I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — „Gesamtkonzept für den Datenschutz in der Europäischen Union“

(2011/C 181/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [2], insbesondere auf Artikel 41 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

A. **ALLGEMEINER TEIL**

1. **Einleitung**

1.1 *Eine erste und allgemeine Beurteilung*

1. Am 4. November 2010 nahm die Kommission eine Mitteilung mit dem Titel „Gesamtkonzept für den Datenschutz in der Europäischen Union“ („die Mitteilung“) an [3]. Die Mitteilung wurde dem EDSB zur Konsultation zugesandt. Der EDSB begrüßt, dass er von der Kommission gemäß Artikel 41 der Verordnung (EG) Nr. 45/2001 konsultiert wurde. Bereits vor der Annahme der Mitteilung wurde dem EDSB die Möglichkeit zur Abgabe informeller Kommentare gegeben. Einige dieser Kommentare wurden in der endgültigen Fassung des Dokuments berücksichtigt.

2. In ihrer Mitteilung legt die Kommission ihr Konzept für eine Reform der EU-Rechtsordnung für den Schutz personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU unter besonderer Berücksichtigung der Herausforderungen der Globalisierung und der neuen Technologien dar [4].

3. Der EDSB begrüßt die Mitteilung im Allgemeinen, da er davon überzeugt ist, dass eine Überprüfung des aktuellen Rechtsrahmens für den Datenschutz der EU erforderlich ist, um einen wirksamen Schutz in einer sich weiterentwickelnden Informationsgesellschaft zu gewährleisten. Der EDSB kam bereits in seiner Stellungnahme vom 25. Juli 2007 über die Durchführung der Datenschutzrichtlinie [5] zu dem Schluss, dass auf längere Sicht Änderungen der Richtlinie 95/46/EG unvermeidlich sein dürften.

4. Die Mitteilung ist ein wichtiger Schritt in Richtung einer Rechtsänderung, die ihrerseits die bedeutendste Entwicklung im Bereich des Datenschutzes in der EU seit der Annahme der Richtlinie 95/46/EG darstellt. Diese Richtlinie wird allgemein als Eckpfeiler des Datenschutzes innerhalb der Europäischen Union (und darüber hinaus innerhalb des Europäischen Wirtschaftsraums) betrachtet.

5. Die Mitteilung stellt auch deshalb den richtigen Rahmen für eine gezielte Überprüfung dar, weil in ihr — allgemein gesagt — die wesentlichen Probleme und Herausforderungen dargelegt werden. Der EDSB teilt die Ansicht der Kommission, dass auch in der Zukunft ein starkes Datenschutzsystem benötigt wird, das auf dem Verständnis basiert, dass die bestehenden allgemeinen Datenschutzgrundsätze in einer Gesellschaft, die sich aufgrund von schnellen technologischen Entwicklungen und der Globalisierung grundlegend wandelt, weiterhin Gültigkeit besitzen. Dies erfordert die Überprüfung der bestehenden rechtlichen Regelungen.

---

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] KOM(2010) 609 endgültig.
[4] Siehe S. 5 der Mitteilung, dritter Absatz.
[5] Stellungnahme des EDSB vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“, (ABl. C 255 vom 27.10.2007, S. 1).

6. In der Mitteilung wird zu Recht herausgestellt, dass die Herausforderungen gewaltig sind. Der EDSB teilt diese Feststellung und betont die Schlussfolgerung, dass die vorgeschlagenen Lösungen entsprechend ehrgeizig sein und die Wirksamkeit des Schutzes verbessern sollten.

1.2 *Ziel der Stellungnahme*

7. Diese Stellungnahme beurteilt die in der Mitteilung vorgeschlagenen Lösungen auf der Grundlage der folgenden zwei Kriterien: Ehrgeiz und Wirksamkeit. Der Tenor der Stellungnahme ist positiv. Der EDSB unterstützt die Mitteilung, nimmt allerdings gleichzeitig eine kritische Haltung gegenüber Aspekten ein, wo seiner mehr Ehrgeiz zu einem wirksameren System führen würde.

8. Der EDSB möchte mit dieser Stellungnahme zu einer Weiterentwicklung des Rechtsrahmens für den Datenschutz beitragen. Er sieht dem für Mitte 2011 erwarteten Vorschlag der Kommission entgegen und hofft, dass seine Empfehlungen bei der Formulierung dieses Vorschlags berücksichtigt werden. Der EDSB stellt ferner fest, dass in der Mitteilung offenbar bestimmte Bereiche wie die Datenverarbeitung durch Organe und Einrichtungen der EU aus dem allgemeinen Rechtsakt ausgeklammert werden. Sollte die Kommission tatsächlich beschließen, bestimmte Bereiche in dieser Phase auszuschließen — was der EDSB bedauern würde —, so fordert der EDSB die Kommission nachdrücklich auf, sich darauf festzulgegen, innerhalb eines kurzen und klar abgesteckten Zeitraums ein umfassendes Konzept auszuarbeiten.

