RAT DER EUROPÄISCHEN UNION

Brüssel, den 28. Mai 2014

10349/14

Interinstitutionelles Dossier: 2012/0011 (COD)

DATAPROTECT 85
JAI 375
MI 467
DRS 74
DAPIX 73
FREMP 106
COMIX 292
CODEC 1384

VERMERK

des	Vorsitzes
für den	Rat
Nr. Vordok.:	9865/2/14 REV 2 DATAPROTECT 71 JAI 312 MI 425 DRS 68 DAPIX 64 FREMP 90 COMIX 263 CODEC 1294
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) – Partielle allgemeine Ausrichtung zu Kapitel V

Hintergrund

1. Grenzüberschreitende Informationsflüsse gehören ganz selbstverständlich zur heutigen globalisierten und vernetzten Welt; daher ist es erforderlich, die Verordnung anzupassen, um mit diesen Entwicklungen Schritt zu halten und um die Aufrechterhaltung des umfassenden Schutzes sicherzustellen, den natürliche Personen in der EU genießen, sowohl wenn sie zum Ziel von außerhalb der EU niedergelassenen Unternehmen werden, als auch wenn ihre personenbezogenen Daten an Drittstaaten oder internationale Organisationen weitergegeben werden. Während der informellen Gespräche, die im Januar 2014 in Athen geführt worden sind, und auf der Tagung des JI-Rates im März 2014 haben die Minister Fragen der internationalen Dimension der Datenschutzreform erörtert.

Bei den informellen Gesprächen im Januar 2014 in Athen haben die Minister ihre allgemeine Zufriedenheit mit den Bestimmungen des Verordnungsentwurfs betreffend internationale Übermittlungen und den räumlichen Geltungsbereich der Verordnung zum Ausdruck gebracht, wobei sie die Notwendigkeit hervorhoben, weitgehend sicherzustellen, dass nicht in der Union niedergelassene für die Verarbeitung Verantwortliche den Unionsvorschriften unterliegen, wenn sie personenbezogene Daten von in der Union ansässigen Personen verarbeiten.

2. Auf der März-Tagung des Rates fand der Entwurf der Bestimmungen zum räumlichen Geltungsbereich der Verordnung (Artikel 3 Absatz 2) breite Unterstützung, wobei darauf hingewiesen wurde, dass weitgehend sichergestellt werden muss, dass Unionsvorschriften auf für die Verarbeitung Verantwortliche, die nicht in der EU ansässig sind, angewendet werden, wenn sie personenbezogene Daten von in der Union ansässigen betroffenen Personen verarbeiten. Die Minister bestätigten ferner ihre Auffassung, dass internationale Übermittlungen personenbezogener Daten an Drittländer auf der Grundlage des Konzepts und der Kernprinzipien des Kapitels V erfolgen sollten. Zudem betonten sie, dass die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen auf der Grundlage von Ausnahmen (d.h. nicht auf der Grundlage der Feststellung, dass geeignete/angemessene Garantien – einschließlich unternehmensinterner Datenschutzvorschriften und Vertragsklauseln – bestehen) als Ausnahmefall zu betrachten ist und dass es Garantien bedarf, um die Einhaltung der in Artikel 8 der EU-Grundrechtecharta verankerten Grundrechte und -freiheiten im Hinblick auf den Schutz personenbezogener Daten sicherzustellen. Die Minister stimmten darin überein, dass weitere technische Arbeiten in Bezug auf Kapitel V erforderlich sind, darunter eine Diskussion über mögliche alternative/ergänzende Modelle für internationale Datenübermittlungen.

3. Die Datenschutz-Grundverordnung baut auf dem bewährten System und den Grundsätzen der Datenschutzrichtlinie (Richtlinie 95/46/EG) auf. Sie bietet einen Rahmen für Datenübermittlungen, der auf Angemessenheitsbeschlüssen, geeigneten Garantien und, falls diese fehlen, auf Ausnahmen für bestimmte, in der Verordnung festgelegte Situationen beruht.

4. Der Verordnungsentwurf stellt eine Fortführung des Konzepts der Datenübermittlung auf der Grundlage von Angemessenheitsbeschlüssen dar; dabei kann die Kommission im Rahmen des Ausschussverfahrens unter Einbeziehung der Vertreter der Mitgliedstaaten und unter der Kontrolle des Europäischen Parlaments durch Beschluss feststellen, ob ein Drittland – einschließlich bestimmter Gebiete oder definierter Sektoren, beispielsweise bestimmte Wirtschaftssektoren eines Drittlands – oder eine internationale Organisation einen angemessenen Schutz bietet. In dem Kompromisstext ist vorgesehen, dass der Europäische Datenschutzausschuss Stellungnahmen an die Kommission richtet, und zwar sowohl im Hinblick auf die Bewertung der Angemessenheit des Schutzniveaus in einem Drittland oder einer internationalen Organisation als auch auf die Beurteilung der Frage, ob das Drittland oder die internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Weitere Präzisierungen wurden vorgenommen in Bezug auf die Faktoren, die bei einem Beschluss über das Ausmaß der Angemessenheit zu berücksichtigen sind (einschließlich einer ausdrücklichen Bezugnahme auf das Europaratsübereinkommen 108[1]), und auf die Pflicht der Kommission, die Wirksamkeit von Angemessenheitsbeschlüssen innerhalb einer angemessenen Frist zu überwachen.

5. Im Kompromisstext ist ausdrücklich vorgesehen, dass Datenübermittlungen an Drittländer gestattet sind, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien bietet, auch durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren, das derzeit nicht vorgesehen ist. Ferner erfolgt eine Klassifizierung zwischen geeigneten Garantien, die keiner besonderen Genehmigung durch die Aufsichtsbehörden bedürfen (d.h. unternehmensinterne Datenschutzvorschriften, Standarddatenschutzklauseln sowie genehmigte Verhaltensregeln und Zertifizierungsverfahren, die sicherstellen, dass der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter oder der Empfänger im Drittland sich dazu verpflichten, den Schutz aus der EU stammender personenbezogener Daten zu garantieren) und geeigneten Garantien, die weiterhin der Genehmigung durch die zuständige Aufsichtsbehörde bedürfen (insbesondere nicht auf Standardvertragsklauseln beruhende Vertragsklauseln).

