5. (…)[17]

Artikel 27

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

(…),

[16] PL äußert sich besorgt über ein Szenario, bei dem die Kommission nicht handeln würde. CY und FR sind dagegen, diese Funktion der KOM zu übertragen (FR könnte möglicherweise akzeptieren, dass dies der Europäische Datenschutzausschuss übernimmt).

[17] Vorbehalt von KOM zur Streichung.

Artikel 28

Aufzeichnungen zu den Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten[18]

(1) Alle für die Verarbeitung Verantwortlichen (...) und gegebenenfalls ihre Vertreter führen eine Aufzeichnung zu allen Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten, die ihrer Zuständigkeit unterliegen. Diese Aufzeichnung enthält folgende Angaben:

a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen und etwaiger gemeinsam mit ihm Verantwortlicher (...), des Vertreters des für die Verarbeitung Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) (…)

c) Angaben über die Zwecke der Verarbeitung einschließlich des berechtigten Interesses, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet;

d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;

e) die (...) Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern;

f) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation (...);

g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien.

h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.

---

18 Prüfungsvorbehalt AT.

(2a) Jeder Auftragsverarbeiter führt eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten, die Folgendes enthält:

a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes für die Verarbeitung Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Vertreters des für die Verarbeitung Verantwortlichen;

b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;

c) die Kategorien von Verarbeitungen, 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.

e) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.

(3a) Die in den Absätzen 1 und 2a genannten Aufzeichnungen sind schriftlich zu führen; dies schließt elektronische oder andere ohne technische Vermittlung nicht lesbare Formate, die in ein lesbares Format umgewandelt werden können, ein.

(3) Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen der Aufsichtsbehörde die Aufzeichnung (...) auf Anforderung zur Verfügung.

(4) Die in den Absätzen 1 und 2a genannten Pflichten gelten nicht für:

a) (…); oder

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

(5) (…)

(6) (…)

Artikel 29

Zusammenarbeit mit der Aufsichtsbehörde

(…)

ABSCHNITT 2
DATENSICHERHEIT

Artikel 30

Sicherheit der Verarbeitung

(1) Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung der verfügbaren Technologie, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Wahrscheinlichkeit und der Höhe des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen, [einschließlich **(...)** der Pseudonymisierung personenbezogener Daten,] um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(1a) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, (...) die mit der Datenverarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Weitergabe von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, – verbunden sind.

(2) (…)

(2a) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 kann als Faktor herangezogen werden, *um die Erfüllung der in Absatz 1 genannten Anforderungen nachzuweisen*.

(2b) Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, sofern sie keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedstaatlichen Recht erwachsenden Pflichten unterliegen.

(3) (…)

(4) (…)

Artikel 31

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde[19]

(1) Bei einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, [Verletzung der (...) Pseudonymität], Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, meldet der für die Verarbeitung Verantwortliche der gemäß Artikel 51 zuständigen Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung und nach Möglichkeit binnen 72 Stunden nach Feststellung der Verletzung. Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen.

(1a) Eine Meldung gemäß Absatz 1 muss nicht erfolgen, wenn eine Benachrichtigung der betroffenen Person gemäß Artikel 32 Absatz 3 Buchstaben a und b nicht erforderlich ist.[20]

(2) (...) Nach Feststellung einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter diese dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung.

---

19 Prüfungsvorbehalt von AT und SI. Vorbehalt von KOM: Die Kohärenz mit der Datenschutzrichtlinie für elektronische Kommunikation sollte gewahrt werden; nach Auffassung von SI könnte dies dadurch erreicht werden, dass in den Artikeln 31 und 32 das Wort "hohes" vor "Risiko" gestrichen wird.

20 Nach Auffassung von BE, AT und PL sollte dieser Absatz gestrichen werden.

(3) Die in Absatz 1 genannte Meldung enthält mindestens folgende Informationen:

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

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

c) (…)

d) eine Beschreibung der wahrscheinlichen Folgen der von dem für die Verarbeitung Verantwortlichen festgestellten Verletzung des Schutzes personenbezogener Daten;

e) eine Beschreibung der von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und

f) gegebenenfalls eine Angabe von Maßnahmen zur Eindämmung etwaiger nachteiliger Auswirkungen der Verletzung des Schutzes personenbezogener Daten.