1.3 *Die Bausteine der vorliegenden Stellungnahme*

9. Diese Stellungnahme steht nicht für sich allein. Sie basiert auf Standpunkten, die der EDSB und die europäischen Datenschutzbehörden bereits früher zu verschiedenen Anlässen eingenommen haben. Insbesondere ist zu betonen, dass in der bereits erwähnten Stellungnahme des EDSB vom 25. Juli 2007 bestimmte Grundelemente für eine künftige Änderung dargelegt und entwickelt wurden ([6]). Die Stellungnahme basiert auch auf Diskussionen mit anderen Interessengruppen im Bereich des Schutzes der Privatsphäre und des Datenschutzes. Die Beiträge dieser Interessengruppen bieten einen sehr nützlichen Hintergrund sowohl für die Mitteilung als auch für die vorliegende Stellungnahme. Diesbezüglich kann der Schluss gezogen werden, dass ein Maß an Synergie besteht, auf dessen Grundlage die Wirksamkeit des Datenschutzes verbessert werden kann.

10. Ein weiterer wichtiger Baustein der vorliegenden Stellungnahme ist das Dokument „Die Zukunft des Datenschutzes", ein gemeinsamer Beitrag der Artikel-29-Datenschutzgruppe und der Arbeitsgruppe Polizei und Justiz zu der Konsultation, die von der Europäischen Kommission 2009 eingeleitet wurde (das „Dokument der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes") ([7]).

11. Vor kurzem hat der EDSB auf einer Pressekonferenz am 15. November 2010 seine ersten Reaktionen auf die vorliegende Mitteilung vorgestellt. In der vorliegenden Stellungnahme werden die eher allgemeinen Überlegungen ausgearbeitet, die auf der Pressekonferenz vorgestellt wurden ([8]).

12. Schließlich profitiert diese Stellungnahme von einer Reihe früherer Stellungnahmen des EDSB sowie von Dokumenten der Artikel-29-Datenschutzgruppe. In der vorliegenden Stellungnahme wird an den entsprechenden Stellen auf diese Stellungnahmen und Dokumente Bezug genommen.

2. **Kontext**

13. Die Überprüfung der Datenschutzbestimmungen findet in einem entscheidenden historischen Augenblick statt. Die Mitteilung beschreibt den Kontext ausführlich und auf überzeugende Weise. Auf der Grundlage dieser Beschreibung ermittelt der EDSB die vier Hauptfaktoren, die das Umfeld, in dem der Überprüfungsprozess stattfindet, bestimmen.

14. Beim ersten Faktor handelt es sich um die technologische Entwicklung. Die heutige Technologie ist nicht mehr dieselbe, wie zum Zeitpunkt, als die Richtlinie 95/46/EG ausgearbeitet und angenommen wurde. Technologische Phänomene, wie Cloud-Computing, verhaltensbasierte Werbung, soziale Netzwerke, Straßengebührenerhebung und elektronische Standortbestimmungsinstrumente haben die Art und Weise verändert, in der Daten verarbeitet werden, und stellen den Datenschutz vor gewaltige Herausforderungen. Eine Überprüfung der europäischen Datenschutzbestimmungen muss diese Herausforderungen auf wirksame Weise bewältigen.

15. Der zweite Faktor ist die Globalisierung. Die allmähliche Abschaffung von Handelsgrenzen hat den Unternehmen eine zunehmend weltumspannende Dimension verliehen. Grenzübergreifende Datenverarbeitung und internationale Übermittlungen haben in den vergangenen Jahren einen rasanten Anstieg erfahren. Darüber hinaus ist die Datenverarbeitung auf Grund der Informations- und Kommunikationstechnologien allgegenwärtig geworden: Internet und Cloud-Computing ermöglichen die dezentrale Verarbeitung großer Datenmengen weltweit. Im letzten Jahrzehnt war auch ein Anstieg der internationalen Tätigkeit von Polizei und Justiz zur Bekämpfung von Terrorismus und anderen Formen des internationalen organisierten Verbrechens zu beobachten, unterstützt durch einen

([6]) Insbesondere (siehe Absatz 77 der Stellungnahme): neue Prinzipien sind nicht erforderlich, aber es besteht ein eindeutiger Bedarf an anderen Verwaltungsregelungen; der breit gefasste Anwendungsbereich der Datenschutzgesetze im Hinblick auf jegliche Nutzung personenbezogener Daten sollte nicht geändert werden; die Datenschutzgesetze sollten einen ausgewogenen Ansatz in konkreten Fällen erlauben und zudem den Datenschutzbehörden ermöglichen, ihre eigenen Prioritäten zu setzen; das System sollte uneingeschränkt für die Nutzung personenbezogener Daten für die Zwecke der Strafverfolgung gelten, wobei jedoch geeignete zusätzliche Maßnahmen zur Bewältigung spezifischer Probleme in diesem Bereich erforderlich sein können.

