EUROPÄISCHE KOMMISSION

Brüssel, den 10.1.2013
C(2012) 9638 final

Herrn Winfried KRETSCHMANN
Präsident des Bundesrates
Leipziger Straße 3-4
D - 10117 BERLIN

Sehr geehrter Herr Präsident,

die Kommission dankt dem deutschen Bundesrat für seine Stellungnahmen und mit Gründen versehenen Stellungnahmen zu dem Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) {COM(2012) 10 final} und dem Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.{COM(2012) 11 final}. Bitte entschuldigen Sie, dass unsere Antwort so lange hat auf sich warten lassen.

Nach Auffassung des Bundesrats sind beide Vorschläge nicht mit dem Subsidiaritätsprinzip vereinbar. Des Weiteren nimmt der Bundesrat Stellung zu einzelnen Bestimmungen der beiden Vorschläge.

Die Kommission möchte hervorheben, dass das von ihr im Januar dieses Jahres vorgeschlagene Datenschutz-Reformpaket darauf zielt, eine moderne, starke, kohärente und umfassende Datenschutzregelung für die Europäische Union auf den Weg zu bringen. Diese Regelung käme natürlichen Personen zugute, da sie ihre Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten stärken, ihr Vertrauen in die Online-Umgebung erhöhen und das rechtliche Umfeld für Unternehmen und den öffentlichen Sektor erheblich vereinfachen würde. Dies dürfte die Entwicklung der digitalen Wirtschaft im EU-Binnenmarkt und darüber hinaus entsprechend den Zielen der Strategie Europa 2020 und der Digitalen Agenda für Europa fördern.

Ferner würde die Reform das Vertrauen der Strafverfolgungsbehörden untereinander stärken, den Datenaustausch zwischen ihnen erleichtern und die Zusammenarbeit bei der Bekämpfung schwerer Kriminalität verbessern, gleichzeitig aber ein hohes Schutzniveau für den Einzelnen garantieren.

Mit diesem Reformpaket kommt die Kommission nachdrücklichen Aufforderungen durch den Rat[1] und das Europäische Parlament[2] sowie von verschiedenen Interessenträgern

---

1 Schlussfolgerungen des Rates zur Mitteilung der Kommission an das Europäische Parlament und den Rat – Gesamtkonzept für den Datenschutz in der Europäischen Union, 3071. Tagung der Justiz- und Innenminister in Brüssel, 24. und 25. Februar 2011.

2 Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union P7_TA_(2011)0323.

nach, einen qualitativ hochwertigen Rechtsrahmen auf der Grundlage eines umfassenden Ansatzes vorzulegen.

Die Kommission ist der Ansicht, dass beide Vorschläge mit dem Subsidiaritätsprinzip uneingeschränkt vereinbar sind. Sie nimmt im Anhang zu diesem Schreiben zu diesem Punkt Stellung sowie zu den anderen Punkten, die der Bundesrat in seinen Stellungnahmen angesprochen hat.

Die Kommission hofft, dass diese Erläuterungen zu einer Klärung der vom Bundesrat angesprochenen Punkte beitragen, und sieht einer Weiterführung des politischen Dialogs erwartungsvoll entgegen.

Mit vorzüglicher Hochachtung

Maroš Šefčovič
Vizepräsident

ANHANG

I. Der Vorschlag für eine Datenschutz-Grundverordnung {COM(2012) 10 final}

1. Die Notwendigkeit einer Verordnung

Gemäß der europäischen Rechtsprechung zielt die aktuelle Datenschutzrichtlinie (95/46/EG von 1995) auf die Harmonisierung der Datenschutzvorschriften in allen Mitgliedstaaten. Doch, wie der Gerichtshof wiederholt klargestellt hat, sollte die Harmonisierung der nationalen Rechtsvorschriften zu einer grundsätzlich umfassenden Harmonisierung führen und nicht auf eine Mindestharmonisierung beschränkt sein (vgl. z. B. Rechtssache C-101/01, Randnr. 96 ff. und die verbundenen Rechtssachen C-468/10 und 469/10, Randnr. 35).