[1] Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dazugehöriges Zusatzprotokoll.

6. Übermittlungen können auch auf der Grundlage von Ausnahmen erfolgen, die für Sonderfälle vorgesehen sind. Weitere Präzisierungen erfolgten in Bezug auf die zu berücksichtigenden Kriterien und auf die gewichtigen Gründe des öffentlichen Interesses (z.B. zwischen Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten zur Verringerung und/oder Beseitigung des Dopings im Sport).

7. Des Weiteren beantragten einige Mitgliedstaaten die Aufnahme einer ausdrücklichen Bestimmung in die Verordnung, nach der die Beschränkung von Datenübermittlungen in Drittländer aus wichtigen Gründen des öffentlichen Interesses zulässig ist. Der Vorsitz hat eine Bestimmung aufgenommen (Artikel 44 Absatz 5a), nach der solche Beschränkungen bei Fehlen einer Angemessenheitsfeststellung der Kommission gestattet sind, wobei die nationalen Maßnahmen der Kommission mitzuteilen sind.

8. Was etwaige künftige neue (alternative/zusätzliche) Modelle für die internationale Datenübermittlung anbelangt, so haben die Mitgliedstaaten keine solchen Modelle vorgeschlagen. Der Vorsitz ist der Auffassung, dass diese Modelle der Logik des derzeit vorgeschlagenen – vielseitigen aber kohärenten – Systems folgen können bzw. sollten, dem die Minister ihre Zustimmung erteilt haben. Der vorliegende Kompromiss ist zukunftssicher und bietet genügend Ausweitungsmöglichkeiten auf neue Modelle, die sich auf angemessene Garantien stützen und somit den Schutz der Personen garantieren, deren Daten international übermittelt werden.

9. In den Sitzungen der Gruppe "Informationsaustausch und Datenschutz" vom 31. März/1. April, 7. Mai sowie 15./16 Mai 2012 wurde der Text des Kapitels V weiter erörtert, um die verbleibenden Fragen zu klären. Im Anschluss an die Erörterungen auf der Tagung des AStV vom 28. Mai 2014 hat der Vorsitz den Text und die entsprechenden Erwägungsgründe weiter überarbeitet. Die jüngsten Änderungen sind durch **Fettdruck und Unterstreichung** gekennzeichnet.

Partielle allgemeine Ausrichtung

10. Der Vorsitz ersucht den Rat, eine partielle allgemeine Ausrichtung zu Artikel 3 Absatz 2 (räumlicher Geltungsbereich), zu den jeweiligen Definitionen von unternehmensinternen Datenschutzvorschriften und "internationalen Organisationen" (Artikel 4 Nummern 17 und 21) und zu Kapitel V (siehe Anlage) 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; sie schließt künftige Änderungen am Text des Kapitels V, die der Gesamtkohärenz der Verordnung dienen, nicht aus;
    ii. die partielle allgemeine Ausrichtung greift horizontalen Fragen wie der Rechtsform des Instruments oder Bestimmungen über delegierte Rechtsakte 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.

11. Um zu dieser partiellen allgemeinen Ausrichtung zu gelangen, wurde folgenden drei Fragen besondere Aufmerksamkeit gewidmet:

Erfordernis einer vorherigen Genehmigung im Falle geeigneter Garantien (Artikel 42)

12. In dem Kompromisstext wird unterschieden zwischen
    a) einer Übermittlung ohne besondere Genehmigung im Falle von rechtsverbindlichen Instrumenten und
    b) einer Übermittlung mit Genehmigung durch die zuständige Datenschutzbehörde in anderen Fällen.

    Der neue Text macht deutlich, dass diese genehmigten Verhaltensregeln und Zertifizierungsverfahren mit einer verbindlichen und durchsetzbaren Verpflichtung seitens des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in dem Drittland einhergehen müssen. Künftig wird sich dies auch in dem Wortlaut der betreffenden Artikel (38-39) in Kapitel IV niederschlagen müssen[2].

[2] So könnte in Betracht gezogen werden, in Artikel 39 eine europaweite Zertifizierungsregelung in solchen Fällen zu gestatten und die europäischen Grundsätze, denen die für die Verarbeitung Verantwortlichen oder die Auftragsverarbeiter in Drittländern gerecht werden sollten, sowie die geeigneten Garantien, die diese zur Erlangung einer solchen Zertifizierung vorweisen sollten, aufzulisten. Eine Liste der zertifizierten für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter könnte unter der Verantwortung des Europäischen Datenschutzausschusses veröffentlicht und regelmäßig auf den neuesten Stand gebracht werden.

Übermittlung aufgrund eines berechtigten Interesses des für die Verarbeitung Verantwortlichen (Artikel 44 Absatz 1 Buchstabe h)

13. Über die Übermittlung auf der Grundlage von Angemessenheitsfeststellungen der Kommission oder geeigneter für den öffentlichen und den privaten Sektor einschließlich NRO geltender Garantien (unternehmensinterne Datenschutzvorschriften, Vertragsklauseln, Verhaltensregeln usw.) hinaus können Übermittlungen auf der Grundlage der Ausnahmen in Artikel 44 erfolgen. Eine dieser Ausnahmen (Artikel 44 Absatz 1 Buchstabe h) gestattet eine Übermittlung aufgrund berechtigter Interessen des für die Verarbeitung Verantwortlichen; dabei gelten folgende Bedingungen:
   – Die Übermittlung darf nicht umfangreich oder häufig sein, d.h. sie muss sporadischen Charakter haben, und
   – die berechtigten Interessen des für die Verarbeitung Verantwortlichen dürfen nicht die Rechte oder Freiheiten der betroffenen Person überwiegen und
   – der für die Verarbeitung Verantwortliche bietet ausreichende Garantien (Einzelheiten siehe Erwägungsgrund 88).