3a) Wenn und soweit die in Absatz 3 Buchstaben d, e und f genannten Informationen nicht zur gleichen Zeit wie die in Absatz 3 Buchstaben a und b genannten bereitgestellt werden können, stellt der für die Verarbeitung Verantwortliche diese Informationen ohne 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. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. (…)

(5) (…)

(6) (….)[21]

[21] Vorbehalt von KOM zur Streichung.

Artikel 32

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person[22]

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, [Verletzung der (...) Pseudonymität,] Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, so benachrichtigt der für die Verarbeitung Verantwortliche (...) die betroffene Person ohne unangemessene Verzögerung von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 31 Absatz 3 Buchstaben b, e und f genannten Informationen und Empfehlungen.

(3) Die Benachrichtigung der betroffenen Person (...) gemäß Absatz 1 ist nicht erforderlich, wenn

a. der für die Verarbeitung Verantwortliche (...) geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die betreffenden Daten für alle Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht werden, etwa durch Verschlüsselung; oder

b. der für die Verarbeitung Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht; oder

c. dies insbesondere angesichts der Zahl der betroffenen Fälle mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesen Fällen hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden; oder

[22] Prüfungsvorbehalt von AT. Vorbehalt von KOM: Die Kohärenz mit der Datenschutzrichtlinie für elektronische Kommunikation sollte gewahrt werden.

d. sie ein wichtiges öffentliches Interesse beeinträchtigen würde.

(4) (…)

(5) (…)

(6) (…)[23]

ABSCHNITT 3
DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION

Artikel 33

Datenschutz-Folgenabschätzung [24]

(1) Wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes[25] Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, [Verletzung der **(...)** Pseudonymität,] Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, führt der für die Verarbeitung Verantwortliche (...)[26] vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (…).

(1a) Der für die Verarbeitung Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

---

23 Vorbehalt von KOM zur Streichung.

24 FR, HU, AT und KOM äußerten Zweifel am Begriff der neuen Formen der Verarbeitung, der jetzt in Erwägungsgrund 70 präzisiert worden ist. Nach Auffassung von UK sollte diese Verpflichtung nicht gelten, wenn ein überwiegendes öffentliches Interesse an der Datenverarbeitung (etwa eine gesundheitliche Krisensituation) besteht.

25 FR, RO, SK und UK warnen vor dem erheblichen Verwaltungsaufwand, zu dem die vorgeschlagene Verpflichtung führen würde. Nach Auffassung von UK sollte jegliche Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung auf diejenigen Fälle beschränkt werden, in denen ein hohes Risiko für die Rechte der betroffenen Personen ausgemacht wurde.

26 Vorbehalt von KOM zur Streichung.

(2) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, (...) die sich auf Profiling gründet und die ihrerseits als Grundlage für Entscheidungen[27] dient, welche Rechtswirkung gegenüber betroffenen Personen entfalten oder erhebliche Auswirkungen für diese mit sich bringen;

b) Verarbeitung spezieller Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 (...)[28], biometrischen Daten oder Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln, wenn die Daten in großem Umfang im Hinblick auf Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen;

c) *weiträumige* Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen (...);

d) (…)

e) (…)[29].

(2a) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss. [30]

---

27 Die Formulierung soll künftig gegebenenfalls an den Wortlaut des Artikels 20 angepasst werden.

28 HU schlägt vor, auch die Daten zu Kindern wieder aufzunehmen.

29 Prüfungsvorbehalt von FR. Nach Auffassung von PL könnte der Europäische Datenschutzausschuss hier eine Funktion übernehmen, um festzustellen, welche Verarbeitungsvorgänge mit einem hohen Risiko einhergehen.

30 Vorbehalt von CZ. HU fragt sich, welche rechtlichen Auswirkungen es gegebenenfalls auf laufende Verarbeitungsvorgänge hätte, wenn eine Datenschutzaufsichtsbehörde eine Form der Verarbeitung in diese Liste aufnehmen würde, und welcher räumliche Geltungsbereich betroffen wäre. Nach Auffassung des Vorsitzes sollte die Rolle, die der Europäische Datenschutzausschuss in diesem Zusammenhang gegebenenfalls spielen könnte, im Rahmen des Kapitels VII erörtert werden.