Folglich verpflichten die derzeitigen Rechtsvorschriften die Mitgliedstaaten bereits, ein harmonisiertes Schutzniveau einzuhalten. Die Erfahrung hat allerdings gezeigt, dass die Umsetzung der Richtlinie von 1995 in nationale Rechtsvorschriften und Gepflogenheiten in den Mitgliedstaaten in einigen Fällen zu weit reichenden Unterschieden bei der Auslegung und Anwendung der Datenschutzbestimmungen geführt hat. Des Weiteren gibt es signifikante Unterschiede in Bezug auf die Stellung, die Ressourcen und die Befugnisse der Datenschutzaufsichtsbehörden. Dies hat zur Folge, dass die in den Mitgliedstaaten auf der Grundlage der Richtlinie erlassenen Datenschutzvorschriften unterschiedlich durchgeführt werden. Die Fragmentierung des rechtlichen Rahmens und die Anwendung der Rechtsvorschriften auf 27 verschiedene Datenschutzsysteme haben Rechtsunsicherheit zur Folge und führen dazu, dass den Bürgern kein einheitliches Schutzniveau geboten werden kann.

Das durch Artikel 8 der Charta der Grundrechte der Europäischen Union und durch Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verankerte Recht auf den Schutz personenbezogener Daten erfordert allerdings ein einheitlich hohes Schutzniveau in allen Mitgliedstaaten, zumal die Bürger zunehmend Dienstleistungen in anderen Ländern in Anspruch nehmen oder die Verarbeitung ihrer Daten in anderen Ländern erfolgt. Dieses einheitliche Schutzniveau lässt sich nur erreichen, wenn in allen Mitgliedstaaten einheitliche Rechtsvorschriften angewandt werden, die auch Bestimmungen über die Übermittlung von Daten an Drittstaaten und internationale Organisationen umfassen. Ohne eine vollständige Rechtsangleichung kann auch der Europäische Binnenmarkt nicht ordnungsgemäß funktionieren. Wenn es den Mitgliedstaaten überlassen bliebe, den Datenschutz an weitere Bedingungen zu knüpfen, die über das einheitlich hohe Schutzniveau hinausgehen, würden die verschiedenen Auflagen, die die Mitgliedstaaten den Unternehmen machen, unnötige Kosten und einen vermeidbaren Verwaltungsaufwand generieren, was die Ziele der Reform, das Potenzial des digitalen Binnenmarktes freizusetzen und Wirtschaftswachstum, Innovation und Beschäftigung zu fördern, unterlaufen würde.

Eine Verordnung ist aufgrund ihrer unmittelbaren Anwendbarkeit das geeignetste Instrument zur Festlegung von Regeln zum Schutz personenbezogener Daten. Eine Verordnung wird die derzeitige rechtliche Fragmentierung beenden und dadurch die Rechtssicherheit und den Schutz der Grundrechte in der Europäischen Union erhöhen und das Funktionieren des Binnenmarktes verbessern.

2. Anwendungsbereich der Verordnung

Da alle personenbezogenen Daten zwischen den Mitgliedstaaten ausgetauscht werden können, kann die Anwendbarkeit der Verordnung nicht davon abhängen – wie dies bei der derzeitigen Richtlinie 95/46/EG der Fall ist –, ob in dem betreffenden Fall ein hinreichender Zusammenhang mit dem freien Datenverkehr zwischen den Mitgliedstaaten besteht (vgl. Rechtssachen C-465/00, C-138/01 und C-139/01, Randnr. 40-43). Aus diesem Grund darf die „lokale Datenverarbeitung" aus dem Anwendungsbereich der Verordnung, der über die Verarbeitung von Daten zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht (Artikel 2 Absatz 2 Buchstabe d) hinausgeht, nicht ausgenommen werden.

Der Verordnungsvorschlag setzt die bewährte Tradition der derzeitigen Datenschutz-Richtlinie 95/46/EG fort, indem er zwischen dem öffentlichen Raum und der Privatsphäre keinen Unterschied macht. Was den Schutz personenbezogener Daten angeht, so wird weder in Artikel 8 der Grundrechte-Charta noch in Artikel 16 Absatz 1 AEUV ein Unterschied zwischen Behörden oder anderen Daten verarbeitenden Stellen gemacht. Darüber hinaus kann die Trennung der öffentlichen von der privaten Sphäre – abhängig von den Rechtssystemen in den einzelnen Mitgliedstaaten – zu Problemen führen. Im Einklang mit dem Anwendungsbereich der bestehenden Rechtsvorschriften und dem Ziel der Kommission, dass das vorgeschlagene Rechtsinstrument einen umfassenden rechtlichen Rahmen für den Datenschutz in der EU gewährleisten soll, sollte die vorgeschlagene Verordnung sowohl für die öffentliche als auch für die private Sphäre gelten.