14. Der Vorsitz ist der Ansicht, dass eine ausgewogene Lösung gefunden wurde und dass daher für diese Ausnahme der bisherige Wortlaut beibehalten werden sollte.

Beschränkung der Übermittlung personenbezogener Daten in Drittländer (Artikel 44 Absatz 5a)

15. In Ausnahmefällen kann es erforderlich sein, dass staatliche Behörden aus Gründen des öffentlichen Interesses den Fluss personenbezogener Daten in Länder außerhalb der Europäischen Union auf der Grundlage des Unions- oder des einzelstaatlichen Rechts beschränken. Eine Delegation hat das Beispiel nationaler Passdaten und elektronischer Gesundheitsakten genannt[3]. Der für diese Ausnahme geltende bisherige Wortlaut dürfte für die Mehrheit der Delegationen annehmbar sein.

_____

[3] 9703/14 DATAPROTECT 68 JAI 303 MI 417 DRS 64 DAPIX 62 FREMP 88 COMIX 254 CODEC 1247.

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

(20) Um sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach dieser Verordnung ein Anrecht haben, sollte die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen in der Union anzubieten. Um festzustellen, ob ein für die Verarbeitung Verantwortlicher diesen betroffenen Personen in der Union Waren oder Dienstleistungen anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Geschäfte mit in einem oder mehreren Mitgliedstaaten der Union ansässigen betroffenen Personen zu tätigen. Während die bloße Zugänglichkeit der Website eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union oder einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der für die Verarbeitung Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt ist, können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, und/oder die Erwähnung von in der Union ansässigen Kunden oder Nutzern darauf hindeuten, dass der für die Verarbeitung Verantwortliche beabsichtigt, diesen betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten.

(21) Die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser Personen in der Europäischen Union zu beobachten. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten mit Hilfe von Datenverarbeitungstechniken nachvollzogen werden, durch die von einer Person ein Profil erstellt wird, das die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.

(22) Ist nach internationalem Recht das innerstaatliche Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, sollte die Verordnung auch auf einen nicht in der EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.

(78) Der grenzüberschreitende Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und wieder zurück ist für die Entwicklung des internationalen Handels und der grenzüberschreitenden Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Der durch diese Verordnung unionsweit garantierte Schutz natürlicher Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an für die Verarbeitung Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht unterminiert werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation stammende personenbezogene Daten an für die Verarbeitung Verantwortliche, Auftragsverarbeiter in demselben[4] oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weitergegeben werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Sie dürfen nur stattfinden, wenn die in Kapitel V festgelegten Bedingungen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

[4] DE: Prüfungsvorbehalt; stellte insbesondere Fragen zur Anwendung der Vorschriften über den Ort des Vertragsabschlusses in Bezug auf Artikel 89a.

(79) Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt. Die Mitgliedstaaten dürfen internationale Übereinkünfte schließen, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen beinhalten, sofern sich diese Übereinkünfte weder auf diese Verordnung noch auf andere Bestimmungen des Unionsrechts auswirken und Schutzklauseln beinhalten, um die Rechte der betroffenen Personen zu schützen[5].

(80) Die Kommission darf (...) mit Wirkung für die gesamte Union feststellen, dass bestimmte Drittländer oder ein Gebiete oder ein bestimmter Sektor wie z.B. der private Sektor oder ein oder mehrere bestimmte Wirtschaftszweige eines Drittlands oder eine internationale Organisation einen angemessenen Datenschutz bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, einen solchen Schutz zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne besondere Genehmigung an diese Länder übermittelt werden.

(81) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung eines Drittlandes oder eines Gebietes oder eines bestimmten Sektors in einem Drittland berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, ein Rechtsschutz existiert und die internationalen Menschenrechtsbestimmungen eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und öffentliche Ordnung sowie das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor in einem Drittland sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmten Verarbeitungsvorgängen und des Geltungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen.

---

[5] FR: Der zweite Satz sollte in Artikel 89a aufgenommen werden. NL fragte, was mit dem neuen Text gemeint sei, und vertrat die Auffassung, dass er beibehalten werden sollte; allerdings müssten Zweck und Sinn präzisiert werden. DE und UK haben noch einen Prüfungsvorbehalt zu dem neuen Text. EE fragte, ob "*sich auswirken*" "nicht im Widerspruch stehen" bedeute oder etwas anderes.

(81a) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere *sollte* der Beitritt des Drittlandes zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll *berücksichtigt werden*. Die Kommission sollte den Europäischen Datenschutzausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet[6].

(81b) Die Kommission sollte die Wirksamkeit von Feststellungen betreffend das Schutzniveau in einem Drittland oder einem Gebiet oder einem bestimmten Sektor in einem Drittland oder einer internationalen Organisation überwachen; dies gilt auch für Feststellungen, die auf der Grundlage des Artikels 25 Absatz 6 oder des Artikels 26 Absatz 4 der Richtlinie 95/46/EG erlassen werden. Die Kommission sollte innerhalb einer angemessenen Frist die Wirksamkeit der letztgenannten Feststellungen bewerten und dem durch diese Verordnung eingesetzten Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 über alle relevanten Erkenntnisse Bericht erstatten.

(82) Die Kommission kann (...) feststellen, dass ein Drittland oder ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation (...) keinen angemessenen Datenschutz mehr bietet. Die Übermittlung personenbezogener Daten in dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen der Artikel 42 bis 44 werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

---

6 DE, die von NL unterstützt wurde, schlug vor, dass die Liste der Prüfungen in Artikel 42 Absatz 2 eine neue Komponente beinhalten sollte, nämlich die Beteiligung von Drittstaaten oder internationalen Organisationen an internationalen Datenschutzsystemen (z.B. APEC und ECOWAS). Nach Ansicht von DE sollte der Verordnungsentwurf diesen Systemen, auch wenn sie sich noch in einem frühen Stadium der praktischen Anwendung befinden, bereits jetzt Rechnung tragen, da sie in Zukunft an Bedeutung gewinnen können. Nach Artikel 41 Absatz 2 Buchstabe d müssen die Systeme grundsätzlich geeignet sein, die Einhaltung von Datenschutzstandards sicherzustellen.

