Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Innenausschuss
A-Drs. 17(4)546

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

Vorsitzender des Innenausschusses
des Deutschen Bundestages
Herrn Wolfgang Bosbach, MdB
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin
TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL eu-datenschutz@bfdi.bund.de
INTERNET www.datenschutz.bund.de

DATUM Bonn, 02.07.2012

Sehr geehrter Herr Vorsitzender,

die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu den von der Europäischen Kommission am 25. Januar 2012 vorgelegten Vorschlägen für eine Reform des europäischen Datenschutzes folgende Stellungnahmen abgegeben, die ich Ihnen hiermit übersende

- Stellungnahme zum Vorschlag für eine Datenschutz-Grundverordnung, KOM(2012) 11 endgültig
- Kernpunkte der Stellungnahme zum Vorschlag für eine Datenschutz-Grundverordnung
- Stellungnahme zum Vorschlag für eine Richtlinie 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, KOM(2012) 10 endgültig
- Kernpunkte der Stellungnahme zum Vorschlag der vorgenannten Richtlinie

Mit freundlichen Grüßen
in Vertretung

Gerhold

Innenausschuss
Eingang mit Anl. am 5.7.2012/3400
1. Vors. m.d.B. um
Kenntnisnahme/Rücksprache
2. Mehrfertigungen mit/ohne An... an Abg. BE, Obl, Sekr.
A-Drs

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge

Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

zur

Richtlinie 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

KOM(2012) 10 endg. vom 25.01.2012

11. Juni 2012

Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Richtlinie auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungsvorgänge im Bereich der Gefahrenabwehr, der Strafverfolgung und des Strafvollzugs erstreckt, bewertet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) den Richtlinienentwurf wie folgt:

Zielsetzung der Richtlinie

Die Richtlinie sollte durch Mindeststandards für die Mitgliedstaaten ein möglichst hohes Datenschutzniveau festschreiben. Den Mitgliedstaaten sollte die Möglichkeit verbleiben, in ihrem nationalen Recht über die Richtlinie hinausgehende datenschutzfreundlichere Regelungen zu treffen. Diese grundsätzliche Weichenstellung sollte in der Richtlinie selbst vorgenommen werden.

Eine solche Klarstellung würde nicht nur die durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) entwickelten Datenschutzgrundsätze wahren (z. B. Rechtsprechung zum Kernbereich der privaten Lebensgestaltung), sondern es darüber hinaus den nationalen Verfassungsgerichten ermöglichen, den Grundrechtsschutz in Zusammenarbeit mit dem Europäischen Gerichtshof weiterzuentwickeln.

Ohne entsprechende Festlegungen in der Richtlinie bestünde die Gefahr, dass grundrechtswahrende nationale Regelungen angesichts der Vorgaben der Richtlinie (die Gewährleistung des Datenschutzes und Sicherstellung des Datenaustauschs zwischen den Mitgliedstaaten gemäß Art. 1 (2) lit. b)) im Sinne einer Vollharmonisierung als richtlinienwidrig ausgelegt werden. Eine entsprechende Auslegung wäre vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs für den Bereich der geltenden Datenschutzrichtlinie 95/46/EG keineswegs ausgeschlossen und hätte unvertretbare Konsequenzen, etwa im Hinblick auf die im Strafprozess- und im Polizeirecht enthaltenen Schutzvorkehrungen für die Rechte der Betroffenen.

Zu den einzelnen Bestimmungen wird folgendermaßen Stellung genommen:

<u>Kapitel I – Allgemeine Bestimmungen</u>

Anwendungsbereich (Art. 1-2)

Die Richtlinie ist gemäß Art. 2 (1) sachlich nur anwendbar, wenn eine „zuständige Behörde" zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung

von Straftaten oder der Strafvollstreckung personenbezogene Daten verarbeitet. Nicht erfasst sind damit Aufgaben im Bereich der Abwehr von Gefahren, die nicht der Abwehr von Straftaten dient (Beispiel: Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat oder nach Strafunmündigen). Inwieweit andere Aufgaben im Bereich der Grenzkontrolle, des Zolls oder des Aufenthaltsrechts, die je nach der Tradition des Mitgliedstaates als eine polizeiliche Aufgabe verstanden werden, ebenfalls in den Anwendungsbereich der Richtlinie fallen, dürfte innerhalb der Mitgliedstaaten der EU durchaus unterschiedlich beurteilt werden. Nach Auffassung der Konferenz sollte vermieden werden, dass dieselbe polizeiliche Tätigkeit in einem Mitgliedstaat der Verordnung und in einem anderen Mitgliedstaat der Richtlinie unterfällt. Für die deutschen Polizeibehörden dürfte aus der vorgesehenen Bestimmung der Anwendungsbereiche von Datenschutz-Grundverordnung und Richtlinie folgen, dass sie in ihrem heutigen Aufgabenbereich sowohl die Datenschutz-Grundverordnung als auch die Richtlinie anzuwenden hätte. Zwar sind Abgrenzungsprobleme für Behörden mit polizeilichen Aufgaben nicht neu, wie etwa im Bereich von Zollverwaltung und Zollfahndung schon heute deutlich wird. Dennoch sollte der daraus folgenden Schwierigkeit der Abgrenzung nach Auffassung der Konferenz in erster Linie dadurch abgeholfen werden, weitest gehende Konsistenz zwischen der Datenschutz-Grundverordnung und der Richtlinie herzustellen.

Soweit der vorgeschlagene Rechtsakt Mindestanforderungen auch für die innerstaatliche Datenverarbeitung bei Polizei- und Strafverfolgungsbehörden umfasst, entspricht dies der schon vor einigen Jahren geäußerten Forderung der Konferenz. Angesichts der zunehmenden Verwirklichung des sog. Grundsatzes der Verfügbarkeit (Schwedische Initiative, Prümer Vertrag etc), wonach ein in einem Mitgliedstaat erhobenes und verarbeitetes Datum auch den Polizei- und Strafverfolgungsbehörden eines anderen Mitgliedstaats zur Verfügung stehen soll, ist die Gewährleistung eines hohen Datenschutzniveaus in allen Mitgliedsstaaten erforderlich.

In Art. 2 (2) wird der Anwendungsbereich im Hinblick auf die Umstände der Verarbeitung bestimmt (automatisiert/nicht-automatisiert). Die Konferenz weist insofern darauf hin, dass der Wortlaut insbesondere auf der Grundlage der deutschen Fassung im Unklaren lässt, ob auch Akten von dem Anwendungsbereich

umfasst sind. Im Ergebnis sollte die Richtlinie auf die Erhebung und die Verarbeitung personenbezogener Daten unabhängig von dem Verarbeitungsmedium Anwendung finden. Eine Unterscheidung zwischen automatisierter bzw. nicht-automatisierter Verarbeitung einerseits und Verarbeitung in Akten anderseits ist nicht sachgerecht. Dies sollte klargestellt werden.

Nach Art. 2 (3) lit. a) soll die Richtlinie keine Anwendung finden, sofern personenbezogene Daten im Rahmen einer Tätigkeit verarbeitet werden, die nicht in den Anwendungsbereich des Unionsrechts fällt, etwa im Bereich der „nationalen Sicherheit". Die Konferenz hält es für erforderlich, den Begriff der „nationalen Sicherheit" zu präzisieren.

Der Richtlinienvorschlag nimmt auch die Organe und Einrichtungen der EU (u. a. Europol) vom Anwendungsbereich aus. Ungeachtet der Frage, durch welches Rechtsinstrument die Einrichtungen der EU erfasst werden sollten, wäre es aus Sicht der Konferenz nicht sachgerecht, sie von den Reformbemühungen um ein erhöhtes Datenschutzniveau auszunehmen. Wenn das Ziel der Datenschutzreform ist, einen umfassenden Rechtsrahmen auf einem hohen Datenschutzniveau in Europa zu schaffen, sollte dieser auch für die Einrichtungen der EU gelten. Zwar ist nachvollziehbar, dass die komplexen Regelungen der ehemaligen 3. Säule nur schwer in einem einzigen Gesetzespaket überarbeitet werden können. Es muss jedoch vermieden werden, dass für die Einrichtungen der EU andere Maßstäbe gelten als für die Polizei- und Justizbehörden der Mitgliedstaaten. Die Konferenz regt daher eine zügigere als in Art. 60 vorgesehene Anpassung der bestehenden Vorschriften an. Es ist zumindest zu prüfen, ob das mit der Richtlinie zu setzende Mindestniveau für alle Mitgliedstaaten auch für alle bestehenden Einrichtungen der EU zum Mindestniveau erklärt werden könnte.

Begriffsbestimmungen (Art. 3)

Zu den Begriffsbestimmungen ist im Rahmen der Richtlinie auf folgende Besonderheiten hinzuweisen:

Die Definition eines Kindes in Art. 3 (13) sollte gestrichen werden, da hieran im Entwurf einer Richtlinie keine spezifischen Verarbeitungsregeln bzw. Schutzgarantien geknüpft sind.

Im Hinblick auf die Regelung in Art. 7 lit. d) sollte eine Definition für den Begriff der „Gefahr für die öffentliche Sicherheit" aufgenommen werden.

Im Hinblick auf die Regelung in Art. 16 (3) sollte die Definition der „Einschränkung der Verarbeitung" in Art. 3 (4) überarbeitet werden.

Kapitel II - Grundsätze

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten (Art. 4)

Wesentliche Grundlagen für den effektiven Schutz personenbezogener Daten sind u. a. enge Vorgaben für die Anforderungen an die Erforderlichkeit, die Zweckbindung und die Datensparsamkeit. Die Prinzipien der Datenverarbeitung gemäß Art. 4 bedürfen nach Auffassung der Konferenz insgesamt der Ergänzung und Präzisierung. Sie sollten grundsätzlich mehr Konsistenz zu den Prinzipien aufweisen, die in Art. 5 für die Datenschutz-Grundverordnung vorgeschlagen sind.

Die Regelung zur Zweckbindung in Art. 4 lit. b) enthält eine sehr offene Formulierung zur zweckändernden Weiterverarbeitung („nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise"). Sie sollte nach Auffassung der Konferenz strikter gefasst werden, insbesondere vor dem Hintergrund der unklaren und offenen Regelung des Art. 7 zur Rechtmäßigkeit der Verarbeitung. Es sollte klargestellt werden, dass Art. 4 und 7 im Zusammenwirken nicht so verstanden werden dürfen, dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzungen für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf.

Es sollte zudem eine engere Bestimmung des Grundsatzes der Erforderlichkeit in Art. 4 lit. c) formuliert werden. Die Bestimmungen „angemessen, sachlich relevant

und nicht exzessiv" stellen nach Auffassung der Konferenz nur eine schwache Begrenzung für die Zulässigkeit der Datenverarbeitung dar. Dies gilt insbesondere deshalb, weil eine Beschränkung auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß, wie sie in Art. 5 lit. c) der Datenschutz-Grundverordnung vorgesehen ist, in dem Entwurf für die Richtlinie fehlt. Zudem wird die Datensparsamkeit nicht als Grundsatz aufgeführt. Es entsteht vielmehr der Eindruck, dass der Grundsatz der Erforderlichkeit kaum mehr beinhaltet als das Verbot exzessiver Datenverarbeitung.

Als weiterer Grundsatz sollte die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten immer die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind.

In sprachlicher Hinsicht sollte es in Art. 4 lit. a) auch in der deutschen Fassung „Fairness" bzw. „faires Verfahren" anstelle von „nach Treu und Glauben" heißen.

Unterscheidungen nach Kategorien von Betroffenen, Richtigkeit und Betroffenheit (Art. 5 und Art. 6)

Der Entwurf sieht vor, dass die Mitgliedstaaten bei der Verarbeitung personenbezogener Daten sowohl im Hinblick auf verschiedene Personenkategorien (Verdächtige, verurteilte Straftäter, Zeugen, Opfer etc., Art. 5) als auch im Hinblick auf die Richtigkeit und Zuverlässigkeit der Daten (Art. 6) – so weit wie möglich – Unterscheidungen vorzunehmen haben. Unterscheidungen nach anderen Kriterien, die für das deutsche Recht maßgeblich sind, sieht der Entwurf nicht vor. Dabei geht es beispielsweise um die Frage, ob der Eingriff den Kernbereich der persönlichen Lebensgestaltung berührt oder die Daten aus besonders einschneidenden Grundrechtseingriffen (Telekommunikationsgeheimnis, Unverletzlichkeit der Wohnung) herrühren. Damit das erreichte und nach deutschem Verfassungsrecht unabdingbare Schutzniveau erhalten bleiben kann, sollte die Richtlinie Mindeststandards und keine Obergrenzen für mitgliedstaatliche Regelungen regeln.