3. Handlungsspielraum der nationalen Parlamente

Die Wahl einer Verordnung bedeutet nicht, dass den nationalen Parlamenten jeglicher Spielraum abgesprochen wird. Die vorgeschlagene Verordnung sieht ebenso wie die derzeitige Datenschutzrichtlinie vor, dass zu den Umständen, unter denen die Datenverarbeitung rechtmäßig ist, auch Situationen gehören, in denen die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt (Artikel 6 Absatz 1 Buchstabe e). Die vorgeschlagene Verordnung sieht auch vor, dass die Verarbeitung eine Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, haben muss (Artikel 6 Absatz 3).

Da die Datenverarbeitung durch Behörden eine Rechtsgrundlage erfordert, die insbesondere dem Grundsatz der Verhältnismäßigkeit Rechnung trägt, bedeutet dies mit Bezug auf den öffentlichen Sektor, dass in den Rechtsvorschriften einiger Mitgliedstaaten die Einzelheiten des öffentlichen Interesses an der Datenverarbeitung, die damit verfolgten Zwecke und die Bedingungen für die Verarbeitung im Rahmen des Verordnungsvorschlags noch festgelegt werden müssten. Da die vorgeschlagene Verordnung auf Regeln für den Datenschutz in sektorspezifischen Rechtsvorschriften beschränkt ist, berührt sie nicht das allgemeine Verfahrensrecht der Mitgliedstaaten.

In bestimmten Bereichen sieht die vorgeschlagene Verordnung ausdrücklich vor, dass die Mitgliedstaaten Rechtsvorschriften erlassen, beispielsweise bei der Definition der Beziehung zwischen der Verarbeitung personenbezogener Daten und der freien Meinungsäußerung (Artikel 80), der Verarbeitung personenbezogener Gesundheitsdaten (Artikel 81) oder der Datenverarbeitung im Beschäftigungskontext (Artikel 82). Desgleichen beziehen sich andere Bestimmungen auf die Rechtsvorschriften der

Mitgliedstaaten, z. B. in Bezug auf die Verarbeitung besonderer, sensitiver Daten, die Auflage, Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorzusehen (Artikel 9 Absatz 2 Buchstabe g) oder notwendige Beschränkungen der Anwendung bestimmter Vorschriften (Artikel 21). Auch im Zusammenhang mit den Datenschutz-Aufsichtsbehörden erlassen die Mitgliedstaaten nationale Rechtsvorschriften (Artikel 46 Absatz 3). Die vorgeschlagene Verordnung trägt den föderalen Strukturen Rechnung, indem sie vorsieht, dass in einem Mitgliedstaat eine oder mehr Aufsichtsbehörden für die Überwachung der Anwendung der Verordnung zuständig sind (Artikel 46 Absatz 1) Im Rahmen der vorgeschlagenen Verordnung haben die Mitgliedstaaten zweifellos die Möglichkeit, national, historisch oder kulturell geprägten Merkmalen Rechnung zu tragen.

4. Delegierte Rechtsakte

Ist in der vorgeschlagenen Verordnung vorgesehen, dass die Kommission detailliertere Vorschriften mittels delegierter Rechtsakte festlegt, so gilt dies für die Anwendung spezifischer Bestimmungen auf der Grundlage von Artikel 290 AEUV, sofern und wenn dies erforderlich ist. Die Befugnisse, delegierte Rechtsakte zu erlassen, betreffen kein zentrales Element des vorgeschlagenen Rechtsakts. Die wichtigsten Bestimmungen sind in dem Vorschlag enthalten, wodurch dieser anwendbar ist, ohne dass im Vorfeld delegierte Rechtsakte erlassen werden müssen.

Die Alternative, d.h. die Festlegung detaillierter Vorschriften für die Anwendung der einzelnen Bestimmungen in bestimmten Sektoren und Situationen in dem Vorschlag, wäre ein unflexibler und sperriger Rechtstext, der Innovationen und neuen Technologien gegenüber nicht aufgeschlossen wäre und der den Spielraum, um gemeinsame Ansätze im Europäischen Datenschutzausschuss zu finden, beschneiden würde.