(83) Bei Fehlen eines Angemessenheitsbeschlusses sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese Garantien können darin bestehen, dass auf verbindliche unternehmensinterne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, von einer Aufsichtsbehörde genehmigte Ad-hoc-Vertragsklauseln oder auf sonstige geeignete, angemessene, aufgrund der Umstände einer Datenübermittlung oder einer Kategorie von Datenübermittlungen gerechtfertigte und von einer Aufsichtsbehörde gebilligte Maßnahmen zurückgegriffen wird. Diese Schutzklauseln sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame administrative und gerichtliche Rechtsbehelfe beachtet werden. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen sowie die Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen beziehen. Datenübermittlungen dürfen auch von staatlichen Behörden oder Stellen an staatliche Behörden oder Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen, beispielsweise eine Absichtserklärung, aufzunehmen sind. Die Genehmigung der zuständigen Aufsichtsbehörde sollte erlangt werden, wenn die Garantien in nicht rechtsverbindlichen Verwaltungsvereinbarungen vorgesehen sind.

(84) Die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter offen stehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln zurückzugreifen, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter keinesfalls daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, einschließlich Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden oder ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und -freiheiten der betroffenen Personen beschneiden.

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

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

(87) Diese Vorschriften sollten insbesondere für Datenübermittlungen gelten, die aus gewichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den grenzüberschreitenden Datenaustausch zwischen Wettbewerbsbehörden, zwischen Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. Die Übermittlung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein Interesse, das für die lebenswichtigen Interessen – einschließlich der körperlichen Unversehrtheit oder des Lebens – der betroffenen Person oder einer anderen Person wesentlich ist, zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben.[7] Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im einzelstaatlichen Recht aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten sollten solche Bestimmungen der Kommission mitteilen.

[7] FR wies auf den Fall hin, dass der Empfänger der Übermittlung eine medizinische Fachkraft ist oder Bestimmungen zur Wahrung des Rechts der betroffenen Person in Bezug auf den Schutz der Privatsphäre und die ärztliche Schweigepflicht vorgesehen hat. Der Vorsitz ist der Ansicht, dass darauf im Rahmen des Kapitels IX genauer eingegangen werden könnte.

(88) Übermittlungen, die weder als umfangreich noch als häufig gelten können, könnten auch zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters möglich sein, sofern die Interessen oder Rechte oder Freiheiten der betroffenen Person nicht überwiegen und der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter sämtliche Umstände der Datenübermittlung geprüft hat. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter sollte insbesondere die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland sowie vorgesehene geeignete Garantien zum Schutz der Grundrechte und -freiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogener Daten berücksichtigen. Bei der Verarbeitung zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Bei der Prüfung, ob eine Übermittlung umfangreich oder häufig ist, sollte berücksichtigt werden, wie viele personenbezogene Daten und wie viele Personen betroffen sind und ob die Übermittlung sporadisch oder regelmäßig erfolgt.

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

(90) Manche Drittländer erlassen Gesetze, Vorschriften und sonstige Rechtsakte, durch die die Datenverarbeitungstätigkeiten natürlicher und juristischer Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar geregelt werden. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets der betreffenden Drittländer kann gegen internationales Recht verstoßen und dem durch diese Verordnung in der Union gewährleisteten Schutz natürlicher Personen zuwiderlaufen. Datenübermittlungen sollten daher nur zulässig sein, wenn die Bedingungen dieser Verordnung für Datenübermittlungen in Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Weitergabe aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist. (…)

(91) Bei der grenzüberschreitenden Übermittlung personenbezogener Daten außerhalb der Union ist der Einzelne womöglich weniger in der Lage, seine Datenschutzrechte wahrzunehmen und sich insbesondere gegen die unrechtmäßige Nutzung oder Weitergabe dieser Informationen zu schützen. Zugleich können die Aufsichtsbehörden unter Umständen nicht in der Lage sein, Beschwerden nachzugehen oder Untersuchungen in Bezug auf Tätigkeiten im Ausland durchzuführen. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, nicht übereinstimmende Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Daher bedarf es der Förderung einer engeren Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. Um Mechanismen der internationalen Zusammenarbeit zu entwickeln, die die internationale Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtern und sicherstellen, sollten die Kommission und die Aufsichtsbehörden Informationen austauschen und bei Tätigkeiten, die mit der Ausübung ihrer Befugnisse in Zusammenhang stehen, mit den zuständigen Behörden der Drittländer nach dem Grundsatz der Gegenseitigkeit und unter Einhaltung der Vorschriften dieser Verordnung, einschließlich der Vorschriften des Kapitels V, zusammenarbeiten.

(107) Auf Unionsebene sollte ein Europäischer Datenschutzausschuss eingerichtet werden. Er sollte die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten ersetzen. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten gebildet werden. Die Kommission sollte ohne Stimmrecht an seinen Beratungen teilnehmen. Der Europäische Datenschutzausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission insbesondere im Hinblick auf das Schutzniveau in Drittländern oder internationalen Organisationen beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Europäische Datenschutzausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.

Artikel 3

Räumlicher Anwendungsbereich

(1) Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.

(2) Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung

a) dazu dient, diesen Personen Waren oder Dienstleistungen in der Union anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist;

b) der Beobachtung ihres Verhaltens dient, soweit ihr Verhalten in der Europäischen Union erfolgt[8].

(3) Diese Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der völkerrechtlich dem Recht eines Mitgliedstaats unterliegt.

[8] UK: Vorbehalt.

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck

(17) "verbindliche unternehmensinterne Datenschutzvorschriften" Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats der Union niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe[9] oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern verpflichtet;

(21) "internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde[10];

9 DE fragte, ob verbindliche unternehmensinterne Datenschutzvorschriften auch für Datenübermittlungen innerhalb der EU gelten könnten. KOM erklärte, im Fall von Datenübermittlungen innerhalb der EU bestehe kein Bedarf an verbindlichen unternehmensinternen Datenschutzvorschriften, doch stehe es dem für die Verarbeitung Verantwortlichen frei, auch in diesen Fällen entsprechende Vorschriften anzuwenden.