(2b) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss.

(2c) Vor Festlegung der in den Absätzen 2a und 2b genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 57 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten. [31]

(3) Die Folgenabschätzung enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung des Risikos, auf das in Absatz 1 Bezug genommen wird, sowie der geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.[32]

3a. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 durch die zuständigen für die Verarbeitung Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Rechtmäßigkeit und der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgängen, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.[33]

(4) *Der für die Verarbeitung Verantwortliche holt die Meinung der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung* unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge (...)[34] *ein*.

---

31 Vorbehalt von CZ.

32 Prüfungsvorbehalt von FR.

33 Nach Auffassung von HU sollte dieser Passus in einen Erwägungsgrund aufgenommen werden.

34 CZ und FR geben zu bedenken, dass es sich hierbei um eine völlig undurchführbare Verpflichtung handelt; Vorbehalt von IE.

(5) Falls (...) die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, beruht und falls die betreffenden Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln[35], gelten die Absätze 1 bis 3 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(6) (…)

(7) (…)

Artikel 34

Vorherige (...) Konsultation[36]

(1) (…)

(2) Der für die Verarbeitung Verantwortliche (...)[37] zieht vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate (...), wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 33 hervorgeht, dass die Verarbeitung ein (...) hohes Risiko zur Folge hätte, sofern *der für die Verarbeitung Verantwortliche* keine Maßnahmen zur Eindämmung des Risikos *trifft*.

---

35 BE und SI erklärten, dieser Passus werde im Rahmen der künftigen Diskussion über die Möglichkeiten der Einbeziehung des öffentlichen Sektors in den Geltungsbereich der Verordnung nochmals geprüft werden müssen.

36 Prüfungsvorbehalt von HU; Vorbehalt von SK zur Übertragung dieser Funktion auf die Datenschutzaufsichtsbehörden, die unter Umständen nicht in allen Fällen in der Lage seien, sich mit diesen Konsultationen zu befassen. ES schlägt vor, die für die Verarbeitung Verantwortlichen von der Pflicht zur vorherigen Konsultation auszunehmen, sofern sie einen Datenschutzbeauftragten benannt haben.

37 Vorbehalt von KOM und LU zur Streichung des Auftragsverarbeiters.

(3) Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 2 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der für die Verarbeitung Verantwortliche *das Risiko* nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem für die Verarbeitung der Daten Verantwortlichen spätestens sechs Wochen nach dem Antrag auf Konsultation schriftlich entsprechende Empfehlungen und kann ihre in Artikel 53 genannten Befugnisse ausüben (...)[38]. Diese Frist kann angesichts der Komplexität der geplanten Verarbeitung um weitere sechs Wochen verlängert werden. Kommt es zu einer Fristverlängerung, wird der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter innerhalb eines Monats nach Eingang des Antrags über die Gründe für die Verzögerung informiert.

(4) (…)

(5) (…)

(6) Der für die Verarbeitung Verantwortliche (...) stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 2 (...) folgende Informationen zur Verfügung:

a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des für die Verarbeitung Verantwortlichen, der gemeinsam für die Verarbeitung Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;

d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 33 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen (...).

---

38 Vorbehalt von UK, der zufolge die Befugnis, Verarbeitungsvorgänge zu untersagen, nicht in Zeiten gelten sollte, in denen ein überwiegendes öffentliches Interesse an der Datenverarbeitung (etwa eine gesundheitliche Notlage) besteht. Nach Auffassung des Vorsitzes sollte dieser Punkt allerdings im Zusammenhang mit Kapitel VI zu den Befugnissen der Datenschutzaufsichtsbehörde erörtert werden, da diese offensichtlich ungeachtet jeglicher Konsultation ausgeübt werden können.

(7) Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzesvorschriften oder von auf solchen Gesetzesvorschriften basierenden Regelungsvorschriften zu Rate, die die Verarbeitung personenbezogener Daten vorsehen (...)[39].

(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[40].