Sowohl in Art. 5 als auch in Art. 6 bleibt offen, was aus den vorzunehmenden Unterscheidungen bzw. was aus dem Unterlassen der Unterscheidung folgen soll. Die Konferenz befürwortet insbesondere engere Grenzen für die Verarbeitung von Daten zu bestimmten Personengruppen (z. B. Opfer oder Zeugen von Straftaten).

Rechtmäßigkeit der Verarbeitung (Art. 7)

Artikel 7 enthält die zentrale Vorschrift zur Bestimmung der Rechtmäßigkeit von Datenverarbeitungen. Dabei bedarf die in Art. 7 getroffene Unterscheidung zwischen lit. a), b), c) und d) nach Auffassung der Konferenz der weiteren Erläuterung.

Ebenfalls erläuterungsbedürftig ist das Zusammenwirken dieser Vorschrift mit den in Art. 4 aufgeführten Prinzipien der Datenverarbeitung, insbesondere im Hinblick auf den Grundsatz der Zweckbindung.

Die Konferenz begrüßt, dass eine Einwilligung als Legitimation für die Datenverarbeitung im Bereich der Richtlinie ausgeschlossen ist. Ihre Anwendung ist von der Konferenz wiederholt infrage gestellt worden, insbesondere dann, wenn dadurch die Grenzen der gesetzlichen Befugnisse erweitert werden sollen.

Kapitel III – Rechte der betroffenen Personen

Rechte der Betroffenen (Art. 10-17)

Umfangreiche Rechte der Betroffenen sind wesentlich für ein hohes Datenschutzniveau. Um den Richtlinienentwurf zu einer geeigneten Grundlage für die Erweiterung der Betroffenenrechte in den Mitgliedstaaten zu machen, bedarf es einzelner Klarstellungen und Änderungen.

Besonderer Klärungsbedarf besteht im Hinblick auf Art. 17 i. V. m. Erwägungsgrund 82. Der Konferenz ist weder klar, in welchen Fällen Art. 17 anwendbar ist, noch, welche Folgen die Anwendbarkeit von Art. 17 hat. Die

Auslegung wird zudem dadurch erschwert, dass die deutsche und die englische Fassung („Gerichtsbeschluss" oder „Gerichtsdokument" / „judicial decision or record") unterschiedliche Interpretationen nahe legen. Eine Klarstellung ist in dieser Frage von besonderer Bedeutung, weil davon letztlich abhängt, ob und inwieweit die Betroffenenrechte während des gesamten staatsanwaltlichen Ermittlungsverfahrens gelten.

Nach Auffassung der Konferenz sollten die in den Art. 11-16 gewährten Rechte grundsätzlich auch im Bereich des staatsanwaltlichen Ermittlungsverfahrens Anwendung finden. Mindeststandards bezüglich der Ausgestaltung der Betroffenenrechte zählen zu den zentralen Elementen eines hohen Datenschutzniveaus und müssen auch bei der Verarbeitung personenbezogener Daten durch Staatsanwaltschaften gelten.

Darüber hinaus sind die Möglichkeiten der Mitgliedstaaten, die Betroffenenrechte einzuschränken, zu weitgehend. Als nicht vertretbar sieht die Konferenz die Regelungen in Art. 11 (5) und Art. 13 (2) der Richtlinie an. Sie eröffnen dem Gesetzgeber die Möglichkeit, bei bestimmten Datenkategorien die Information bzw. die Auskunftserteilung an den Betroffenen per se auszuschließen, ohne dass eine Abwägung im Einzelfall erfolgen muss. Es sollte vielmehr in Art. 11 und 13 klargestellt werden, dass Einschränkungen stets nur nach Prüfung des Einzelfalls zulässig sind.

Es ist nachvollziehbar, dass die Information des Betroffenen bzw. sein Auskunftsrecht in bestimmten Fällen (zunächst) beschränkt werden muss. Die Beschränkungen müssen allerdings in der Richtlinie hinreichend konkret bestimmt werden. Insofern werfen die Art. 11 (4) und Art. 13 (1) erneut Fragen auf. Sie eröffnen einen zu weiten Spielraum für den nationalen Gesetzgeber, die Rechte der Betroffenen einzuschränken.

Die Information der betroffenen Person über die Erhebung personenbezogener Daten sollte zudem unverzüglich (d. h. ohne schuldhaftes Zögern) erfolgen. Die Angabe „innerhalb einer angemessenen Frist" in Art. 11 (3) lit. b ist insoweit zu unbestimmt.

In Art. 15 sollte klargestellt werden, ob unter einem „Korrigendum" eine Richtigstellung zu verstehen ist.

Zudem sollte der Richtlinienentwurf dahingehend ergänzt werden, dass den Betroffenen in geeigneten Fällen neben dem Auskunftsrecht auch ein Akteneinsichtsrecht zu gewähren ist.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Vorschriften über die Verarbeitung Verantwortlicher und Auftragsverarbeiter (Art. 18-32)

Die Konferenz bedauert, dass die Vorschrift zu „Datenschutz durch Technik" („privacy by design") in Art. 19 keine konkreten Vorgaben macht und so zu einem reinen Programmsatz ohne praktische Auswirkungen werden könnte. Zudem könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der entstehenden Kosten in der vorliegenden Formulierung zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden.

Bei verschiedenen Vorschriften des Kapitels IV sieht die Konferenz einen weiteren Klarstellungsbedarf. Dazu gehört das Verhältnis der „unabhängigen internen oder externen Prüfer" zum Datenschutzbeauftragten und zu den Aufsichtsbehörden nach Art. 18 (3). Dazu gehören ebenso die Regelungsgehalte der Art. 20 und 22 (z. B. hinsichtlich der Kontrollpflichten des Auftragnehmers) und das Verhältnis der Art. 20 und 21 zueinander.

Die in Art. 23 (2) formulierten Dokumentationspflichten sollten ergänzt werden durch eine Beschreibung der betroffenen Personengruppen, der diesbezüglichen Daten oder Datenkategorien und durch eine Festlegung von Regelfristen zur Datenlöschung.

Die Vorschriften über die Datensicherheit (Art. 27-29) sollten um Datenschutzzielbestimmungen ergänzt werden.

Die nach Art. 27 (2) erforderliche Risikobewertung ist nur als angemessene Sicherheitsmaßnahme zu bewerten, wenn eine kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet ist. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Artikel 27 sollte daher durch die Forderung nach einem Sicherheitskonzept, welches Teil der Verfahrens-dokumentation gemäß Art. 23 (2) werden muss, ergänzt werden.

Die in Art. 28 (5) enthaltene Delegation an die Kommission bedarf der Überprüfung. Die Kriterien und Anforderungen für die Feststellung einer Verletzung des Schutzes personenbezogener Daten sind so wesentlich, dass sie im Rechtsakt selbst bestimmt werden sollten.

Die in Art. 29 (3) geregelte Pflicht zur Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten sollte nicht davon abhängig gemacht werden, ob die verantwortliche Stelle ausreichende technische Schutzmaßnahmen getroffen hat.

Bei den Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sollten in der Richtlinie entsprechend den Vorgaben der Datenschutz-Grundverordnung nicht nur die „vorherige Zurateziehung" („prior consultation") der Datenschutzbehörden, sondern auch eine Folgenabschätzung („privacy impact assessment") durch die jeweilige Stelle vorgesehen werden.

Bei den Anforderungen an den Datenschutzbeauftragten ist der Begriff der „Zuverlässigkeit" aufzunehmen (Art. 30 (2). Darüber hinaus sollte eine Verschwiegenheitspflicht des Datenschutzbeauftragten festgelegt werden sowie die Aufnahme eines Benachteiligungsverbots, eines Kündigungsschutzes und die Möglichkeit der Teilnahme an Fort- und Weiterbildungsveranstaltungen.

In Art. 32 der Richtlinie sollte zudem klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten die verantwortliche Stelle nicht von ihren eigenen Pflichten entbindet, d. h., dass sie sich nicht unter Verweis auf die Nicht- oder

Schlechterfüllung durch den Datenschutzbeauftragten exkulpieren kann. Insbesondere Art. 32 lit. a), lit. d) und lit. h) sind insoweit missverständlich.

Kapitel V - Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Die Vorschriften zu den Übermittlungen von personenbezogenen Daten in Drittstaaten sind in einem wichtigen Punkt widersprüchlich und sind insgesamt zu weit gefasst.

Im Hinblick auf die Übermittlung von personenbezogenen Daten an internationale Organisation sollte in Art. 33 klargestellt werden, dass nur solche internationale Organisationen gemeint sind, die einen Bezug zu Fragen der inneren Sicherheit aufweisen. Dies gilt ebenso für die sog. Weiterübermittlungen („onward transfers"), die in einer spezifischen Vorschrift geregelt werden sollten.

Es fehlt eine Klarstellung, dass bestehende Angemessenheitsbeschlüsse, die auf der Grundlage der RL 95/46/EG ergangen sind, für den JI-Bereich nicht gelten.

Entsprechend den bisherigen Regelungen in der Richtlinie 95/46/EG enthält der Vorschlag die Einführung von Angemessenheitsbeschlüssen zum Datenschutzniveau von Drittstaaten. Sofern die Kommission einen solchen Beschluss gefasst hat, ist die Angemessenheit des Datenschutzniveaus verbindlich festgestellt. Es bedarf allerdings der Klarstellung, dass bei Negativbeschlüssen der Kommission nach Art. 34 (5) Datenübermittlungen nur auf der Grundlage der Ausnahmen nach Art. 36, nicht aber auf der Grundlage des Art. 35 (1) vorgenommen werden dürfen. Die Vorschriften des Art. 34 (5) und Art. 35 (1) sind in dieser Frage widersprüchlich.

Die Möglichkeit der Mitgliedstaaten, personenbezogene Daten auf der Grundlage einer eigenen Einschätzung in Drittstaaten zu übermitteln, ist im Hinblick auf Art. 35 (1) lit. b) zu unbestimmt gefasst. Jedenfalls ist eine Bezugnahme auf Art. 34 (2) lit. a) vorzunehmen, der die bei der Angemessenheitsentscheidung zu berücksichtigenden

Faktoren aufführt. Darüber hinaus sollte die Einbeziehung des Auftragsverarbeiters in Art. 35 gestrichen werden.

Die Konferenz hält die Ausnahmevorschrift des Art. 36 für zu weit gefasst. Dies gilt insbesondere für lit. d) und lit. e), nach denen kaum noch eine Übermittlung denkbar ist, die nicht auf eine der Ausnahmeklauseln gestützt werden könnte. Die Konferenz regt daher im Hinblick auf die in den lit. a) bis e) enthaltenen Ausnahmevorschriften die Streichung der lit. d) und e) an. Zudem sollte in Art. 36 eine Dokumentationspflicht entsprechend des Art. 35 (2) aufgenommen werden.

Artikel 37 bezieht sich auf die Übermittlung von Daten in Drittstaaten, für die auf nationaler Ebene besondere Verwendungsbeschränkungen gelten. Insofern seien alle „vertretbaren Vorkehrungen" zu treffen, um diese Beschränkungen einzuhalten. Dies ist nach Auffassung der Konferenz zu unbestimmt und sollte daher, insbesondere auch bezüglich der zu ergreifenden technischen und organisatorischen Maßnahmen, konkretisiert werden. Die Vorschrift sollte zudem um die Verpflichtung ergänzt werden, den Empfänger der übermittelten Daten über Berichtigungs- und Löschungsansprüche zu informieren.

Artikel 37 ist nicht auf Übermittlungen zwischen den Mitgliedstaaten anwendbar. Daher muss die Richtlinie an geeigneter Stelle klarstellen, dass die in den nationalen Vorschriften der Mitgliedstaaten enthaltenen Verwendungsbeschränkungen und Mitteilungspflichten auch für Datentransfers innerhalb der Europäischen Union gelten. Die Richtlinie sollte die Daten empfangenden Mitgliedstaaten verpflichten, die Verwendungsbeschränkungen des übermittelnden Mitgliedstaates umzusetzen.