10 NL fragte, ob auch Absichtserklärungen unter diese Begriffsbestimmung fielen. FI fragte, ob auch Interpol erfasst sei. CZ, DK, LV, SI, SE und UK wünschten die Streichung dieser Begriffsbestimmung.

KAPITEL V
ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN[11] [12] [13] [14]

Artikel 40

Allgemeine Grundsätze der Datenübermittlung

(…)

---

[11] In Anbetracht der Tatsache, dass die Ausnahme des öffentlichen Interesses in den meisten Fällen der Hauptgrund für eine internationale Übermittlung personenbezogener Daten sein dürfte, fragten einige Delegationen (CZ, DE, LV, UK), ob der "alte" Angemessenheitsgrundsatz/-test in dieser detaillieren Form beibehalten werden sollte, da er in der Praxis nicht in allzu vielen Fällen zum Tragen kommen dürfte. Insbesondere DE war der Ansicht, dass die Fülle der Ausnahmen der Angemessenheitsregel ihren Sinn nehme. Ohne das Ziel des Schutzes vor der Übermittlung personenbezogener Daten an Drittländer in Frage zu stellen, bezweifelte sie, dass der Angemessenheitsgrundsatz hierfür das geeignete Instrument sei, wenn man die zahlreichen praktischen und politischen Schwierigkeiten bedenke (Letzteres insbesondere in Anbetracht der Gefahr eines negativen Angemessenheitsbeschlusses: DE, FR, UK). Ob es machbar sei, den Angemessenheitstest beizubehalten, wurde auch vor dem Hintergrund der massiven Ströme personenbezogener Daten im Rahmen des Cloud Computing in Zweifel gezogen: BG, DE, FR, IT, NL, SK und UK. FR und DE fragten, ob die Datenübermittlung im Rahmen des Cloud Computing oder die Bekanntmachung personenbezogener Daten im Internet als internationale Datenübermittlung gälten. DE vertrat ferner die Ansicht, dass die Verordnung einen Rechtsrahmen für Vereinbarungen der "Safe Harbour"-Art schaffen sollte, in deren Rahmen bestimmte Garantien, die Unternehmen in einem Drittland auf freiwilliger Basis übernommen haben, von den Behörden dieses Landes überwacht werden. Es wurde die Anwendbarkeit der Bestimmungen dieses Kapitels auf den öffentlichen Sektor (EE) sowie die Abgrenzung des Geltungsbereichs der vorgeschlagenen Richtlinie (FR) in Frage gestellt. Mehrere Delegationen (FR, PL) warfen die Frage nach den Auswirkungen dieses Kapitels auf bestehende Vereinbarungen der Mitgliedstaaten auf.

[12] NL und UK wiesen darauf hin, dass nach der Datenschutzrichtlinie von 1995 der für die Verarbeitung Verantwortliche, der Daten übermitteln möchte, der erste ist, der zu beurteilen hat, ob dies nach den geltenden Rechtsvorschriften (der EU) möglich ist, und diese Delegationen wünschen die Beibehaltung dieses Grundsatzes, der im Kommissionsvorschlag offensichtlich fallengelassen wurde.

[13] DE fragte, welche Rechtsvorschriften auf an in Drittländern niedergelassene für die Verarbeitung Verantwortliche übermittelte Daten, die unter Artikel 3 Absatz 2 fallen, Anwendung finden, d.h. ob es sich nach Maßgabe dieser Bestimmung um EU-Recht handeln würde.

[14] AT unterbreitete eine Reihe von Vorschlägen zu diesem Kapitel, die in Dokument 10198/14 DATAPROTECT 82 JAI 363 MI 458 DRS 73 DAPIX 71 FREMP 103 COMIX 281 CODEC 1351 enthalten sind.

Artikel 41

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses[15]

1. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission[16] festgestellt hat, dass das betreffende Drittland bzw. ein Gebiet oder ein oder mehrere spezifische Sektoren dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung.

2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission insbesondere

   a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die (...) in dem betreffenden Drittland bzw. der betreffenden internationalen Organisation geltenden Vorschriften[17] sowohl allgemeiner als auch sektoraler Art, Datenschutzbestimmungen und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation sowie die Existenz wirksamer und durchsetzbarer Rechte der betroffenen Person und wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen (...), deren personenbezogene Daten übermittelt werden[18];

---

15 Einige Delegationen äußerten Bedenken in Bezug auf den Zeitaufwand der Angemessenheitsverfahren und unterstrichen die Notwendigkeit, diesen Prozess zu beschleunigen. KOM betonte, dass dies nicht auf Kosten der Qualität des Angemessenheitsverfahrens gehen sollte.

16 CZ, DE und SI: Vorbehalt gegen die Übertragung einer diesbezüglichen Befugnis an die Kommission. NL und UK wiesen darauf hin, dass mit diesem Vorschlag offensichtlich von der Datenschutzrichtlinie von 1995 abgewichen werde, der zufolge für die Beurteilung des Datenschutzrechts eines Drittlandes in erster Linie der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermitteln möchte, zuständig ist. UK hat erhebliche Zweifel an der Praxistauglichkeit der Aufzählung in Absatz 2.

17 AT hätte die Aufnahme einer Bezugnahme auf die nationale Sicherheit vorgezogen.

18 Nach Auffassung von NL stützt sich Artikel 41 auf Grundrechte und Rechtsvorschriften, während die Safe Harbour-Regelung auf Freiwilligkeit beruht; daher sei es sinnvoll, die Safe Harbour-Aspekte in einem separaten Artikel zu behandeln. DE fragte, wie der Safe Harbour-Aspekt in Kapitel V integriert werden könne.

b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden[19] in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind;

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere (...) Verpflichtungen, die sich aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

2a. Der Europäische Datenschutzausschuss richtet eine Stellungnahme an die Kommission[20], in der er die Angemessenheit des gebotenen Schutzes in einem Drittland oder einer internationalen Organisation beurteilt und prüft, ob das Drittland, das Gebiet, die internationale Organisation oder der spezifische Sektor keinen angemessenen Datenschutz mehr bietet.