5. Das Kohärenzverfahren und die Unabhängigkeit der Aufsichtsbehörden

Die vorgeschlagene Verordnung stärkt die Unabhängigkeit und die Befugnisse der Aufsichtsbehörden gemäß den einschlägigen Urteilen des Gerichtshofs (Artikel 46ff.). Das Kohärenzverfahren verleiht der Kommission nicht die Möglichkeit, auf die unabhängigen Datenschutz-Aufsichtsbehörden Einfluss zu nehmen. Es soll ein Konsens zwischen den Datenschutz-Aufsichtsbehörden im Europäischen Datenschutzausschuss gefördert werden. Entscheidungen in bestimmten Fällen und die Durchführung sollen grundsätzlich den zuständigen nationalen Datenschutzbehörden überlassen werden. Nicht nur jedes Mitglied ist unabhängig; der Europäische Datenschutzausschuss handelt auch bei der Erfüllung seiner Aufgaben unabhängig (Artikel 65 Absatz1).

6. Anpassung der nationalen Rechtsvorschriften, insbesondere in Bezug auf elektronische Kommunikationsdienste

Artikel 88 Absatz 2 der vorgeschlagenen Verordnung, wonach Verweise auf die Richtlinie 95/46/EG – die nach Artikel 88 Absatz 1 aufgehoben würde – als Verweise auf die vorgeschlagene Verordnung gelten, bezieht sich nicht nur auf die Richtlinie 2002/58/EG sondern betrifft auch Verweise auf die Bestimmungen der derzeitigen Datenschutzrichtlinie.

Artikel 89 der vorgeschlagenen Verordnung zeigt, dass der Vorschlag natürlichen oder juristischen Personen in Bezug auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer

Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der Richtlinie 2002/85/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. In den meisten Fällen sieht der Vorschlag eine Übergangsfrist von zwei Jahren für die Änderung der nationalen Rechtsvorschriften vor (Artikel 91 Absatz 2).

7. Abgrenzung zwischen den beiden Rechtsinstrumenten

Im Gegensatz zur Datenschutz-Grundverordnung ist die vorgeschlagene Richtlinie ein spezifisches Rechtsinstrument zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden (Artikel 1 Absatz 1, Artikel 2 Absatz 2 der vorgeschlagenen Richtlinie und Artikel 2 Absatz 2 Buchstabe e der vorgeschlagenen Verordnung). Wenn die zuständigen Behörden andere Aufgaben als das Verarbeiten von Daten für die Zwecke der Richtlinie haben, kommt die Verordnung zur Anwendung. Das schafft keine fundamental neue Situation, da jede Behörde und jeder Beamter derzeit bereits völlig unterschiedlichen Datenschutzvorschriften unterliegt, z. B. ein für Polizeikontrollen an einer Außengrenze und für die Einwanderungskontrolle zuständiger Polizeibeamter, wobei die Einwanderungskontrolle durch die Richtlinie 95/46/EG abgedeckt wird. Mit Blick auf die derzeit rechtliche Situation liegt der Unterschied darin, dass die vorgeschlagene Richtlinie Teil eines umfassenden rechtlichen Rahmens ist, mit zwei Rechtsinstrumenten, mit denen zwei Ziele – Garantierte Achtung der Grundrechte und der freie Datenverkehr - auf der Grundlage der einheitlichen Datenschutzgrundsätze verfolgt werden.

II. Der Vorschlag für eine Richtlinie zur Datenverarbeitung im polizeilichen Bereich und im Bereich der Strafjustiz {COM(2012) 11 final}

1. Rechtsgrundlage der Richtlinie

Da die vorgeschlagene Richtlinie auf die Harmonisierung der Datenschutzvorschriften der Mitgliedstaaten im polizeilichen Bereich und im Bereich der Strafjustiz zielt, wird nicht zwischen grenzübergreifendem Datenaustausch und nationaler Datenverarbeitung durch die zuständigen Behörden unterschieden. In diesem Punkt wird mit der vorgeschlagenen Richtlinie der gleiche Ansatz wie mit der Richtlinie 95/46/EG und der vorgeschlagenen Datenschutzverordnung verfolgt, bei denen auch kein Unterschied zwischen nationaler Datenverarbeitung und grenzübergreifender Datenverarbeitung gemacht wird.