Schließlich sollte die Regelung des Art. 38 dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Schutz.

Kapitel VI und VII - Unabhängige Aufsichtsbehörden und Zusammenarbeit

Die Regelungen zur Unabhängigkeit sind grundsätzlich positiv zu werten. In Art. 39 (1) Satz 2 sollte allerdings klargestellt werden, dass die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit der Kommission sowie den anderen Aufsichtsbehörden garantiert sein muss.

Eine im Bereich von Polizei und Justiz zentrale Frage betrifft die Zuständigkeit von Datenschutzbehörden bei der Datenverarbeitung durch Gerichte im Rahmen ihrer gerichtlichen Tätigkeiten. Im Text von Art. 44 (2) sollte unmissverständlich klargestellt werden, dass der Ausschluss der Zuständigkeit der Aufsichtsbehörden sich nicht auf Akte der Exekutive bezieht, die nach nationalem Recht unter Beteiligung eines Richters zustande gekommen sind (in Deutschland etwa im Hinblick auf Maßnahmen der Strafverfolgungsbehörden, die einem Richtervorbehalt unterlegen haben).

In Art. 45 (4) sollte verdeutlicht werden, dass die Nutzung eines Formulars für Beschwerden nicht verbindlich ist und technische Schutzvorkehrungen im Sinne des Art. 27 zu treffen sind.

Die Konferenz begrüßt, dass Art. 46, insbesondere lit. b), die bisherige Ausgestaltung der aufsichtsbehördlichen Befugnisse im deutschen Recht auch weiterhin zulässt, ohne Änderungen für die Zukunft auszuschließen, wie die Verleihung von Anordnungskompetenzen. Die Frage der Ausgestaltung der Befugnisse für die Aufsichtsbehörden ist von besonderer Bedeutung und steht in engem Zusammenhang mit der Möglichkeit der gerichtlichen Auseinandersetzung zwischen der Aufsichtsbehörde und der beaufsichtigten Stelle und/oder dem Betroffenen (vgl. Art. 51).

Zur Vermeidung jeden Zweifels, der aus dem Vergleich mit der Datenschutz-Grundverordung resultieren könnte, sollte gleichfalls in der Richtlinie ausdrücklich klargestellt werden, dass Art. 46 auch den anlasslosen Zugang zu Diensträumen umfasst.

Zuletzt muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggf. durch das Sekretariat des

Datenschutzausschusses). Die Amtshilfeverpflichtung nach Art. 48 sollte durch Ausnahmevorschriften, etwa zum Schutz von Geheimhaltungsvorschriften, ergänzt werden.

Kapitel VIII - Rechtsbehelfe, Haftung und Sanktionen

Die Erweiterung der Vertretungsbefugnis für Einrichtungen, Organisationen und Verbände gemäß Art. 50 (2) ist grundsätzlich zu begrüßen.

In Art. 51 (1) sollte klargestellt werden, dass gerichtliche Rechtsbehelfe nur gegen Entscheidungen der Aufsichtsbehörde mit Regelungswirkung gegenüber Bürgern und anderen Behörden möglich sind.

In Art. 51 (2) sollte klargestellt werden, dass die vorgesehene Klagemöglichkeit gegen die Aufsichtsbehörde auf die Untätigkeit der Aufsichtsbehörde begrenzt ist. Die unklare Formulierung „wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist" sollte gestrichen werden.

Die Regelung über gemeinsame Vorschriften zum Gerichtsverfahren (Art. 53) sieht in Absatz 2 vor, dass jede Aufsichtsbehörde das Recht hat (im Englischen: „shall have the right"), Klage zur Durchsetzung der in der Richtlinie enthaltenen Rechte zu erheben. Die Konferenz spricht sich dafür aus, Art. 53 (2) so zu ändern, dass die Mitgliedstaaten eine entsprechende Berechtigung der Aufsichtsbehörden vorsehen können, jedoch nicht hierzu verpflichtet sind.

Die in Art. 54 (2) der Richtlinie vorgesehene Einführung einer gesamtschuldnerischen Haftung aller an der Verarbeitung beteiligten Stellen wird von der Konferenz als sinnvoll angesehen und daher begrüßt.

Kapitel IX und X - Delegierte Rechtsakte und Durchführungsbestimmungen, Schlussbestimmungen

Die Konferenz begrüßt, dass internationale Übereinkommen, die von den Mitgliedstaaten vor Inkrafttreten der Richtlinie geschlossen worden sind, innerhalb von fünf Jahren überarbeitet werden sollen, um sie in Übereinstimmung mit den Vorgaben der Richtlinie zu bringen (Art. 60). Es sollte klargestellt werden, dass die Richtlinie insofern nur als ein Mindestniveau anzusehen ist und in keinem Fall eine Herabstufung bestehender höherer Standards zu erfolgen hat. Die bisher fehlende Anwendbarkeit der Richtlinie auf die Einrichtungen der EU darf nicht dazu führen, dass die zwischen der EU und Drittstaaten vereinbarten Abkommen (wie etwa das TFTP-Abkommen oder das PNR-Abkommen) von dieser Regelung ausgenommen sind.

Entsprechend der allgemeinen Forderung der Konferenz sollte eine substanziellere Vorschrift für die Evaluierung der Richtlinie aufgenommen werden, als dies gegenwärtig in Art. 61 (3) vorgesehen ist. Die Evaluierungsklausel sollte auch die Hinzuziehung von externem Sachverstand enthalten

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge

Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Kernpunkte

der

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

zur Datenschutz-Grundverordnung

KOM (2012) 11 endg. vom 25.01.2012

11. Juni 2012

- Die Konferenz hält es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst **hohes Niveau** für alle Mitgliedsstaaten vorgeschrieben wird. Den Mitgliedsstaaten sollte deshalb im Sinne eines europäischen Mindestdatenschutzniveaus zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit **eröffnet** werden, durch einzelstaatliches Recht weitergehende Regelungen zu treffen (siehe Stellungnahme, Einleitung und Art. 6, 21 und 80-85).

- Die vorgesehenen zahlreichen Ermächtigungen der Kommission für **delegierte Rechtsakte** müssen im Hinblick auf den Wesentlichkeitsgrundsatz entspre-

chend Art. 290 AEUV auf das unbedingt erforderliche Maß reduziert werden. Die für den Grundrechtsschutz wesentlichen Punkte sind in der Verordnung selbst oder durch Gesetze der Mitgliedstaaten zu regeln (siehe Stellungnahme, Einleitung und Art 86 sowie u.a. Art 6, 9, 12, 20, 26 und 39).

- Ein zukunftsfähiger Datenschutz umfasst **technische und organisatorische Maßnahmen**, die Datenschutz und Datensicherheit angemessen berücksichtigen. Um dies zu gewährleisten, sind die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen aufzunehmen. Dieser Grundsatz ist in der Verordnung selbst zu verankern (siehe Stellungnahme u. a. zu Art. 5, 12, 15, Kapitel IV, Art. 23, Art. 30-32).

- Es bedarf einer strikten Reglementierung der **Profilbildung**, insbesondere deren Verbot bei Minderjährigen. Insoweit ist der unterbreitete Regelungsvorschlag stark ergänzungsbedürftig (siehe Stellungnahme zu Art. 8 und insbesondere Art. 20).

- Die Regelung des „**One-Stop-Shops**" ist für die Datenschutzaufsichtsbehörden nur praktikabel, wenn sie nicht als ausschließliche Zuständigkeit, sondern als „Federführung" zu verstehen ist. Sie sollte bei Sachverhalten, die schwerpunktmäßig die Anwendung nationalen Datenschutzrechts eines Mitgliedstaats betreffen, nicht zur Anwendung kommen. Mangels eines einheitlichen Verwaltungsverfahrens-, Verwaltungsprozess- und Verwaltungsvollstrekkungsrechts kann die Aufsichtsbehörde in anderen Mitgliedsstaaten grundsätzlich nicht selbst tätig werden. Derartige hoheitliche Maßnahmen sollten daher nur im Wege der Amtshilfe möglich sein (siehe Stellungnahme zu Art. 4, 51, 55/56).

- Das **Kohärenzverfahren** bindet die Aufsichtsbehörden in ein komplexes Konsultationsverfahren ein, was zu einer erheblichen Bürokratisierung des Datenschutzes führt und deren Unabhängigkeit beeinträchtigen kann. Es muss es stark vereinfacht, praktikabler gestaltet und insbesondere auf die wesentlichen Fallgruppen beschränkt werden (siehe Stellungnahme, Einleitung und Art. 58, Art. 59-63).

- Die durch Art. 8 der Grundrechtecharta und Art. 16 AEUV gewährleistete **Unabhängigkeit** der Aufsichtsbehörden gilt auch gegenüber der Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht in vollem Umfang vereinbar (siehe Stellungnahme, Einleitung und insbesondere Art. 47/48, 59-63).

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge

Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Datenschutz-Grundverordnung KOM (2012) 11 endg. vom 25.01.2012

11. Juni 2012

Angesichts des rasanten technologischen Fortschritts, zunehmender Vernetzung und Globalisierung ist der grundrechtsorientierte Ansatz des europäischen Datenschutzrechts mit vielfältigen Herausforderungen konfrontiert. Das durch Art. 8 der Europäischen Grundrechtecharta garantierte Grundrecht auf den Schutz personenbezogener Daten ist seit dem Inkrafttreten des Vertrags von Lissabon unmittelbar anwendbares Recht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) begrüßt deshalb das von der Kommission verfolgte Ziel eines hohen gemeinsamen Datenschutzniveaus in der gesamten Europäischen Union.

Mit der Datenschutz-Grundverordnung (Verordnung) strebt die Kommission eine Harmonisierung des Datenschutzrechts an. Die Konferenz hält es für sinnvoll und

erforderlich, einen effektiven Datenschutz für alle Bürgerinnen und Bürger in Europa zu gewährleisten. Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Verordnung auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungen im öffentlichen Bereich erstreckt, ist die Konferenz der Auffassung, dass auch insoweit ein möglichst hoher Mindeststandard gewährleistet werden muss. Es darf insgesamt zu keiner Absenkung des in den Mitgliedsstaaten bereits erreichten Schutzniveaus kommen. Die Mitgliedsstaaten sollten daher auch in Zukunft – vor allem bei besonders sensiblen Datenverarbeitungen – gesetzliche Regelungen mit einem möglichst hohen Schutzniveau erlassen dürfen. Die Verordnung muss in jedem Fall den Verfassungs- und Rechtstraditionen der Mitgliedsstaaten Rechnung tragen.

Der Entwurf ermächtigt die Kommission in einer Vielzahl von Vorschriften zu einer näheren Regelung durch delegierte Rechtsakte. Die Konferenz appelliert an das Europäische Parlament und den Rat, die Notwendigkeit jeder einzelnen Delegationsermächtigung kritisch zu überprüfen. Im Hinblick auf den Wesentlichkeitsgrundsatz müssen entsprechend Art. 290 AEUV die entscheidenden Regelungen in der Verordnung selbst getroffen oder aber im Hinblick auf fachspezifische Regelungen dem nationalen Gesetzgeber überlassen werden. Auch wenn das Parlament bei einer Ausübung der Delegationsrechte durch die Kommission auf den Erlass dieser Rechtsakte einwirken kann, ist deren demokratische Legitimation deutlich geringer, als bei einer Regelung der wesentlichen Punkte in der Verordnung selbst. Die Konferenz lehnt daher insbesondere solche delegierten Rechtsakte ab, bei denen grundlegende materiell- und verfahrensrechtliche Regelungen (wie z. B. in Art. 6 bei der Rechtmäßigkeit der Verarbeitung) konkret ausgestaltet werden sollen.

Die Konferenz weist auch darauf hin, dass der Entwurf in zahlreichen Regelungen unbestimmte Rechtsbegriffe sowie Interessenabwägungen enthält, deren hoher Abstraktionsgrad einen großen Spielraum bei der Auslegung und Anwendung zulässt.