[19] NL fragte, wie streng diese Unabhängigkeit zu prüfen sei. BE schlug vor, einen Hinweis auf unabhängige Justizbehörden aufzunehmen; FI schlug vor, nur von "Behörden" zu sprechen.

[20] CZ wünscht einen deutlicheren Hinweis auf die Verpflichtung der Kommission, den Europäischen Datenschutzausschuss um Stellungnahme zu ersuchen.

3. Nach der Beurteilung der Angemessenheit[21] des Schutzniveaus kann die Kommission durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne des Absatzes 2 bietet. (…)[22]. In jedem Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte(n) (unabhängige(n)) Aufsichtsbehörde(n) angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.[23]

3a. *Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 (...) der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission*[24] gemäß dem in Artikel 87 Absatz 2 genannten Prüfverfahren *geändert, ersetzt oder aufgehoben werden.*[25]

---

[21] CZ, RO und SI: Vorbehalt gegen die Übertragung einer diesbezüglichen Befugnis an die Kommission. Nach Auffassung von DE sollten die Interessenträger in diesen Prozess einbezogen werden. NL und UK wiesen darauf hin, dass mit diesem Vorschlag offensichtlich von der Datenschutzrichtlinie von 1995 abgewichen werde, der zufolge für die Beurteilung des Datenschutzrechts eines Drittlandes in erster Linie der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermitteln möchte, zuständig ist.

[22] Nach Auffassung von CZ, DE DK, HR, IT, NL, PL, SK und RO sollte dem Europäischen Datenschutzausschuss eine bedeutende Rolle bei der Bewertung dieser Elemente übertragen werden. KOM wies darauf hin, dass in Ausschussverfahren gemäß den Verträgen und der Verordnung 182/2011 kein zusätzlicher Schritt eingeplant werden könne.

[23] DE warf die Frage nach den Maßnahmen im Anschluss an einen derartigen Beschluss auf und warnte davor, dass Drittländer, denen ein Angemessenheitsbeschluss zugute kommt, in der Folge nicht mehr dasselbe Datenschutzniveau bieten könnten. KOM erklärte, dass Drittländer, für die ein Angemessenheitsbeschluss gefasst worden ist, überwacht werden.

[24] Von Absatz 8 übernommen. Nach Auffassung von CZ und AT sollte eine absolute Höchstfrist (Verfallsklausel) festgesetzt werden; KOM lehnte dies ab. Nach Auffassung von NL, PT und SI ist Absatz 3a überflüssig bzw. zumindest unklar. RO war darüber hinaus der Ansicht, dass dieser Absatz, wenn er beibehalten werde, an das Ende der Verordnung verschoben werden sollte.

[25] DE und ES schlugen vor, den Ausschuss um Stellungnahme zu ersuchen. KOM wies darauf hin, dass in Ausschussverfahren gemäß den Verträgen und der Verordnung 182/2011 kein zusätzlicher Schritt eingeplant werden könne. DE fragte, ob Beschlüsse gemäß Absatz 3a unbegrenzt gültig seien. Nach Auffassung von IE bietet Absatz 3a die notwendige Flexibilität. Nach Auffassung von CZ sollten neue Staaten gegenüber denjenigen, für die im Rahmen der Richtlinie von 1995 ein Angemessenheitsbeschluss gefasst wurde, nicht benachteiligt werden.

4. (…)

4a. Die Kommission überwacht die Wirksamkeit der nach Absatz 3 sowie nach Artikel 25 Absatz 6 und Artikel 26 Absatz 4 der Richtlinie 95/46/EG[26] gefassten Beschlüsse.

5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland bzw. ein Gebiet oder ein spezifischer Sektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne des Absatzes 2 mehr bietet, und erforderlichenfalls derartige Beschlüsse ohne rückwirkende Kraft widerrufen, ändern oder aussetzen. Die Durchführungsrechtsakte werden gemäß dem in Artikel 87 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen (...) gemäß dem in Artikel 87 Absatz 3 genannten Verfahren angenommen.[27]

5a. Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

6. Übermittlungen personenbezogener Daten an das betreffende Drittland bzw. an das Gebiet oder den spezifischen Sektor dieses Drittlands oder an die betreffende internationale Organisation gemäß den Artikeln 42 bis 44 werden durch einen Beschluss nach Absatz 5 nicht berührt[28].

---

26 BE hinterfragte den Verweis auf die Richtlinie von 1995. CZ hält ihn für überflüssig.

27 FR und UK schlugen vor, dass der Europäische Datenschutzausschuss Stellung nimmt, bevor KOM beschließt, einen Angemessenheitsbeschluss zu widerrufen.

28 DE beantragte die Streichung von Absatz 6. DK hält den Zeitpunkt, zu dem Drittländer konsultiert werden sollten, für unklar.

7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste aller Drittländer bzw. Gebiete und spezifischen Sektoren eines Drittlandes und aller internationalen Organisationen, zu denen Beschlüsse gemäß den Absätzen 3, 3a und 5 gefasst wurden.

8. (…)

Artikel 42

Datenübermittlung auf der Grundlage geeigneter Garantien[29]

1. Falls kein Beschluss nach Artikel 41 Absatz 3 vorliegt, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an (...) ein Drittland oder eine internationale Organisation übermitteln, sofern der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien, einschließlich für die Datenweitergabe (...), vorgesehen hat.

29 UK äußerte Bedenken hinsichtlich der Dauer der Genehmigungsverfahren sowie der Belastung, den diese für die Ressourcen der Datenschutzbehörden darstellen würden. Der Nutzen dieser Verfahren im Hinblick auf den Datenfluss beim Cloud Computing wurde ebenfalls hinterfragt.