(8) (…)

(9) (…)

[39] Prüfungsvorbehalt von IE zu dieser Streichung.
[40] Prüfungsvorbehalt von SE.

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 –[41] einen Datenschutzbeauftragten benennen (...).

(2) Eine Gruppe von Unternehmen darf einen gemeinsamen Datenschutzbeauftragten ernennen.

(3) Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Einrichtung handelt, kann für mehrere solcher Behörden oder Einrichtungen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

(4) (…)

(5) Der (...) Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt , das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben, namentlich des Nichtvorhandenseins von Interessenkonflikten. (…)

(6) (…)

(7) (…). Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 37 nicht mehr erfüllt, außer es liegen schwerwiegende Gründe nach dem Recht des betreffenden Mitgliedstaats vor, die eine Entlassung eines Beschäftigten oder Bediensteten rechtfertigen.

---

41 Wurde aufgrund eines Beschlusses des Rates fakultativ ausgestaltet. Prüfungsvorbehalt von AT. DE, HU und AT hätten es vorgezogen, wenn die Fälle einer obligatorischen Benennung des Datenschutzbeauftragten in der Verordnung selbst festgelegt worden wären, und möchten eventuell zu einem späteren Zeitpunkt auf diese Frage zurückkommen. Vorbehalt von KOM zur fakultativen Benennung und zur Streichung der Buchstaben a bis c.

(8) Der Datenschutzbeauftragte kann Beschäftigter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(9) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

(10) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(11) (…)

Artikel 36

Stellung des Datenschutzbeauftragten

(1) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 37 und stellt (...) die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung.

(3) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben unabhängig handeln kann und keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters.

(4) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Artikel 37

Aufgaben des Datenschutzbeauftragten

(1) Dem (...) Datenschutzbeauftragten obliegen (...) folgende Aufgaben:

a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten (...);

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten sowie der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) (…),

d) (…),

e) (…),

f) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 33;

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

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

(2) (…),

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

ABSCHNITT 5
VERHALTENSREGELN UND ZERTIFIZIERUNG

Artikel 38
Verhaltensregeln [42]

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche und der besonderen Bedürfnisse von Kleinst-, Klein- und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

(1a) Verbände und andere Vereinigungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, damit die Anwendung von Bestimmungen dieser Verordnung beispielsweise in Bezug auf folgende Aspekte präzisiert wird:

a) faire und transparente Datenverarbeitung;

aa) die berechtigten Interessen des für die Verarbeitung Verantwortlichen in bestimmten Zusammenhängen;

b) Datenerhebung;

bb) Pseudonymisierung personenbezogener Daten;

c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;

d) Ausübung der Rechte betroffener Personen;

e) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Zustimmung der Eltern oder des Vormundes einzuholen ist;

(ee) Maßnahmen und Verfahren gemäß den Artikeln 22 und 23 und Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 30;

---

[42] Vorbehalt von AT, FI, SK und PL.

(ef) Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und Benachrichtigung der betroffenen Person von solchen Verletzungen;

f) (…)

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

(1b) Die Verhaltensregeln sehen Verfahren vor, die es der in Artikel 38a Absatz 1 genannten Stelle ermöglichen, die obligatorische[43] Überwachung der Einhaltung ihrer Bestimmungen durch die für die Verarbeitung Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen, unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde, die nach Artikel 51 oder 51a zuständig ist.

(2) Verbände und andere Vereinigungen gemäß Absatz 1a, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, legen den Entwurf der Verhaltensregeln der Aufsichtsbehörde vor, die nach Artikel 51 zuständig ist. Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf der Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind und genehmigt diesen Entwurf oder diese geänderten oder erweiterten Verhaltensregeln, wenn sie der Auffassung ist, dass er/sie ausreichende geeignete Garantien bietet/bieten.

(2a) Wird durch die Stellungnahme nach Absatz 2 bestätigt, dass die Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar sind, so werden die Verhaltensregeln genehmigt, und beziehen sich die Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht die Einzelheiten der Verhaltensregeln.