Sie empfiehlt dringend, die notwendigen Klarstellungen in den Regelungen selbst vorzunehmen.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf vorgesehene Kohärenzverfahren, welches in der gegenwärtigen Ausgestaltung die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb stark vereinfacht und praktikabler gestaltet werden. Die durch Art. 8 der Grundrechtecharta und Art. 16 AEUV gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Die Konferenz hält es für erforderlich, die in den Art. 8 (3), 12 (6), 14 (7) und 22 (4) vorgesehenen Ausnahmen für die Datenverarbeitung kleiner und mittlerer Unternehmen (KMU) zu überprüfen. Ausnahmen sollten sich generell weniger an der Größe eines Unternehmens, sondern vielmehr an den Gefahren und Risiken für die Rechte und Freiheiten des Einzelnen orientieren. Auch von sehr kleinen Unternehmen können erhebliche Gefährdungen für den Datenschutz ausgehen.

Der Entwurf der Verordnung führt in erheblichem Umfang zu Abgrenzungsschwierigkeiten mit der RL 2002/58/EG. Art. 89 (1) ist insoweit zu abstrakt und unklar formuliert. Welche besonderen Pflichten gibt es konkret, die in der Richtlinie 2002/58/EG festgelegt sind? Weder Art. 89 noch die einschlägige Erwägung 135 geben hierüber Aufschluss.

Die Konferenz schlägt vor, eine Regelung „Erziehung und Bildung" aufzunehmen. Der Datenschutz dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamt-

gesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

„Art. Xx – Erziehung und Bildung

Um sich in der Informationsgesellschaft behaupten zu können, ist den Bürgerinnen und Bürgern durch geeignete Maßnahmen Datenschutzkompetenz zu vermitteln. Sie ist Teil der übergreifenden Medienkompetenz; ihre Vermittlung ist eine gesamtgesellschaftliche Aufgabe in den Mitgliedstaaten, die hierbei von der Union unterstützt werden."

Zu den einzelnen Regelungen nimmt die Konferenz wie folgt Stellung:

<u>Kapitel I – Allgemeine Bestimmungen</u>

Zu Art. 2:

Die Konferenz spricht sich dafür aus, dass auch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union entweder in den Geltungsbereich der Verordnung einbezogen werden (Art. 2 (2) lit. b)) oder die Verordnung 45/2001 zeitgleich angepasst wird. Es wäre nicht vertretbar, wenn sich die EU selbst von der angestrebten Modernisierung des Datenschutzrechts ausnehmen würde. Zudem spricht auch das Ziel der Harmonisierung für eine Einbeziehung der Organe der Union, da zunehmend auch zwischen diesen und den Mitgliedstaaten ein Austausch personenbezogener Daten stattfindet.

Die Beibehaltung der Ausnahme der Datenverarbeitung durch natürliche Personen zu ausschließlichen persönlichen oder familiären Zwecken in Art. 2 (2) lit. d) wird grundsätzlich begrüßt. Allerdings wäre eine Klarstellung wünschenswert, die in einer differenzierten Regelung die datenschutzrechtlichen Pflichten von natürlichen Personen angemessen ausgestaltet. Dies könnte beispielsweise in einer eigenständigen Regelung zur Veröffentlichung personenbezogener Daten an einen unbestimmten Personenkreis geschehen.

Zu Art. 3:

Die Konferenz begrüßt die Einführung des Marktortprinzips in der Verordnung.

Zum räumlichen Anwendungsbereich für Verarbeitungen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen weist sie darauf hin, dass Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen. In Vorentwürfen der Verordnung war deshalb bereits vorgesehen, dass der innerhalb der EU zu bestellende Vertreter (Art. 25) umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten solle. Dessen zusätzliche Einbeziehung in die Rechte und Pflichten wäre aus Sicht der Konferenz zu begrüßen.

Der Begriff der "Beobachtung" sollte konkretisiert werden (Art. 3 (2) lit. b)), weil nicht hinreichend klar ist, welche Anwendungsfälle hierdurch erfasst werden sollen.

Zu Art. 4:

Die Definition der „betroffenen Person" sollte ohne die Formulierung "nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde", die damit eine subjektive Komponente impliziert, wie folgt gefasst werden: "eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt von der für die Verarbeitung verantwortlichen oder jeder sonstigen natürlichen oder juristischen Person bestimmt werden kann" (Art. 4 (1)).

Es sollte auch klargestellt werden, dass Kennnummern, Standortdaten usw. zu den personenbezogenen Daten zählen (siehe Erwägungsgrund 23 der bekannt gewordenen Entwurfsfassung 56; Art. 4 (1) und (2)).

Es sollte definiert werden, was "automatisiert" bedeutet (Art. 4 (3)).

In der Definition der "Datei" sollte klargestellt werden, dass die Zugänglichkeit nach mindestens einem bestimmten Kriterium ausreicht (Art. 4 (4)).

Die Definition der "biometrischen Daten" sollte nicht nur auf die eindeutige Identifizierbarkeit abstellen, sondern auch das harmonisierte biometrische Vokabular verwenden: "Daten zu den physischen, physiologischen oder verhaltenstypischen Charakteristika eines Menschen wie Gesichtsbilder oder daktyloskopische Daten" (Art. 4 (11)).

Für Betroffene und Aufsichtsbehörden fehlt es an Transparenz und Verlässlichkeit, wenn die Hauptniederlassung über unternehmensinterne Regelungen ("Ort (...), an dem die Grundsatzentscheidungen (...) getroffen werden") bzw. über den Schwerpunkt der Verarbeitung ("Ort, an dem die Verarbeitungstätigkeiten (...) hauptsächlich stattfinden") definiert wird. Eine Präzisierung wird dringend für erforderlich gehalten, insbesondere im Hinblick auf die Regelungen des „One-Stop-Shops" in Art. 51 (2) sowie die Regelungen des gerichtlichen Rechtschutzes in Kapitel VIII.

Die Definition des „Dritten" sollte in Art. 4 aufgenommen werden, um insbesondere die Figur des Auftragsdatenverarbeiters entsprechend Art. 2 lit. f)) der RL 95/46/EG klarer zu fassen.

Die Begriffe „Anonymisierung" und „Pseudonymisierung" sollten ebenfalls definiert werden, da beiden Vorgängen materiell-rechtlich eine größere Bedeutung eingeräumt wird und aus Sicht der Konferenz auch eingeräumt werden sollte.

Kapitel II – Grundsätze

Zu Art. 5:

Als weiterer Grundsatz sollte in Art. 5 die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind, um die hohe Bedeutung des technologischen Datenschutzes zu unterstreichen.

Die Zweckbindung ist bei der Verarbeitung personenbezogener Daten eines der wichtigsten Grundprinzipien zur Gewährleistung des Datenschutzes. Im Hinblick auf

Art. 5 lit. b) sollte die Zweckbindung deshalb strikter gefasst werden. Zumindest erwartet die Konferenz die Klarstellung, dass der in der Verordnung gewählte Begriff der Zweckvereinbarkeit der Zweckbindung im Sinne des deutschen Datenschutzrechts entspricht.
In Art. 5 lit. e) sollte zusätzlich die anonyme und pseudonyme Nutzung der Daten als Gestaltungsauftrag mit aufgenommen werden. Dies sollte im Weiteren mit Regelungen zu einer Privilegierung der pseudonymen Datenverarbeitung flankiert werden.

Zu Art. 6:

Die Abwägungsklausel des Art. 6 (1) lit. f) wird in der Praxis eine herausragende Bedeutung erlangen. Die Vorgaben und Maßstäbe, anhand derer die Interessenabwägung innerhalb dieser Auffangregelung vorzunehmen ist, müssen daher hinreichend klar sein. In Art. 6 (1) lit. f) sollte eine Regelungsstruktur gefunden werden, die branchen- und situationsspezifischen Konkretisierungen Rechnung trägt. Die Verordnung sollte dabei beispielsweise auf die spezifischen Datenschutzaspekte der Auskunfteien und des Scorings eingehen. Im Hinblick auf die Verarbeitung von personenbezogenen Daten zu Direktmarketingzwecken sollte – wie in der bekannt gewordenen Entwurfsfassung 56 – grundsätzlich ein Einwilligungserfordernis (opt-in) vorgesehen werden.

Zudem erscheint es – wie Art. 20 des Vorschlags zeigt – auch denkbar, abschließende Fallgruppen zu definieren, die einer Interessenabwägung aufgrund des hohen Gefährdungspotentials der Datenverarbeitung von vornherein nicht zugänglich sind.

Vor dem Hintergrund des in Art. 290 AEUV niedergelegten Wesentlichkeitsgrundsatzes sollten die hier geforderten Konkretisierungen in der Verordnung selbst formuliert werden, da es sich um wesentliche Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten handelt. Art. 6 (5) wäre daher zu streichen.

Ausgehend von Art. 6 (3) lit. b) ist sicherzustellen, dass durch den Verweis auf das mitgliedstaatliche Recht im öffentlichen Bereich ein über die Anforderungen der Verordnung hinausgehendes Datenschutzrecht erhalten bleiben kann, wie dies in verschiedenen bundes- und landesrechtlichen Regelungen bereits jetzt verwirklicht ist. Es muss auch weiterhin ohne Zweifel gewährleistet sein, dass in einem ausdifferen-

zierten bereichsspezifischen Datenschutzrecht dem erhöhten Schutzbedarf staatlicher Datenverarbeitung auch in Zukunft Rechnung getragen wird. Dies muss sich eindeutig und ausdrücklich aus dem Wortlaut von Art. 6 (3) lit. b) ergeben. Anderenfalls wäre der derzeit bestehende besondere Schutz, beispielsweise der in der Bundesrepublik Deutschland bestehende Schutz von Sozialdaten, durch die Verordnung gefährdet.

Zu Art. 7:

Die Konferenz unterstützt die Absicht der Kommission, in Art 7 (4) die Freiwilligkeit von Einwilligungen zu konkretisieren. Sie weist allerdings darauf hin, dass ein erhebliches Ungleichgewicht nur ein Indiz für Unfreiwilligkeit sein kann.

Zu Art. 8:

Der besondere Schutz von Kindern und Jugendlichen bei der Verarbeitung der auf sie bezogenen Daten ist der Konferenz ein besonderes Anliegen. Insofern begrüßt sie, dass sich der Verordnungsentwurf dieser Thematik annimmt und sie in einer spezifischen Regelung verankern will. Die Vorschrift sollte sich jedoch stärker an den konkreten, für diese Altersgruppe spezifischen Gefährdungen orientieren. Aus diesem Grunde sollte bei Einwilligungen auch stärker auf die Einsichtsfähigkeit des Kindes und weniger auf starre Altersgrenzen abgestellt werden.

In Art. 8 (1) sollte das Regelungsziel der Norm präzisiert werden. Es ist zu klären, ob eine Beschränkung auf Dienste der Informationsgesellschaft ausreichend ist, da es sich gemäß der Begriffsbestimmung aus der Richtlinie 98/34/EG hierbei in der Regel um gegen Entgelt erbrachte Dienste handelt, obwohl offensichtlich auch entgeltfreie Dienste erfasst werden sollen. Einer Klarstellung bedarf auch, wann einem Kind solche Dienste „direkt" angeboten werden. Es ist ebenfalls zu klären, ob sich Art. 8 (1) ausschließlich auf solche Datenverarbeitungen bezieht, bei denen die Rechtmäßigkeit nach Art. 6 (1) lit. a) auf die Einwilligung gestützt wird oder ob bei jeder Datenverarbeitung der Einwilligungsvorbehalt der Eltern bzw. gesetzlichen Vertreter gelten soll.

Zudem ist das Verhältnis zwischen den Absätzen 1 und 2 des Art. 8 klärungsbedürftig.

Die Profilbildung (Art. 20) sollte bei Minderjährigen generell verboten sein.

Zu Art. 9:

Art. 9 soll den bedeutsamen Bereich der Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten regeln. Die Konferenz sieht hier den aus Art. 8 der RL 95/46/EG übernommenen Ansatz eines abschließenden Katalogs sensitiver Daten kritisch. Vorzugswürdig wäre es, auf den tatsächlichen Verarbeitungskontext abzustellen und den Katalog der sensitiven Daten als Regelbeispiele auszugestalten.
Die Vorgaben sind im Sinne des Wesentlichkeitsgrundsatzes in der Verordnung selbst zu treffen, die entsprechend zu ergänzen ist. Die in Art. 9 (3) enthaltene Delegationsermächtigung wird deshalb abgelehnt.