2. Die in Absatz 1 genannten geeigneten Garantien *können* (...) , ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

oa) einem rechtsverbindlichen **und durchsetzbaren** Instrument **zwischen den staatlichen Behörden oder Stellen**[30] oder

a) verbindlichen unternehmensinternen Datenschutzvorschriften gemäß Artikel 43 oder

b) Standarddatenschutzklauseln, die (...) von der Kommission[31] gemäß dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen werden, oder

c) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission nach dem Prüfverfahren gemäß Artikel 87 Absatz 2 angenommen wurden, oder

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

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

---

30 HU hat ernste Bedenken; die vorgeschlagene allgemeine Klausel ("ein rechtsverbindliches Instrument") sei zu vage, da sie im Text inhaltlich nicht definiert werde. Darüber hinaus sehe der Text auch keine vorherige Prüfung durch die Datenschutzbehörde vor. HU schlägt daher vor, diesen Buchstaben entweder zu streichen oder für ein solches Instrument die Genehmigung durch die Datenschutzbehörde vorzuschreiben, da ihres Erachtens eine reelle Gefahr bestehe, dass Übermittlungen auf der Grundlage eines solch vagen Instruments die Rechte der betroffenen Personen ernsthaft unterminieren könnten.

31 Vorbehalt von FR hinsichtlich der Möglichkeit, dass KOM derartige Standardklauseln erlässt.

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

a) Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der Daten im Drittland oder der internationalen Organisation vereinbart (...) wurden, oder

b) (…)

c) (…)

d) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind (…).

3. (…)

4. (…)

5a. Die Aufsichtsbehörde bringt das Kohärenzverfahren zur Anwendung, wenn ein Fall gemäß Artikel 57 Absatz 2 Buchstabe ca, d, e oder f vorliegt.

5b. *Sämtliche von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben so lange in Kraft, bis sie von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden.*[32] Sämtliche von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission[33] nach dem Prüfverfahren gemäß Artikel 87 Absatz 2[34] geändert, ersetzt oder aufgehoben werden.

Artikel 43

Verbindliche unternehmensinterne Datenschutzvorschriften[35]

1. Die zuständige Aufsichtsbehörde *genehmigt*[36] nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahrens *verbindliche unternehmensinterne Datenschutzvorschriften*, sofern diese
   a) rechtsverbindlich sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern angewendet werden;

---

32 UK und ES waren gegen den Grundsatz, für nicht standardisierte Verträge eine vorherige Genehmigung durch Datenschutzbehörden vorzuschreiben. Dies wäre ein Verstoß gegen den Grundsatz der Rechenschaftspflicht. DE hob hervor, dass es einer Überwachung bedarf.

33 Nach Ansicht von AT sollte eine absolute Zeitspanne festgelegt werden.

34 DE und ES schlugen vor, den Ausschuss um Stellungnahme zu bitten. KOM wies darauf hin, dass im Ausschussverfahren gemäß den Verträgen und der Verordnung 182/2011 kein zusätzlicher Schritt eingeplant werden könne.

35 NL wünschte eine Ausweitung seiner Tragweite. BE und NL hielten eine Übergangsregelung für notwendig, damit angestammte verbindliche unternehmensinterne Datenschutzvorschriften gewahrt werden können. NL fragte, ob diese Vorschriften auch für Angestellte verbindlich sein sollten. SI vertrat die Auffassung, verbindliche unternehmensinterne Datenschutzvorschriften sollten auch in Bezug auf einige Behörden möglich sein, woraufhin KOM erklärte, sie sehe im öffentlichen Sektor keine Anwendungsmöglichkeiten für verbindliche unternehmensinterne Datenschutzvorschriften. HU teilte mit, ihres Wissens würden nicht nur gewinnorientierte Unternehmen, sondern auch internationale Einrichtungen und Nichtregierungsorganisationen verbindliche unternehmensinterne Datenschutzvorschriften anwenden.

36 Bedenken von DE und UK hinsichtlich der Langwierigkeit und der Kosten solcher Genehmigungsverfahren. Es wurde gefragt, welche Datenschutzbehörden in die Genehmigung solcher verbindlicher unternehmensinterner Datenschutzvorschriften im Rahmen des Kohärenzverfahrens einbezogen werden sollten.

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen;

c) die in Absatz 2 festgelegten Anforderungen erfüllen.

2. Die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der *betreffenden* Unternehmensgruppe und *jedes ihrer* Mitglieder;

b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Datenschutzvorschriften;

d) die Anwendung der allgemeinen Datenschutzgrundsätze, (...) die Datenqualität, die Rechtsgrundlage für die Verarbeitung, die Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese unternehmensinternen Datenschutzvorschriften gebundene Stellen (...);

e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner Profilerstellung (...) nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Datenschutzvorschriften; der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann [37];

[37] Nach Auffassung von DE sollte die Bezugnahme auf Befreiungen an dieser Stelle gestrichen werden.

g) die Art und Weise, wie die betroffenen Personen gemäß den Artikeln 14 und 14a über die verbindlichen unternehmensinternen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 35 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der (...) Überwachung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften in der Unternehmensgruppe sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

hh) die Beschwerdeverfahren;

i) die innerhalb der Gruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens oder der Gruppe von Unternehmen mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Ersuchen zur Verfügung gestellt werden;

j) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der (...) Gruppe gewährleisten, insbesondere durch Offenlegung der Ergebnisse von (...) Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde[38];

l) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Gruppe in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen unternehmensinternen Datenschutzvorschriften bieten[39], und

---

38 BE schlug vor, dies für den Fall eines Konflikts zwischen den für ein Mitglied der Gruppe geltenden "örtlichen" Rechtsvorschriften und den verbindlichen unternehmensinternen Datenschutzvorschriften ausdrücklicher zu regeln.

39 CZ äußerte Zweifel an Zweck und Anwendung dieser Bestimmung. UK betrachtete diesen Punkt als zu bindend und wünschte flexiblere unternehmensinterne Datenschutzvorschriften, so dass sie auf verschiedene Situationen anwendbar wären.

m) geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten (...).