Ebenso wie beim Verordnungsvorschlag ist auch bei der vorgeschlagenen Richtlinie die Rechtsgrundlage Artikel 16 Absatz 2 AEUV, der vorsieht, dass das Europäische Parlament und der Rat Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr in der Europäischen Union erlassen. Weder dieses Erfordernis noch der Schutz des Einzelnen, der durch Artikel 8 der Charta der Grundrechte der Europäischen Union und Artikel 16 Absatz 1 AEUV garantiert ist, ist auf die Datenverarbeitung mit grenzübergreifenden Auswirkungen beschränkt. Dies entspricht auch der Rechtsprechung des Gerichtshofs, wonach die Anwendung der Richtlinie 95/46/EG nicht voraussetzen kann, dass ein Zusammenhang mit dem freien Datenverkehr zwischen den Mitgliedstaaten besteht (vgl. Rechtssachen C-465/00, C-138/01 und C-139/01, Randnummern 40-43).

Da alle personenbezogenen Daten zwischen den Mitgliedstaaten übermittelt werden können – dies haben einige Mitgliedstaaten während der Konsultation der Kommission bestätigt -, könnte die Unterscheidung zwischen nationaler und grenzübergreifender Datenverarbeitung sogar praktische Probleme für die betreffenden Behörden zur Folge haben, z.B. wenn bei Ermittlungsverfahren zwischen Daten unterschiedlicher Herkunft unterschieden werden muss, so dass die Verarbeitung dieser Daten unterschiedlichen Vorschriften unterliegen können. In der Praxis ist es auf jeden Fall unwahrscheinlich, dass es eine klare Trennlinie gibt zwischen personenbezogenen Daten, die in einem Land erhoben wurden und Daten, die auch zwischen Ländern ausgetauscht werden dürfen.

Der Richtlinienvorschlag betrifft die Anforderungen in Bezug auf den Schutz bei der Datenverarbeitung durch die zuständigen Behörden in dem in Artikel 2 und Artikel 1 Absatz 1 genannten Anwendungsbereich; er wirkt sich aber auf die Befugnisse der Mitgliedstaaten in Strafverfahren oder Polizeirecht oder bei der Aufrechterhaltung der öffentlichen Ordnung oder den Schutz der inneren Sicherheit nicht aus. Aus diesem Grund braucht nicht auf besondere Vorschriften des Vertrags über die polizeiliche und justizielle Zusammenarbeit in Strafsachen zurückgegriffen werden, die über die in Artikel 16 Absatz 2 AEUV enthaltene allgemeine Rechtsgrundlage für Datenschutzvorschriften hinausgehen. Deshalb lässt der Vorschlag Artikel 72 AEUV unberührt. Der Richtlinienvorschlag gilt auch nicht für die Datenverarbeitung durch die zuständigen Behörden im Zusammenhang mit anderen, nicht in den Anwendungsbereich der vorgeschlagenen Richtlinie fallenden Aufgaben.

2. Vereinbarkeit mit dem Subsidiaritätsprinzip

Bei der Vorbereitung ihrer Vorschläge schenkte die Europäische Kommission dem Subsidiaritätsprinzip besondere Beachtung und analysierte die damit zusammenhängenden Aspekte sorgfältig. Bei dieser Analyse stützte sie sich nicht nur auf einzelne Studien sondern auch auf die Ergebnisse einer umfassenden Konsultation der Beteiligten. Zusätzlich zu den öffentlichen Konsultationen in den Jahren 2009 und 2010/2011 veranstaltete sie Anhörungen mit Vertretern von Strafverfolgungsbehörden. Am 29. Juni 2010 fand unter Beteiligung der Behörden der Mitgliedstaaten ein Workshop zur Anwendung der Datenschutzvorschriften in Ämtern statt, wozu auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen gehörte. Am 2. Februar 2011 veranstaltete die Kommission einen Workshop mit den Behörden der Mitgliedstaaten, um die Durchführung des Rahmenbeschlusses 2008/977/JI und Datenschutzthemen im Zusammenhang mit der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu erörtern.

Die Auswertung der Analyse zum Subsidiaritätsprinzip hat ergeben, dass – zusätzlich zu dem gemäß Artikel 8 der Grundrechtecharta und Artikel 16 Absatz 1 AEUV geforderten einheitlichen Datenschutzniveau – aus folgenden Gründen im Bereich polizeiliche und strafrechtliche Angelegenheiten Maßnahmen auf EU-Ebene erforderlich sind:

Die Strafverfolgungsbehörden in den Mitgliedstaaten haben zur Bekämpfung von Kriminalität und Terrorismus, die an den nationalen Grenzen nicht haltmachen, einen ständig steigenden Bedarf an immer schnellerer Datenverarbeitung und Datenaustausch. Einheitliche und eindeutige Datenschutzvorschriften auf EU-Ebene würden zum Ausbau der Zusammenarbeit zwischen diesen Behörden beitragen.