Zu Art. 10:

Das von der Verordnung hier offenbar verfolgte Regelungsziel wird in Erwägungsgrund 45 deutlich. Dort wird ausführt, dass der für die Verarbeitung Verantwortliche nicht verpflichtet sein sollte, zusätzliche Daten einzuholen, um eine betroffene Person zu bestimmen. Er sollte das Recht haben, bei der betroffenen Person, falls diese von ihrem Auskunftsrecht Gebrauch macht, weitere Informationen einzuholen, um die zu dieser Person gesuchten personenbezogenen Daten zu lokalisieren. Dies spiegelt sich im Wortlaut des Art. 10 jedoch nicht wider. Dieser sollte deshalb so gefasst werden, dass sich der Erwägungsgrund 45 im Regelungstext selbst niederschlägt.

Kapitel III - Rechte der betroffenen Person

Zu Art. 11:

Der Vorschlag wird grundsätzlich begrüßt. Es sollte jedoch in Abs. 1 klargestellt werden, was der für die Verarbeitung Verantwortliche (konkret) leisten muss.

Zu Art. 12:

Aus Gründen der Bestimmtheit und wegen der Erheblichkeit der hier zu treffenden Konkretisierungen sollte unmittelbar in der Verordnung selbst dargelegt werden, unter welchen Voraussetzungen ein Antrag offenkundig unverhältnismäßig ist, insbesondere auch, wann eine missbräuchliche Häufung von Betroffenenrechten vorliegt (vgl. Art. 12 (4)). Die Befugnis der Kommission zu delegierten Rechtsakten in Art. 12 (5) sollte daher entfallen.

Die Konferenz spricht sich gegen eine Missbrauchsgebühr aus. Aus ihrer Sicht reicht es aus, dass in Missbrauchsfällen das jeweilige Betroffenenrecht nicht in Anspruch genommen werden kann. Sofern an der Missbrauchsgebühr festgehalten wird, muss vermieden werden, dass sich Betroffene völlig unerwartet Gebührenforderungen gegenübersehen. Deshalb sollte der für die Verarbeitung Verantwortliche die betroffene Person im konkreten Einzelfall darüber informieren müssen, wenn er die Ausübung der Betroffenenrechte für offenkundig unverhältnismäßig erachtet und aus diesem Grund ein Entgelt verlangen will. Die Höhe des Entgelts muss verhältnismäßig sein und sich an dem tatsächlichen Aufwand bemessen.

Art. 12 sollte um das Erfordernis sicherer Übertragungswege für personenbezogene Daten nach dem Stand der Technik ergänzt werden.

Zu Art. 13:

Die Regelung wird grundsätzlich begrüßt. Die Nachberichtspflicht gemäß Art. 13 sollte sich jedoch auch auf Widersprüche nach Art. 19 erstrecken.

Zu Art. 14:

In der Verordnung ist unter Art. 14 (4) lit. b) klarzustellen, was unter einer „angemessenen" Frist zu verstehen ist. Ferner ist zu prüfen, ob anstatt dieser nicht ein „unverzügliches Handeln" geboten ist. Benachrichtigungen erst bei Datenübermittlungen

dürfen nur bei Datenverarbeitern möglich sein, die geschäftsmäßig Daten zur Übermittlung vorhalten (u. a. Auskunfteien, Adresshandel, Detekteien).

Zu Art. 15:

In Art. 15 (1) lit. g) sollte die Einschränkung auf die (lediglich) „verfügbaren" Herkunftsdaten gestrichen werden, da eine Angabe über die Herkunft personenbezogener Daten stets geboten ist und diese nicht verschleiert werden darf.

Die Aufklärungspflicht nach Art. 15 (1) lit. h) sollte auf die „Bedeutung und Tragweite" der Verarbeitung erstreckt werden. Ein (ausdrücklicher) Hinweis auf besondere Risiken bei der Profilbildung, Auskunfteien oder dem Scoring ist aufzunehmen.

Es muss zudem sichergestellt werden, dass für eine Mitteilung in elektronischer Form gemäß Art. 15 (2) nur sichere Übertragungswege nach dem Stand der Technik in Betracht kommen.

Zu Art. 16:

Es ist klarzustellen, ob unter einem Korrigendum eine Richtigstellung zu verstehen ist. Zudem regelt die Vorschrift nicht, wie zu verfahren ist, wenn sich die Unrichtigkeit oder Richtigkeit der Daten nicht beweisen lässt, bzw. wer die Beweislast trägt. Dieser Punkt sollte ergänzt werden. Denkbar wäre z. B. eine Verpflichtung, diese Daten im Sinne von Art. 17 (4) zu beschränken.

Zu Art. 17:

In Art. 17 (2) sollte eine Pflicht der Dritten zur Löschung der Daten analog Art. 17 (1) geregelt werden. Insbesondere sollte klargestellt werden, ob die Regelung auf den Bereich des Internets beschränkt ist und ob sie nach Maßgabe des Lindqvist-Urteils auch für Privatpersonen gilt.

Das Verhältnis der „umgehenden" Löschungspflicht in Art. 17 (3) zu der in Art. 12 (2) geregelten Monatsfrist ist klärungsbedürftig. Es erscheint jedenfalls nicht sinnvoll, wenn der für die Verarbeitung Verantwortliche zwar einerseits die personenbezoge-

nen Daten umgehend löschen müsste, andererseits aber für die Benachrichtigung des Betroffenen über die Löschung einen Monat Zeit hätte.

Die Formulierung in Art. 17 (2) „alle vertretbaren Schritte" bedarf insbesondere aus technischer Sicht der Präzisierung.

Die Beschränkung nach Art. 17 (4) sollte verpflichtend vorgegeben werden.

Zu Art. 18:

Die Konferenz unterstützt die Einführung eines Rechts auf Datenportabilität in Art. 18 (1). Dieses Recht sollte aber nicht davon abhängen, ob der für die Verarbeitung Verantwortliche seine Verarbeitungen in einem gängigen Format tätigt. Vielmehr sollte durch die Streichung des Wortes „gängige" eine allgemeine Konvertierungspflicht geregelt werden. Es ist klärungsbedürftig, ob Art. 18 (1) auch den öffentlichen Bereich erfasst.

Die in Art. 18 (2) verwandten Begriffe des Zur-Verfügung-Stellens und des Entziehens von Daten sollten in der Verordnung definiert werden, falls auf diese Begriffe nicht in Gänze verzichtet werden kann.

Zu Art. 19:

In Art. 19 (1) sollte der Begriff „schutzwürdige Gründe" durch „berechtigte Interessen" ersetzt werden. Es sollte zudem geprüft werden, ab wann und wie der Nachweis für das überwiegende Verarbeitungsinteresse des für die Verarbeitung Verantwortlichen als erbracht gelten soll.

Kommerzielle Werbung sollte, wie bereits zu Art. 6 angemerkt, grundsätzlich nur mit Einwilligung des Betroffenen gestattet sein. Art. 19 (2) sollte deshalb entsprechend angepasst werden. Die Konferenz empfiehlt zudem, den Begriff „unentgeltlich" in Art. 19 (2) zu streichen, da sich die Unentgeltlichkeit bereits aus Art. 12 (4) Satz 1 ergibt. Andernfalls wäre im Einzelnen darzulegen, weshalb welche Maßnahmen nach Kapitel III jeweils entgeltfrei sein sollen oder nicht.

Unter Hinweis zu den Anmerkungen zu Art. 13 sollte auch Art. 19 entsprechend angepasst werden.

Zu Art. 20:

Die Konferenz unterstützt grundsätzlich die Aufnahme einer speziellen Regelung zur Profilbildung. Allerdings hält sie den Vorschlag für stark ergänzungsbedürftig.

Schon die Profilbildung selbst (z. B. in sozialen Netzwerken, beim Scoring und bei Auskunfteien) greift in erheblicher Weise in das Grundrecht auf Datenschutz ein und ist deshalb regelungsbedürftig.

Art. 20 (1) sollte zudem auf jede – auch nur teilweise automatisierte – systematische Verarbeitung zur Profilbildung Anwendung finden und daher das Wort „rein" gestrichen werden.

Bei Minderjährigen (Art. 8) sollte die Profilbildung generell verboten sein.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wird wegen ihrer besonderen Sensitivität äußerst kritisch gesehen. Dort, wo sensitive Daten für eine Prognose unerlässlich sind, wie z.B. bei der Risikobeurteilung im Krankenversicherungsbereich, müssen enge, branchenspezifische Ausnahmetatbestände eingeführt werden, die an dem Grundsatz der Erforderlichkeit auszurichten sind. In Art. 20 (3) ist zudem klarzustellen, ob die Voraussetzungen des Art. 9 kumulativ gelten sollen. Dies würde sicherstellen, dass die Verwendung besonderer Kategorien personenbezogener Daten materiell-rechtlichen Beschränkungen unterliegt und sie nicht beliebig in Profilbildungen einfließen können.

Im Hinblick auf die besonderen Risiken der Bildung von Profilen, die auf einzelne Personen bezogen werden können, ist die Wiederherstellung eines Personenbezugs bei unter Pseudonym oder einem technischen Identifikationsmerkmal geführten Profilen grundsätzlich zu untersagen.

Wegen der Erheblichkeit der in Art. 20 (5) zu treffenden Konkretisierungen und aus Gründen der Bestimmtheit sollte eine entsprechende Reglung in die Verordnung aufgenommen und die Befugnis der Kommission zu delegierten Rechtsakten gestrichen werden.

Zu Art. 21:

Statt einer Öffnungsklausel für den nationalen Gesetzgeber nur zur Beschränkung der Rechte Betroffener (Art. 21) sollten weiter reichende Betroffenenrechte gewährt werden dürfen. Dies gilt ungeachtet der bereits zu Art. 6 geforderten generellen Öffnungsklausel für den öffentlichen Bereich.

Art. 21 (1) lit. c) sollte gestrichen werden. Es ist nicht nachvollziehbar, weshalb die bisher in der RL 95/46/EG nicht vorgesehene Beschränkung in Bezug auf den Schutz sonstiger öffentlicher Interessen geboten sein soll. Zumindest sollten die Anforderungen an die Beschränkung strikter formuliert werden, damit die Betroffenenrechte nicht leerlaufen.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Ein zukunftsfähiger Datenschutz umfasst technische und organisatorische Maßnahmen, die Datenschutz und Datensicherheit angemessen berücksichtigen. Um dies zu gewährleisten, sind die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen in die Bestimmungen der Art. 23 ff. aufzunehmen.

Zu Art. 22:

Um sicherzustellen, dass eine Verarbeitung personenbezogener Daten erst dann erfolgt, wenn die geeigneten Strategien und Maßnahmen auch umgesetzt sind, sollte Art. 22 (1) wie folgt formuliert werden: „Der für die Verarbeitung Verantwortliche stellt durch *die Umsetzung* geeigneter Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann."

Art. 22 (3) sollte dahingehend ergänzt werden, dass die Entscheidung über Konsequenzen aus der Überprüfung der in den Absätzen 1 und 2 genannten Maßnahmen

nicht dem Prüfer, sondern weiterhin dem für die Verarbeitung Verantwortlichen obliegt.

Zu Art. 23:

In Art. 23 (1) könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der Implementierungskosten zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden. Zumindest müssen – wie in Art. 30 (1) – die Implementierungskosten technisch-organisatorischer Maßnahmen in ein angemessenes Verhältnis zum konkreten Gefahrenpotential der Datenverarbeitung gesetzt werden, um eine Relation zwischen Kosten und Eingriffstiefe in das Recht auf informationelle Selbstbestimmung herzustellen.

Art. 23 (2) sollte präzisiert und um Kriterien und Anforderungen in Bezug auf die zu treffenden Maßnahmen und Verfahren ergänzt werden. Hierbei sind insbesondere Anonymisierung und Pseudonymisierung nach dem Stand der Technik zu fordern, sofern dies nicht bereits in Art. 5 geregelt wird.

Es sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft.

Die Grundeinstellungen von Produkten und Diensten sind so zu gestalten, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden und bereits ohne Zutun der Nutzer eine datenschutzfreundliche Nutzung sichergestellt wird.

Die Regelung sollte ausdrücklich auch für Verhaltensbeobachtungen ("Tracking") im Internet durch den für die Verarbeitung Verantwortlichen oder durch Dritte gelten.