---

43 CZ zieht eine fakultative Überwachung vor.

(2b) Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die nach Artikel 51 zuständige Aufsichtsbehörde ihn – vor Genehmigung – nach dem Verfahren gemäß Artikel 57 dem Europäischen Datenschutzausschuss vor, der zu der Frage Stellung nimmt, ob der Entwurf der Verhaltensregeln oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind oder – im Fall nach Absatz 1ab – geeignete Garantien vorsieht/vorsehen[44].

(3) Wird durch die Stellungnahme nach Absatz 2b bestätigt, dass der Entwurf oder die geänderten oder erweiterten Verhaltensregeln mit dieser Verordnung vereinbar ist/sind oder – im Fall nach Absatz 1ab – geeignete Garantien vorsieht/vorsehen, so übermittelt der Europäische Datenschutzausschuss seine Stellungnahme der Kommission.

(4) Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen genehmigten Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender genehmigter Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.

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

(5a) Der Europäische Datenschutzausschuss nimmt alle genehmigten Verhaltensregeln beziehungsweise Änderungen daran in ein Register auf und veröffentlicht sie in geeigneter Weise, z.B. über das Europäische E-Justiz-Portal.

---

[44] FR legte einen Vorschlag für einen Absatz 2c vor: 'Genehmigte Verhaltensregeln nach Absatz 2a stellen ein Element des vertraglichen Verhältnisses zwischen dem für die Verarbeitung Verantwortlichen und der betroffenen Person dar. Ist in den Verhaltensregeln festgelegt, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter diese Verordnung einzuhalten hat, so sind sie rechtsverbindlich und durchsetzbar.'

Artikel 38a

Überwachung der genehmigten Verhaltensregeln[45]

1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 38 Absatz 1b von einer Stelle durchgeführt werden[46], die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde.

2. Eine Stelle gemäß Absatz 1 kann zu diesem Zweck akkreditiert werden, wenn

   (a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

   (b) sie Verfahren festgelegt hat, die es ihr ermöglichen, zu bewerten, ob für die Verarbeitung Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der Verhaltensregeln durch die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter zu überwachen und die Anwendung der Verhaltensregeln regelmäßig zu überprüfen;

   (c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;

   (d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

---

45 Prüfungsvorbehalt von AT und LU.

46 CZ, ES und LU lehnen es ab, dass diese Rolle derart getrennten Stellen übertragen wird. Es wurden Bedenken u.a. hinsichtlich des Verwaltungsaufwands, der durch die Einrichtung dieser Stellen entsteht, geäußert. Die Verhaltensregeln sind ein gänzlich freiwilliger Mechanismus, an dem sich kein für die Verarbeitung Verantwortlicher beteiligen muss.

3. Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 57 an den Europäischen Datenschutzausschuss.

4. Unbeschadet des Kapitels VIII kann eine Stelle gemäß Absatz 1 vorbehaltlich angemessener Garantien im Falle einer Verletzung der Verhaltensregeln durch einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter geeignete Maßnahmen ergreifen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters von den Verhaltensregeln. Sie unterrichtet die zuständige Aufsichtsbehörde über solche Maßnahmen und 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.

6. Dieser Artikel gilt nicht für die Verarbeitung personenbezogener Daten durch Behörden oder öffentliche Einrichtungen.

Artikel 39

Zertifizierung[47]

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

[47] Prüfungsvorbehalt von AT, FR und FI. FR hält die verwendete Terminologie für unklar; der Datenschutzbeauftragte sollte in der Lage sein, die Einhaltung der zertifizierten Datenschutzmaßnahmen zu überprüfen, was in Artikel 53 präzisiert werden sollte.

(1a) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 2a *genehmigt* worden sind, vorgesehen werden, um nachzuweisen, dass die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 42 Absatz 2 Buchstabe e geeignete Garantien bieten. Diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher Instrumente oder auf andere Weise die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.

(2) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörde, die gemäß Artikel 51 oder 51a zuständig ist.

(2a) Eine Zertifizierung nach diesem Artikel wird *durch die* Zertifizierungs*stellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde* anhand der von der zuständigen Aufsichtsbehörde genehmigten Kriterien oder – *gemäß Artikel 57* – durch den Europäischen Datenschutzausschuss erteilt[48].

(3) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 39a *oder gegebenenfalls der zuständigen Aufsichtsbehörde* alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.