Aufgrund der praktischen Schwierigkeiten bei der Durchführung der Datenschutzvorschriften und der nötigen Zusammenarbeit zwischen den Mitgliedstaaten und ihren Behörden ist die Organisation auf EU-Ebene erforderlich, um die einheitliche Durchführung der Rechtsvorschriften der Europäischen Union zu gewährleisten. In bestimmten Situationen ist die EU am besten in der Lage, sicherzustellen, dass bei der Übermittlung personenbezogener Daten an Drittstaaten alle Betroffenen effektiven und gleichen Schutz genießen.

Im Alleingang können die Mitgliedstaaten die bestehenden Probleme, besonders die durch den Mangel an einheitlichen nationalen Rechtsvorschriften hervorgerufenen Probleme, nicht bewältigen. Deshalb besteht ein besonderer Bedarf an einem harmonisierten und kohärenten System, das die reibungslose Übermittlung personenbezogener Daten innerhalb der EU ermöglicht und gleichzeitig für alle Betroffenen effektiven Datenschutz EU-weit garantiert.

Aufgrund der Art und des Ausmaßes der Probleme, die nicht auf einen oder mehrere Mitgliedstaaten beschränkt sind, wäre eine Datenschutzrichtlinie in diesem Bereich insgesamt wirksamer als vergleichbare Maßnahmen auf Ebene der Mitgliedstaaten.

3. Bestehende internationale Übereinkünfte der Mitgliedstaaten

Die den Mitgliedstaaten auferlegte Pflicht, vor Inkrafttreten der vorgeschlagenen Richtlinie geschlossene internationale Übereinkünfte zu prüfen und gegebenenfalls (z.B. wenn das Übereinkommen nicht mit den Bestimmungen der Richtlinie vereinbar ist) zu ändern (Artikel 60), ist zur Gewährleistung des gleichen Datenschutzes EU-weit

erforderlich. Anderenfalls bestünde die Gefahr, dass Daten an Drittstaaten übermittelt würden, die keinen adäquaten Datenschutz garantieren und so das durch den Richtlinienvorschlag garantierte Schutzniveau und damit auch das gegenseitige Vertrauen zwischen den Mitgliedstaaten unterlaufen, auf dem die Bestimmungen des Vorschlags zur Übermittlung von Daten in Drittstaaten oder an internationale Organisationen (Artikel 33 – 38) basieren. Die in dem Richtlinienvorschlag enthaltenen Standards sind fester Bestandteil des EU-Rechts und müssen als solche Vorrang haben vor Maßnahmen der Mitgliedstaaten, einschließlich zuvor geschlossener Übereinkünfte. Bestehende Übereinkünfte zu ändern, gehört zur Pflicht der Mitgliedstaaten, alle erforderlichen Maßnahmen zu ergreifen, um den sich aus den Verträgen oder Rechtsakten der EU-Organe ergebenden Verpflichtungen nachzukommen (Artikel 4 Absatz 3 des Vertrags über die Europäische Union). Artikel 351 AEUV bezieht sich auf internationale Übereinkünfte, die vor dem im ersten Absatz dieser Bestimmung genannten Zeitpunkt geschlossen wurden.

Nur Übereinkünfte betreffend den Datenaustausch, die nicht mit der Richtlinie vereinbar sind, müssen geändert werden. Die für Änderungen vorgesehene Frist - fünf Jahre nach Inkrafttreten der vorgeschlagenen Richtlinie - ist wesentlich länger als die für die Durchführung der Richtlinie vorgesehene Frist von zwei Jahren (Artikel 62 Absatz 1).

4. Die Datenschutzbeauftragten

Die Bestimmungen über die Datenschutzbeauftragten in dem Richtlinienvorschlag beschränken sich auf die Benennung (Artikel 30), die Stellung (Artikel 31) und die Aufgaben (Artikel 32) der Datenschutzbeauftragten. Diese Elemente sind zur Beschreibung der Funktion der Datenschutzbeauftragten erforderlich. Allerdings haben die Mitgliedstaaten weiterhin das Recht, die Struktur der Behörde festzulegen (vgl. Artikel 30 Absatz 3) und, wie aus dem Wort „mindestens" in Artikel 32 hervorgeht, die Datenschutzbeauftragten auch mit anderen Aufgaben zu betrauen.