Satz 2 des Art. 23 (2) sollte wie folgt lauten: „Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich *nur den von der betroffenen Person zu bestimmenden Personen* zugänglich gemacht werden." Damit soll erreicht werden, dass die betroffene Person den Personenkreis selbst bestimmt, dem ihre personenbezogenen Daten zugänglich gemacht werden dürfen, und der für die Verarbeitung Verantwortliche hierfür die entsprechenden Vorkehrungen zu treffen hat.

Zu Art. 24:

In Art. 24 sollte im Text ausdrücklich ergänzt werden, dass sich die betroffene Person zur Wahrnehmung ihrer Rechte an jeden der für die gemeinsame Verarbeitung Verantwortlichen wenden kann.

Zu Art. 25:

Die Konferenz schlägt vor, auch in den Fällen des Art. 25 (2) lit. a) einen Vertreter zu bestellen. Art. 25 (2) lit. a) sollte daher gestrichen werden.

Der in Art. 25 (2) lit. b) geplante Verzicht bei Unternehmen mit weniger als 250 Mitarbeitern auf die Benennung eines Vertreters, der umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten sollte, stellt eine Ausnahme dar, die nicht nachvollziehbar ist. Die Konferenz schlägt daher vor, diese Ausnahmeregelung ebenfalls zu streichen. Diese Klausel eröffnet weitgehende Umgehungsmöglichkeiten, da nicht geprüft werden kann, wie viele Beschäftigte bei einem nicht in der Union niedergelassenen Unternehmen tatsächlich tätig sind.

Zu Art. 26:

Der in Art. 26 (2) geregelte Mindestinhalt eines Vertrages oder Rechtsaktes zur Auftragsdatenverarbeitung sollte die wesentlichen Aspekte enthalten und daher um die Angabe von Gegenstand und Dauer des Auftrags sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung, der Art der Daten und den Kreis der Betroffenen ergänzt werden. In lit. a) sollte durch Streichung des 2. Halbsatzes sichergestellt werden, dass der Auftragsverarbeiter in jedem Fall ausschließlich auf Weisung des für die Verarbeitung Verantwortlichen tätig wird und nicht nur in besonderen Fällen, in denen die Übermittlung der Daten nicht zulässig ist.

Der Schutz der betroffenen Person erfordert die Klarstellung, dass sie sich bei gemeinsam für die Verarbeitung Verantwortlichen gemäß Art. 24 sowohl an den für die Verarbeitung Verantwortlichen als auch an den Auftragsverarbeiter wenden kann.

Eine wirksame Kontrolle des Auftragsverarbeiters kann nur umfassend erfolgen, wenn dem für die Verarbeitung Verantwortlichen in Art. 26 (2) auch ein Kontrollrecht,

beispielsweise durch einen Treuhänder, eingeräumt wird und den Auftragsverarbeiter entsprechende Mitwirkungspflichten treffen. Dies gilt auch für etwaige Unterauftragsverhältnisse.

Die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters sind wesentliche Fragen, die letztlich auch die Zulässigkeit der Auftragsdatenverarbeitung insgesamt berühren. Insbesondere wäre etwa die Einführung und nähere Ausgestaltung eines Konzernprivilegs eine wesentliche Frage, die im Sinne von Art. 290 AEUV – soweit in den Absätzen 1 bis 4 nicht ohnehin bereits geschehen – in der Verordnung selbst geregelt werden sollte. Die Konferenz sieht daher die in Art. 26 (5) vorgesehene Ermächtigung zu delegierten Rechtsakten kritisch.

Zu Art. 28:

In Art. 28 sollte geregelt werden, dass die Dokumentation grundsätzlich vor Aufnahme der Verarbeitung personenbezogener Daten zu erstellen ist. Zudem sollte der für die Verarbeitung Verantwortliche verpflichtet werden, die Dokumentation dem Datenschutzbeauftragten (soweit vorhanden) zur Verfügung zu stellen.

Die zeitliche Befristung einer Verarbeitung personenbezogener Daten ist im Sinne des Erforderlichkeitsprinzips ein wesentlicher Grundsatz. Art. 28 (2) lit. g) sollte daher in „eine *konkrete* Angabe der Fristen für die Löschung der verschiedenen Datenkategorien" geändert werden.

Zu Art. 30 bis 32 allgemein:

Verfahren mit Personenbezug müssen durch technische und organisatorische Maßnahmen, ausgerichtet an den Datenschutzzielen, geschützt werden. Dieser Grundsatz ist in der Verordnung selbst zu verankern. Die Konferenz verweist in diesem Zusammenhang auf Vorbemerkungen zu Kapitel IV. Im Übrigen sollten Aufzählungen technischer und organisatorischer Maßnahmen durch entsprechende Verweise ersetzt werden.

Zu Art. 30:

Die in Art. 30 (1) geforderten angemessenen technischen und organisatorischen Maßnahmen können nur durch eine vorab und kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet werden. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Art. 30 (1) sollte daher durch die Forderung nach einem Sicherheitskonzept ergänzt werden, welches Teil der Verfahrensdokumentation gemäß Art. 28 (2) lit. h) werden muss.

Wie in Art. 23 (1) sollte auch in Art. 30 (1) die Bezugnahme auf Implementierungskosten gestrichen werden.

Zu Art. 32:

Die in Art. 32 (3) geforderte Verschlüsselung personenbezogener Daten muss dahingehend präzisiert werden, dass sie durch Verfahren nach dem Stand der Technik erfolgen muss.

Zu Art. 33:

Eine Regelung der Datenschutz-Folgenabschätzung (Art. 33), die nachhaltig dem Schutz personenbezogener Daten dienen soll, muss die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit umsetzen, um vollumfänglich Risiken und dafür angemessene Maßnahmen identifizieren zu können. Die Ergebnisse sind in einem regelmäßigen Monitoring zu überprüfen.

Die Begriffe der Datenschutz-Folgenabschätzung und der Vorab-Genehmigung bzw. -Zurateziehung sollten voneinander abgegrenzt werden, da sich diese wechselseitig nicht ersetzen können.

Da jede der in Art. 33 (2) lit. a) genannten Auswertungen bereits erhebliche Risiken mit sich bringt, sollten die Worte „systematische und umfassende" entfallen.

Die Konferenz schlägt vor, in Art. 33 (2) lit. c) das Wort „weiträumig" zu streichen, da der Begriff zu unbestimmt ist und aus Sicht der betroffenen Person kein Unterschied besteht, ob die Überwachung weiträumig oder kleinräumig stattfindet.

In Art. 33 (2) lit. d) sollte die Durchführung einer Datenschutz-Folgenabschätzung für die Verarbeitung personenbezogener Daten aus Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten, nicht vom Umfang der Datei abhängen, sondern in jedem Fall erfolgen. Das Wort „umfangreich" sollte daher gestrichen werden.

Für die Datenschutz-Folgenabschätzung muss auch zwingend in Art. 33 (3) eine Dokumentationspflicht aufgenommen werden.

Schließlich sollte Art. 33 um einen zusätzlichen Absatz ergänzt werden, der das Verbot der Datenverarbeitung bei unangemessen hohen Eingriffen in die Rechte der Betroffenen fordert. Grundsätzlich sollten Verfahren ausgewählt werden, die den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung mit sich bringen.

Zu Art. 34:

Die Konferenz hält den Vorschlag, dass der interne Datenschutzbeauftragte die Beantragung einer vorherigen Genehmigung bzw. Zurateziehung nach Art. 37 (1) lit. f) nur überwachen soll, für nicht ausreichend. Zur Entlastung der Aufsichtsbehörden und zur Stärkung des betrieblichen Datenschutzes sollte ihm diese Aufgabe komplett übertragen werden können. Deutschland hat mit der Durchführung der Vorabkontrolle durch die internen Datenschutzbeauftragten gute Erfahrungen gemacht.

Zu Art. 35:

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv.

Es sollte eine Frist geregelt werden, innerhalb derer der Datenschutzbeauftragte nach Aufnahme der Daten verarbeitenden Tätigkeit zu bestellen ist. Die Konferenz schlägt hierfür eine Frist von einem Monat vor.

Die Konferenz bedauert, dass in Art. 35 (1) lit. b) eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten vorgesehen ist. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Art. 35 (1) lit. c) sollte dahingehend geändert werden, dass bei jeder risikobehafteten Datenverarbeitung (z.B. Auskunfteien, Detekteien, Callcenter, Lettershops etc.) unabhängig von der Mitarbeiterzahl eine Bestellungspflicht für einen Datenschutzbeauftragten besteht. Das Gleiche gilt für Unternehmen, bei denen eine Datenschutzfolgenabschätzung erforderlich ist. Die Anknüpfung an die „regelmäßige und systematische Beobachtung von betroffenen Personen" ist insoweit nicht ausreichend.

Durch die in Art. 35 (7) geregelte Möglichkeit der Befristung der Amtszeit des Datenschutzbeauftragten kann die Unabhängigkeit beeinträchtigt werden. Die Amtszeit des internen Datenschutzbeauftragten sollte daher nicht befristet werden und das dem Amt zugrunde liegende Arbeitsverhältnis nur aus wichtigem Grund kündbar sein. Die Amtszeit von externen Datenschutzbeauftragten sollte mindestens vier Jahre betragen.

Art. 35 (11) ist zu streichen. Die Fälle, in denen unabhängig von der Mitarbeiterzahl ein Datenschutzbeauftragter zu bestellen ist, betreffen eine wesentliche Frage und sind deshalb in der Verordnung selbst zu regeln.

Zu Art. 36:

Der Datenschutzbeauftragte sollte nicht nur ein unmittelbares Vorspracherecht gegenüber der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters haben, sondern dieser – als Ausdruck seiner Unabhängigkeit – unmittelbar unterstellt sein. Außerdem sollte für interne Datenschutzbeauftragte ein wirksamer arbeitsrechtlicher Kündigungsschutz sowie die Aufnahme eines Benachteiligungsverbots vorgesehen werden, um seine Unabhängigkeit besser zu sichern.

In Art. 36 (3) ist das Recht des Datenschutzbeauftragten auf Fort- und Weiterbildung sowie die Kostenübernahme hierfür zu normieren. Zudem sind Regelungen zur Verschwiegenheit des Datenschutzbeauftragten sowie zum Zeugnisverweigerungsrecht aufzunehmen.

Zu Art. 37:

Die Aufgaben des Datenschutzbeauftragten sind in der deutschen Sprachfassung missverständlich formuliert. So wird sprachlich nicht hinreichend deutlich, ob der Datenschutzbeauftragte beispielsweise selbst die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 31 vornehmen muss oder diese Meldung nur zu überwachen hat (Art. 37 (1) lit. e).

In diesem Zusammenhang sollte auch klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten den für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter nicht von seinen Pflichten entbinden bzw., dass keine Möglichkeit zur Exkulpation bei Nicht- oder Schlechterfüllung seitens des Datenschutzbeauftragten besteht.

Zu Art. 38 und Art. 39:

In Art. 39 (2) sollten die wesentlichen Regelungstatbestände einer Zertifizierung und der Vergabe eines Siegels und Zeichens direkt aufgenommen und nicht an die Kommission delegiert werden. Die Zertifizierungs- und Vergabekriterien sind insbesondere an den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5, der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6, der Betroffenenrechte und an den Datenschutzzielen in Art. 30 nach Maßgabe der Verordnung auszurichten.

Zertifizierungs-, Vergabe- und Widerrufsverfahren müssen den Anforderungen des Grundsatzes der Transparenz hinsichtlich der Kriterien, des Verfahrens und der wesentlichen Evaluierungsergebnisse genügen. Die Unabhängigkeit und Fachkunde der Zertifizierungs- und Vergabestellen und der Evaluatoren sind zu gewährleisten.

Eine datenschutzspezifische Zertifizierung gemäß Art. 39 (1) beinhaltet stets auch eine Bewertung der IT-Sicherheit. Diese sollte sich an europäischen und internatio-

nalen Standards orientieren und die Datenschutzziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit aus Betroffenensicht einbeziehen. Ein entsprechender Zusatz - unter Einbeziehung des Ergänzungsvorschlags der Konferenz zu Kapitel IV (elementare Datenschutzziele) - ist daher vorzusehen.