(2a) Der Europäische Datenschutzausschuss berät die Kommission über das Format und die Verfahren für den Austausch von Informationen zwischen den für die Verarbeitung Verantwortlichen, den Auftragsverarbeitern und den Aufsichtsbehörden in Bezug auf verbindliche unternehmensinterne Datenschutzvorschriften.

[3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für verbindliche unternehmensinterne Datenschutzvorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Datenschutzvorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.][40]

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

[40] Vorbehalt von CZ, IT, SE und NL. Prüfungsvorbehalt von FR in Bezug auf (öffentliche) Archive. Nach Auffassung von RO und HR sollte der Europäische Datenschutzausschuss einbezogen werden. PL und KOM möchten Absatz 3 beibehalten.

Artikel 44

Ausnahmen für Sonderfälle[41]

1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 42, einschließlich verbindlicher unternehmensinterner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten (...) in ein Drittland oder an eine internationale Organisation nur zulässig, wenn
   a) die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich[42] eingewilligt hat, nachdem sie darüber unterrichtet wurde, dass derartige Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien *Risiken* für sie beinhalten kann, oder
   b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist, oder
   c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist, oder
   d) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses[43] notwendig ist,
   e) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist, oder

---

41 Vorbehalt von EE. Parlamentsvorbehalt von NL. Nach Ansicht von CZ, EE, UK und anderen Delegationen würden diese "Ausnahmen" in der Praxis zur Hauptgrundlage für die internationale Datenübermittlung werden, was an sich auch im Text der Verordnung anerkannt werden sollte.

42 Nach Auffassung von UK muss die Frage der Einwilligung horizontal erörtert werden.

43 DE verwies auf die Notwendigkeit, die Wirkung des Buchstabens d in Verbindung mit Absatz 5 zu prüfen, insbesondere was die Datenübermittlung auf der Grundlage von Gerichtsurteilen oder Verwaltungsentscheidungen aus Drittstaaten sowie geltende Rechtshilfeverträge anbelangt. IT legte einen Vorbehalt zur (subjektiven) Verwendung des Begriffs des öffentlichen Interesses ein. HR schlug vor, "sofern die rechtlichen Interessen der betroffenen Person nicht überwiegen" hinzuzufügen.

f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, oder

g) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder

h) die nicht in großem Maßstab oder *häufig*[44] erfolgende Übermittlung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, und falls der für die Verarbeitung Verantwortliche (...) alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und (...) auf der Grundlage dieser Beurteilung geeignete Garantien[45] zum Schutz personenbezogener Daten vorgesehen hat.

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

---

44 AT, ES, HU, MT, PL, PT und SI würden eine Streichung dieser ihres Erachtens zu weit gefassten Ausnahme vorziehen; Datenübermittlungen, die aufgrund des berechtigten Interesses des für die Verarbeitung Verantwortlichen erfolgten und an Drittländer gingen, in denen die Rechte der betroffenen Personen nicht angemessen geschützt seien, brächten eine ernste Gefahr mit sich, das derzeit im EU-Besitzstand vorgesehene Schutzniveau abzusenken. DE und ES legten einen Prüfungsvorbehalt zu den Begriffen "häufig oder massiv" ein, die sie für unklar halten. DE, die von SI unterstützt wurde, schlug die Einschränkung "übergeordnete berechtigte Interessen" vor. ES schlug vor, die Formulierung durch "in kleinem Maßstab und sporadisch" zu ersetzen; UK hinterfragte die Notwendigkeit einer weiteren Einschränkung des berechtigten Interesses, die ihrer Auffassung nach dem risikobasierten Ansatz zuwiderlaufen würde.

45 Vorbehalt von AT und NL aufgrund der unklaren Verbindung zwischen dieser Bezugnahme auf geeignete Garantien und die geeigneten Garantien in Artikel 42.

3. (…)

4. Absatz 1 Buchstaben a, b, c und h gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen[46].

5. Das öffentliche Interesse im Sinne des Absatzes 1 Buchstabe d muss im Unionsrecht oder im nationalen Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.

5a. Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im einzelstaatlichen Recht aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden[47]. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit[48].

6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h in der Dokumentation gemäß Artikel 28 (...).

6a. (…)

7. (…)

---

[46] Prüfungsvorbehalt von BE. Prüfungsvorbehalt von FR betreffend die Ausnahmeregelung für Behörden.

[47] SI und UK: Prüfungsvorbehalt. Nach Auffassung von FR und ES sollte diese Vorschrift in eine andere Vorschrift aufgenommen werden.

[48] Einige Delegationen (FR, PL, SI) wiesen auf den Vorschlag von DE (für den neuen Artikel 42a: 12884/13 DATAPROTECT 117 JAI 689 MI 692 DRS 149 DAPIX 103 FREMP 116 COMIX 473 CODEC 186) und die vom Europäischen Parlament angenommene Änderung (Artikel 43a) hin, die Erörterungen zu einem späteren Zeitpunkt erforderlich machen.

Artikel 45

Internationale Zusammenarbeit zum Schutz personenbezogener Daten[49]

1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur
   a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die *tatsächliche* Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,
   b) internationalen Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch (...), Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen[50],
   c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zur Förderung der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten dienen,
   d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praxis zum Schutz personenbezogener Daten.

2. (…)

_____

[49] Nach Auffassung von PL könnte Artikel 45 (teilweise) in die Präambel aufgenommen werden. NL, RO und UK äußerten Zweifel an der Notwendigkeit dieses Artikels im Zusammenhang mit der Angemessenheit und plädierten dafür, jegliche andere internationale Zusammenarbeit zwischen Datenschutzbehörden in Kapitel VI zu regeln. Nach Auffassung von NL könnte dieser Artikel gestrichen werden. ES unterbreitete einen Alternativvorschlag, der in Dokument 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394 enthalten ist.

[50] AT und FI hielten diesen Unterabsatz für unklar und klärungsbedürftig.