(4) Die Zertifizierung wird einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die einschlägigen Voraussetzungen weiterhin erfüllt werden. Sie wird durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

---

48 Unbeschadet der künftigen Erörterung über die genauen Befugnisse des Europäischen Datenschutzausschusses. Diese Erörterung wird in Verbindung mit der Erörterung über das Prinzip der zentralen Kontaktstelle ("one-stop-shop mechanism) stattfinden.

(5) Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z.B. über das Europäische E-Justiz-Portal.

Artikel 39a

Zertifizierungsstelle und -verfahren[49]

(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat teilt mit, ob diese Zertifizierungsstellen akkreditiert wurden von[50]

(a) der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde und/oder

(b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.

(2) Die Zertifizierungsstelle nach Absatz 1 kann zu diesem Zweck nur akkreditiert werden, wenn

(a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;

---

49 Prüfungsvorbehalt von AT, FR und LU.

50 Prüfungsvorbehalt von BE.

aa) sie sich verpflichtet hat, die Kriterien *nach Artikel 39 Absatz 2a*, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – von dem Europäischen Datenschutzausschuss genehmigt wurden, einzuhalten;

(b) sie Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzsiegel und -prüfzeichen festgelegt hat;

(c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht;

(d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die Akkreditierung der Zertifizierungsstellen nach Absatz 1 erfolgt anhand der Kriterien, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder, *gemäß Artikel 57*, von dem Europäischen Datenschutzausschuss genehmigt wurden[51]. *Im Fall einer Akkreditierung nach Absatz 1 Buchstabe b ergänzen diese Anforderungen diejenigen, die in der Verordnung 765/2008 und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.*

(4) Die Zertifizierungsstelle nach Absatz 1 ist unbeschadet der Verantwortung, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die Stelle die Anforderungen erfüllt.

(5) Die Zertifizierungsstelle nach Absatz 1 teilt der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

---

51 Unbeschadet der künftigen Erörterung über die genauen Befugnisse des Europäischen Datenschutzausschusses. Diese Erörterung wird in Verbindung mit der Erörterung über das Prinzip der zentralen Kontaktstelle ("one-stop-shop mechanism) stattfinden.

(6) Die Anforderungen nach Absatz 3 und die Kriterien nach Artikel 39 Absatz 2a *werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht*. Die Aufsichtsbehörde übermittelt diese auch dem Europäischen Datenschutzausschuss. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z.B. über das Europäische E-Justiz-Portal.

(6a) Unbeschadet der Bestimmungen des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind[52].

(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].

(7a) Der Europäische Datenschutzausschuss gibt der Kommission gegenüber eine Stellungnahme zu den Kriterien und Anforderungen, auf die in Absatz 7 Bezug genommen wird, ab[53].

(8) Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen festlegen. Die betreffenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen[54].

---

52 CZ, FR und HU: Allerdings sollte die nationale Akkreditierungsstelle die Datenschutzbehörde immer konsultieren, bevor sie eine Zertifizierungsstelle akkreditiert.

53 Unbeschadet der künftigen Erörterung über die genauen Befugnisse des Europäischen Datenschutzausschusses. Diese Erörterung wird in Verbindung mit der Erörterung über das Prinzip der zentralen Kontaktstelle ("one-stop-shop mechanism") stattfinden.

54 DE plädiert für eine Streichung der letzten beiden Absätze aus und schlägt folgenden neuen Absatz vor: "Die vorstehenden Absätze berühren nicht die Bestimmungen über die Verantwortung der nationalen Zertifizierungsstellen, die Akkreditierungsverfahren und die Spezifizierung der Kriterien für Sicherheit und Datenschutz. Die Befugnis der Kommission zum Erlass von Rechtsakten nach den Absätzen 7 und 8 betrifft nicht die auf dieser Grundlage durchgeführten nationalen und internationalen Zertifizierungsverfahren. Sicherheitsbescheinigungen, die von den zuständigen Stellen oder von Stellen, die von den zuständigen Stellen im Rahmen dieser Verfahren akkreditiert worden sind, ausgestellt werden, werden gegenseitig anerkannt." ES war auch der Auffassung, dass dies nicht ausschließlich der Kommission überlassen werden sollte.