Zertifizierungen sind zeitlich zu befristen. Eine Rücknahme eines Zertifikates bei gravierenden Mängeln muss auch vor Fristablauf möglich sein.

Bei der Ausgestaltung der Verhaltensregeln und Zertifizierungsverfahren ist der Europäische Datenschutzausschuss zu beteiligen.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Zu Art. 41:

Die Kommission sollte bei der Angemessenheitsprüfung nach Art. 41 (2) stets auch die Stellungnahme des Europäischen Datenschutzausschusses einholen und berücksichtigen müssen. Im Zusammenhang mit Art. 41 (6) muss klargestellt werden, dass in den Fällen, in denen die Kommission durch Beschluss feststellt, dass kein angemessenes Datenschutz-Niveau gegeben ist, die Datenübermittlung automatisch verboten ist, so dass es keines weiteren Umsetzungsaktes durch die Aufsichtsbehörde bedarf.

Ferner muss klargestellt werden, ob die Formulierung „unbeschadet der Art. 42 - 44" bedeutet, dass bei einem Negativ-Beschluss gleichwohl Datenübermittlungen nach allen diesen Vorschriften vorgenommen werden können. Insbesondere die Vorschriften des Art. 41 (6) und des Art. 42 (1) erscheinen in dieser Frage widersprüchlich.

Zu Art. 42:

Da die Genehmigungsfähigkeit der Datenflüsse von vornherein fraglich ist, wenn keine geeigneten Garantien vorliegen, ist der Anwendungsbereich der Regelung des Art. 42 (5) unklar (Auffangtatbestand?). Deshalb sollte der Absatz 5 (bis auf den letz-

ten Satz) entweder gestrichen oder um die genehmigungspflichtigen Fälle präzisiert werden.

Zu Art. 43:

In Art. 43 (1) sollte die Rechtsfolge der Genehmigung der BCR durch die Aufsichtsbehörde explizit aufgenommen werden, z. B. durch folgenden Satz 2: „In diesem Fall gilt die Genehmigung in der gesamten EU."

Die in Art. 43 (3) genannten Kriterien und Anforderungen an BCR sollten nicht von der Kommission, sondern ausschließlich von dem Europäischen Datenschutzausschuss festgelegt werden.

Zu Art. 44:

Es sollte eine Klausel zum Umgang mit Aufforderungen zur Datenübermittlung durch Gerichte oder Behörden aus Drittstaaten eingefügt werden. Eine (interne) Vorversion des Vorschlags der Kommission beinhaltete eine solche explizite Klausel. Derartige Aufforderungen sollten hiernach grundsätzlich unbeachtlich sein und unter Genehmigungsvorbehalt durch zuständige nationale Behörden stehen. Die Konferenz fordert, dass Datentransfers grundsätzlich nur auf der Basis gegenseitiger Rechtshilfeabkommen (Mutual Legal Assistance Treaties, MLATs) zulässig sind.

In Art. 44 (1) müssen bei sensitiven Daten zusätzlich zur informierten Einwilligung geeignete Garantien vorgesehen werden, weil sonst zwar die Datenübermittlung nach Art. 44 (1) lit. a) legitimiert ist, die Datenverarbeitung im Drittland aber keinen besonderen Anforderungen unterliegt. Das Wort „zugestimmt" sollte durch „eingewilligt" (entsprechend Art. 7) ersetzt werden.

Art. 44 (1) lit. d) darf nicht für den Datenaustausch „zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten zuständigen Behörden" gelten, wie Erwägungsgrund 87 es vorsieht. Dies würde im Widerspruch zum sachlichen Anwendungsbereich der Verordnung nach Art. 2 (2) lit. e) stehen. Deshalb sollten diese Fälle in Erwägungsgrund 87 gestrichen werden.

Der Anwendungsbereich des Art. 44 (1) lit. h) ist unklar. Insbesondere ist fraglich, ob es sich um einen Auffangtatbestand handeln soll. Die Regelung muss konkretisiert werden. In jedem Fall muss eine Abwägung der berechtigten Interessen des für die Verarbeitung Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person vorgesehen werden.

Die Anwendungsbereiche der Art. 44 (3), (4), (6) und (7) sind unklar und müssen konkretisiert werden.

Zu Art. 45:

Art. 45 (2) sollte dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Datenschutz.

Kapitel VI – Unabhängige Aufsichtsbehörden

Zu Art. 47 und 48:

Die Regelung zur völligen Unabhängigkeit der Aufsichtsbehörden in Art. 47 (1) ist grundsätzlich positiv zu werten. Es sollte allerdings überdacht werden, wie die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit den anderen Aufsichtsbehörden, insbesondere im Rahmen des Kohärenzverfahrens, garantiert werden kann (Art. 46 (1) Satz 2).

Zu Art. 51:

Die Regelung des „One-Stop-Shops" gemäß Art. 51 (2) ist nur praktikabel, wenn sie nicht im Sinne einer ausschließlichen Zuständigkeit, sondern im Sinne einer „Federführung" der Aufsichtsbehörde des Mitgliedstaates der Hauptniederlassung zu verstehen ist, falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über mehrere Niederlassungen innerhalb der EU verfügt.

Der One-Stop-Shop-Grundsatz sollte dann nicht gelten, wenn es sich um einen Sachverhalt handelt, der im Schwerpunkt die Anwendung nationalen Datenschutzrechts eines Mitgliedstaats im Sinne des Kapitels IX betrifft, so dass es hier bei der allgemeinen Zuständigkeit nach Art. 51 (1) bleiben sollte.

Mangels eines einheitlichen Verwaltungsverfahrens-, -prozess- und -vollstreckungsrechts kann die Aufsichtsbehörde in anderen Mitgliedsstaaten grundsätzlich nicht selbst tätig werden. Derartige hoheitliche Maßnahmen sollten daher nur im Wege der Amtshilfe möglich sein. Diese Klarstellung ist auch im Hinblick auf Art. 55 (1) und (2) sowie Art. 63 notwendig.

Es sollte überprüft werden, ob die sich aus Erwägungsgrund 19 ergebende Einbeziehung rechtlich selbständiger Tochtergesellschaften in die One-Stop-Shop-Regelung tatsächlich erforderlich ist. Diese könnten aufgrund ihrer rechtlich selbständigen Handlungsfähigkeit auch getrennt betrachtet werden. Sofern eine Einbeziehung für erforderlich gehalten wird, sollte dies einschließlich einer Definition des Begriffs Tochtergesellschaft unmittelbar im Verordnungstext und nicht nur in einem Erwägungsgrund geregelt werden.

Zu Art. 52:

Ausgehend von dem Vorschlag, eine Regelung zu „Erziehung und Bildung" aufzunehmen (s.o.), sollten auch die Aufgaben der Aufsichtsbehörden entsprechend erweitert werden. Die Konferenz schlägt für Art. 52 (2) daher folgenden Wortlaut vor:

„Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über geeignete Maßnahmen zum eigenen Schutz. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder."

Die in Art. 52 (6) vorgesehene Missbrauchsgebühr sollte gestrichen werden, da nach den Erfahrungen der deutschen Aufsichtsbehörden derartige Beschwerden äußerst selten vorkommen, so dass – auch im Hinblick auf den Verwaltungsaufwand – eine Erhebung von Gebühren unverhältnismäßig wäre.

Zu Art. 53:

Die Konferenz weist darauf hin, dass auch die EU-rechtlich gebotene Unabhängigkeit der Aufsichtsbehörden nur im Rahmen der jeweiligen verfassungsrechtlichen Staatsstrukturprinzipien bestehen kann (Art. 4 Abs.2 EUV). Dies gilt insbesondere für deren Sanktionsbefugnisse und Sanktionspflichten.

Art. 53 (2) sollte auch den anlasslosen Zugang zu Geschäfts- und Diensträumen umfassen. Unklar ist, was in Art. 53 (3) mit der Formulierung, dass Verstöße gegen die Verordnung den Justizbehörden zur Kenntnis zu bringen sind, gemeint ist.

Zu Art. 54:

Art. 54 sollte gestrichen werden. Hilfsweise wird angeregt, die Aufsichtsbehörden lediglich zur Erstellung eines regelmäßigen Jahresberichts zu verpflichten, der der Öffentlichkeit (und damit automatisch dem nationalen Parlament, der Kommission, dem Europäischem Datenschutzausschuss u.a.) zugänglich gemacht werden muss.

Kapitel VII – Zusammenarbeit und Kohärenz

Zu Art. 55 und Art. 56:

In dem in Art. 55, 56 geregelten Verfahren der Amtshilfe und der Zusammenarbeit sollten die betroffenen Behörden grundsätzlich sowohl im Hinblick auf die rechtliche Bewertung eines Sachverhalts als auch hinsichtlich erforderlicher aufsichtsbehördlicher Maßnahmen einvernehmlich zusammenwirken. Dies gilt insbesondere dann, wenn es sich um eine Maßnahme der federführenden Behörde i.S.d. Art. 51 (2) handelt, die von der Aufsichtsbehörde eines anderen Mitgliedstaates durchzuführen ist. Bei Divergenzen im Hinblick auf die Bewertung eines Sachverhalts oder die Vornahme aufsichtsbehördlicher Maßnahmen sollte der Europäische Datenschutzausschuss von den beteiligten Behörden angerufen werden können.

Die Gründe, aus denen Amtshilfeersuchen nach Art. 55 (4) abgelehnt werden können, sind zu eng. Sie sollten auch zwingende Hinderungsgründe nach nationalem Recht (z. B. im Falle des Sozialgeheimnisses) umfassen.

In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter zwar über mehrere Niederlassungen innerhalb der EU verfügt, es sich aber um einen rein nationalen Sachverhalt handelt, sollte es aus Gründen der Verfahrensökonomie ebenfalls bei der allgemeine Zuständigkeitsregelung des Art. 51 (1) bleiben. Anderenfalls würde die Abstimmung mit der Hauptniederlassungsbehörde einen unverhältnismäßigen Verfahrensaufwand bedeuten. In diesen Fällen sind die Voraussetzungen der Art. 55, 56 (Betroffenheit von Personen in mehreren Mitgliedstaaten) nicht erfüllt.

Unbestimmt ist, was unter „Vorkehrungen für eine wirksame Zusammenarbeit" in Art. 55 (1) und „praktische Aspekte spezifischer Kooperationsmaßnahmen" in Art. 56 (4) zu verstehen ist. Die verfahrenstechnischen Aspekte der Amtshilfe und der Zusammenarbeit sollten in Art. 55, 56 klar formuliert werden.

Es muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggfs. durch das Sekretariat des Datenschutzausschusses).

Die Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten betreffend „Form und Verfahren der Amtshilfe (...)" in Art. 55 (10) sollte präzisiert und beschränkt werden. Das Verfahren der Amtshilfe sollte in der Verordnung, die Form der Amtshilfe und die Ausgestaltung des elektronischen Informationsaustausches im Sinne einer Standardisierung hingegen in einem Durchführungsrechtsakt geregelt werden.

Zu Art. 58:

Im Hinblick auf Art. 58 (2) lit. a) sollte klargestellt werden, ob hiervon ausschließlich der Fall des Art. 3 (2) lit. a), b) umfasst ist, oder ob auch Fälle ohne Drittlandbezug dem Kohärenzverfahren unterfallen sollen. Ansonsten würden unübersehbar viele Fälle der Kohärenz unterfallen (z. B. Versandhandel innerhalb der EU).

Zu Art. 59 – Art. 63:

Die Kompetenzen der Kommission im Verhältnis zum unabhängigen Datenschutzausschuss sowie in Bezug auf das Kohärenzverfahren (Art. 59 – 63) sind abzulehnen. Dies gilt insbesondere im Hinblick auf die umfassenden Informationspflichten des Ausschusses gegenüber der Kommission und die Befugnis der Kommission zur Aufforderung der Aussetzung aufsichtsbehördlicher Maßnahmen. Gleiches gilt hinsichtlich der Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten über die „ordnungsgemäße Anwendung" der Verordnung aus Anlass eines aufsichtsbehördlichen Einzelfalles und von „sofort geltenden Durchführungsrechtsakten" in Fällen „äußerster Dringlichkeit". Diese Kompetenzen der Kommission sind mit Art. 8 (3) Grundrechtecharta und 16 (2) Satz 2 AEUV nicht vereinbar, weil die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. Auf der Ebene der Mitgliedstaaten soll die Datenschutzkontrolle völlig unabhängig von jeglichem Einfluss erfolgen. Daher ist es widersprüchlich, wenn für die Kommission mit ihren unterschiedlichsten Aufgaben, auch solchen, die in einem Spannungsverhältnis zum Datenschutz stehen, jene Maßstäbe keine Geltung haben sollen.

