

**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

vom 11. Juni 2012

***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

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 unvermeidbare 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:

Kapitel I – Allgemeine Bestimmungen

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 andererseits 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 Gesetespaket 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. „fairer 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 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 Verfahrensdokumentation 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 Schlecht-

erfüllung 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 Ausnahmvorschrift 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 Ausnahmvorschriften 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 unterliegen 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 Anordnungs Kompetenzen. 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-Grundverordnung 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 substantiellere 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.