Über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, sollte als Folge der Unabhängigkeit der Aufsichtsbehörden – statt der Kommission – ausschließlich der Datenschutzausschuss entscheiden. Im Hinblick auf den personellen, sächlichen und zeitlichen mit dem Kohärenzverfahren verbundenen Aufwand sollte dessen Anwendungsbereich beschränkt werden. Es wird wesentlich im Interesse der Funktionsfähigkeit des Kohärenzverfahrens und eines europaweit wirksamen Datenschutzes darauf ankommen, entsprechende Fallgruppen zu definieren. Nicht alle datenschutzrechtlichen Fragen, die auch in anderen Mitgliedstaaten der EU auftauchen können, bedürfen einer Behandlung im Kohärenzverfahren. Für dieses eignen sich insbesondere:

- Fragen des Drittstaatentransfers
- BCR mit mitgliedstaatenübergreifendem Bezug
- Konstellationen, in denen unterschiedliche Auffassungen zwischen einer nach dem One-Stop-Shop-Prinzip zuständigen Aufsichtsbehörde und einer anderen Aufsichtsbehörde nicht zu einem einvernehmlichen Ergebnis führen

- Fälle von grundsätzlicher Bedeutung für den Datenschutz in der EU, insbesondere bei einer Datenverarbeitung außerhalb der EU, falls alle Mitgliedstaaten betroffen sind und es nicht allein einer unternehmens- oder konzerninternen Verteilung von Verantwortlichkeiten überlassen bleiben kann, die verantwortliche Behörde in Europa festzulegen.

Es sollte darüber hinaus den Aufsichtsbehörden möglich sein, Fragen von sich aus an den Europäischen Datenschutzausschuss heranzutragen. Es ist zu erwägen, ob der Ausschuss in Fällen, in denen eine Aufsichtsbehörde von der Stellungnahme des Ausschusses abzuweichen beabsichtigt, eine verbindliche Stellungnahme annehmen kann, für die ein höheres Abstimmungsquorum als die einfache Mehrheit der Mitglieder zu fordern wäre.

Die Vollstreckbarkeit von Entscheidungen anderer Aufsichtsbehörden nach Art. 63 sollte unter dem Vorbehalt stehen, dass es sich hierbei um rechtmäßige Entscheidungen der nach Art. 51 zuständigen Aufsichtsbehörde handelt, die unter Beachtung der Vorschriften des Kapitel VII (Amtshilfe, Zusammenarbeit, Kohärenz) getroffen wurden.

Zu Art. 64:

Die umfassende Informationspflicht über alle Tätigkeiten des unabhängigen Ausschusses gegenüber der Kommission nach Art. 64 (4) ist unangemessen.

Zu Art. 66:

Die Streichung der in Art. 30 (1) lit. d) RL 95/46 ausdrücklich enthaltenen Befugnis zur Abgabe von Stellungnahmen zu Verhaltensregeln auf EU-Ebene wird abgelehnt. Der Ausschuss sollte ebenfalls bei der Entwicklung von Zertifizierungsverfahren mitwirken und auch, entsprechend dem jetzigen Art. 30 (1) lit. b) RL 95/46, Stellung nehmen können zum Schutzniveau in der EU und in Drittstaaten.

Es ist abzulehnen, dass die bisherige Kompetenz der Art. 29-Gruppe gemäß Art. 30 (3) RL 95/46, „von sich aus Empfehlungen zu allen Fragen" abzugeben, „die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Ge-

meinschaft betreffen", nach Art. 66 (1) lit. a) unter der einschränkenden Zweckbestimmung der Beratung der Kommission stehen soll.

Über die in Art. 66 genannten Kompetenzen hinaus sollte dem Ausschuss ein Stellungnahmerecht insbesondere zu Entwürfen der Kommission für delegierte Rechtsakte zukommen. Auf diesem Wege könnten die Expertise und die Kompetenz der Datenschutzbehörden in diesen Bereich eingebracht und gewahrt werden. Zudem würde hierdurch die Transparenz des Delegations- und Komitologieverfahrens erhöht.

Zu Art. 69:

Art. 69 (1) Satz 2 sollte gestrichen werden. Vorsitz- und Stellvertreterposten des Ausschusses sollten ausschließlich durch eine Wahl besetzt werden. Weshalb dem Europäischen Datenschutzbeauftragten zumindest die Funktion eines Stellvertreters zustehen soll, erscheint nicht nachvollziehbar, zumal die Verordnung in der derzeitigen Entwurfsfassung nicht für Organe und Ämter der EU gilt.

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Zu Art. 73 bis Art. 79:

Es ist sicherzustellen, dass durch den neuen Rechtsrahmen auch ein EU-weit wirksamer Rechtsschutz für die Betroffenen gewährleistet wird. Die in Kapitel VIII vorgesehenen Regelungen sind unklar gefasst und erfüllen diese Voraussetzungen nicht.

Länderübergreifende Klagen durch Aufsichtsbehörden im Namen Betroffener nach Art. 74 (4) gegen Aufsichtsbehörden anderer Mitgliedsstaaten können zu gegenseitigen Kontrollen der Aufsichtsbehörden führen, die im Gegensatz zum sonst geregelten Zusammenarbeitsgebot stehen würden. Es wären Klagen möglich, die der eigenen Rechtsauffassung der Aufsichtsbehörden zuwiderliefen.

Kapitel IX – Vorschriften für besondere Datenverarbeitungssituationen

Zu Art. 80 bis Art. 85:

Die Art. 81, 82 und 84 eröffnen den Mitgliedsstaaten die Befugnis, eigene Regelungen „in den Grenzen dieser Verordnung" zu treffen. Entscheidend ist, dass damit nicht nur Konkretisierungen auf der Ebene des durch die Verordnung geregelten Datenschutzniveaus möglich sind, sondern dass durch nationalstaatliche Regelungen im Interesse des Datenschutzes weitergehende Anforderungen normiert werden können. Es sollte eine ausdrückliche Klarstellung im Verordnungstext in diesem Sinne erfolgen. Eine solche Regelung müsste mit den unter Art. 6 und Art. 21 vorgeschlagenen Öffnungsklauseln für mitgliedsstaatliches Recht abgestimmt werden.

Soweit in den Art. 81 (3) und 82 (3) auf die Möglichkeit für die Kommission verwiesen wird, delegierte Rechtsakte zu erlassen, ist deren Geltung auf die Mitgliedstaaten zu beschränken, die keinen Gebrauch von der Möglichkeit gemacht haben, die betreffenden Sachbereiche selbst zu regeln. Anderenfalls würde sich der Rechtsakt selbst in Widerspruch setzen. Wenn die Mitgliedstaaten die Ermächtigung bekommen, diese Bereiche selbst zu regeln, ist nicht nachvollziehbar, warum der Kommission dennoch weitreichende Regelungskompetenzen zur Konkretisierung eingeräumt werden sollen. Diese Konkretisierungen sollten dann konsequenterweise unmittelbar von den Mitgliedstaaten selbst vorgenommen werden können.

Gesundheitsdaten dürfen nach Art. 81 (2) unter den gleichen Voraussetzungen zu historischen oder statistischen Zwecken sowie zu wissenschaftlichen Zwecken verarbeitet werden wie sonstige personenbezogene Daten. Gesundheitsdaten sollten aber auch in diesem Zusammenhang stärker geschützt werden.

Anders als die Art. 80 bis 82 sieht der Art. 83 keine Ermächtigung für die Mitgliedsstaaten vor. Die Vorschrift würde also unmittelbar geltendes Recht werden. Die Konferenz erwartet hier – ebenso wie bereits bei Art. 6 (3) ausgeführt – dass das ausdifferenzierte nationale Statistikrecht und dessen vielfach strengere Vorgaben (im Vergleich zum allgemeinen Datenschutzrecht) weiterhin bestehen bleiben können. Dies sollte in Art. 83 klargestellt werden.

In Art. 85 sollte klargestellt werden, dass sich der Vorbehalt zugunsten kirchlicher Regelungen auf die Bereiche beschränkt, die von Art. 17 AEUV erfasst werden (vgl. Erwägungsgrund 128).

Kapitel X – Delegierte Rechtsakte und Durchführungsrechtsakte

Zu Art. 86 und Art. 87:

Im Hinblick auf die Rechtssicherheit sollten die Delegationsermächtigungen nach Art. 86 auf ein Mindestmaß reduziert werden. Nach Auffassung der Konferenz sind, wie bereits ausgeführt, alle wesentlichen materiellen Fragen in der Verordnung selbst bzw. durch Gesetze der Mitgliedstaaten zu regeln.

Hinsichtlich der verbleibenden Delegationsermächtigungen sollte in die Verordnung eine Verpflichtung der Kommission zur Konsultation des Europäischen Datenschutzausschusses vor dem Erlass delegierter Rechtsakte aufgenommen werden.

Anhang: Fehler und Übersetzungsfehler

In Art. 6 (1) lit. c) sollte in der deutschen Übersetzung das Wort „gesetzlichen" durch das Wort „rechtlichen" ersetzt werden, um auch - wie bisher in Art. 7 lit. c)) der RL 95/46/EG - untergesetzliche Normen mit einzubeziehen. Der englische Wortlaut („legal obligation") ist in beiden Vorschriften identisch.

In Art. 26 (1) sollte „...dass die betreffenden technischen und organisatorischen Maßnahmen... " durch „...dass geeignete technische und organisatorische Maßnahmen..." ersetzt werden.

In Art. 26 (2) lit. f) sollte „... den Auftragsverarbeiter ..." durch „... den für die Verarbeitung Verantwortlichen..." ersetzt werden.

In Art. 30 (3) muss es im letzten Satz anstatt „Art. 4" „Abs. 4" heißen.

In den Art 11 (1), Art 22 (1), Art 37 (1) lit. b) und Art 79 (6) lit. e) sollte anstatt „Strategie" eine zutreffendere Übersetzung für "policy" gefunden werden.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge

Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Kernpunkte

der

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

zur Richtlinie 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

KOM(2012) 10 endg. vom 25.01.2012

11. Juni 2012

- Die Richtlinie sollte durch **Mindeststandards** für die Mitgliedstaaten ein möglichst **hohes Datenschutzniveau** festschreiben. Die grundsätzliche Weichenstellung, dass den Mitgliedstaaten die Möglichkeit verbleibt, in ihrem nationalen Recht über die Richtlinie hinausgehende datenschutzfreundlichere Regelungen zu treffen, sollte in der Richtlinie selbst festgelegt werden (siehe Stellungnahme, Zielsetzung der Richtlinie).

- Die **Grundsätze der Datenverarbeitung** bedürfen insgesamt der Ergänzung und Präzisierung. Insbesondere muss der Grundsatz der Erforderlichkeit enger bestimmt und eine Verpflichtung aufgenommen werden, dass bei der Datenverarbeitung auch die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind (siehe Stellungnahme zu Kapitel II).

- Der Katalog besonders schutzbedürftiger **Datenkategorien** sollte offener formuliert werden (siehe Stellungnahme zu Kapitel II).

- Die Möglichkeiten der Mitgliedstaaten, die **Betroffenenrechte** einzuschränken, müssen reduziert werden. Nicht vertretbar sind die Regelungen in Art. 11 (5) und Art. 13 (2) (siehe Stellungnahme zu Kapitel III).

- Die Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sollten entsprechend den Vorgaben der Datenschutz-Grundverordnung auch eine **Folgenabschätzung** umfassen (siehe Stellungnahme zu Kapitel IV).

- Die Konferenz hält es für wesentlich, dass **Ausnahmeregelungen** zu Übermittlungsvorschriften in Drittländer oder internationale Organisationen nicht zu weit gefasst sind. Die in Art. 36 lit. d) und e) formulierten Ausnahmen sollten gestrichen werden, da andernfalls fast jede Übermittlung darauf gestützt werden könnte (siehe Stellungnahme zu Kapitel V).