([7]) Dokument WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp114_de.pdf). Die Hauptbotschaft ist, dass Gesetzesänderungen eine gute Gelegenheit bieten für die Klarstellung einiger wesentlicher Regeln und Grundsätze (z. B. Einwilligung, Transparenz), die Einführung einiger neuer Grundsätze (z. B. eingebauter Datenschutz, Rechenschaftspflicht), die Steigerung der Wirksamkeit durch die Modernisierung der Vereinbarungen (z. B. durch die Einschränkung der bestehenden Meldepflichten) und die Integration aller Regeln und Grundsätze in einen umfassenden Rechtsrahmen (einschließlich der polizeilichen und justiziellen Zusammenarbeit).

([8]) Die Stichpunkte der Pressekonferenz sind von der Website des EDSB abrufbar: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_DE.pdf

gewaltigen Informationsaustausch zu Strafverfolgungszwecken. All dies erfordert eine ernsthafte Erwägung der Frage, wie der Schutz personenbezogener Daten in einer globalisierten Welt wirksam gewährleistet werden kann, ohne die internationalen Verarbeitungstätigkeiten wesentlich zu behindern.

16. Der dritte Faktor ist der Vertrag von Lissabon. Mit dem Inkrafttreten des Vertrags von Lissabon beginnt eine neue Ära für den Datenschutz. Artikel 16 AEUV enthält nicht nur ein individuelles Recht der betroffenen Personen, sondern stellt auch eine direkte Rechtsgrundlage für ein starkes, EU-weites Datenschutzrecht dar. Darüber hinaus verpflichtet die Abschaffung der Pfeilerstruktur das Europäische Parlament und den Rat, den Datenschutz für alle Bereiche des EU-Rechts zu gewährleisten. Mit anderen Worten, der Vertrag von Lissabon ermöglicht einen umfassenden Rechtsrahmen für den Datenschutz, der auf den privaten und den öffentlichen Sektor in den Mitgliedstaaten und die Organe und Einrichtungen der EU anwendbar ist. Das Stockholmer Programm ([9]) legt diesbezüglich übereinstimmend fest, dass die Union eine umfassende Strategie zum Datenschutz innerhalb der EU sowie in den Beziehungen zu anderen Ländern gewährleisten muss.

17. Der vierte Faktor sind Parallelentwicklungen im Zusammenhang mit internationalen Organisationen. Es gibt verschiedene fortlaufende Debatten über die Modernisierung der aktuellen Rechtsakte für den Datenschutz. Diesbezüglich ist es wichtig, die aktuellen Überlegungen, die im Hinblick auf die künftige Überprüfung des Übereinkommens Nr. 108 des Europarats ([10]) und der OECD-Richtlinien über Datenschutz ([11]) angestellt werden, zu erwähnen. Eine andere wichtige Entwicklung betrifft die Annahme von internationalen Standards zum Schutz personenbezogener Daten und der Privatsphäre, die möglicherweise zu der Annahme eines verbindlichen globalen Datenschutzinstruments führen wird. Alle diese Initiativen verdienen volle Unterstützung. Ihr gemeinsames Ziel sollte die Gewährleistung eines wirksamen und einheitlichen Schutzes in einem technologiegeprägten und globalisierten Umfeld sein.

3. **Grundlegende Sichtweisen**

3.1 *Datenschutz schafft Vertrauen und muss andere (öffentliche) Interessen fördern*

18. Ein starker Datenschutzrahmen ist die zwangsläufige Folge der Bedeutung, die dem Datenschutz im Vertrag von Lissabon, insbesondere in Artikel 8 der Charta der Grundrechte der Europäischen Union und in Artikel 16 AEUV beigemessen wird, und der starken Verknüpfung mit Artikel 7 der Charta ([12]).

19. Allerdings dient ein starker Datenschutzrahmen auch den breiteren öffentlichen und privaten Interessen einer Informationsgesellschaft mit einer allgegenwärtigen Datenverarbeitung. Datenschutz schafft Vertrauen, und Vertrauen ist ein wesentlicher Bestandteil des guten Funktionierens unserer Gesellschaft. Es ist essentiell, dass die Vereinbarungen zum Datenschutz in einer Weise ausgelegt werden, in der sie so weit wie möglich gesetzliche Rechte und berechtigte Interessen aktiv unterstützen, anstatt diese zu behindern.

20. Wichtige Beispiele für weitere berechtigte Interessen sind eine starke europäische Wirtschaft, die Sicherheit des Einzelnen sowie die Rechenschaftspflicht von Regierungen.

21. Die wirtschaftliche Entwicklung der EU geht mit der Einführung und der Vermarktung von neuen Technologien und Dienstleistungen einher. In der Informationsgesellschaft hängen das Entstehen und der erfolgreiche Einsatz der Informations- und Kommunikationstechnologie und der entsprechenden Dienstleistungen von Vertrauen ab. Wenn die Menschen den IKT nicht vertrauen, werden diese Technologien wahrscheinlich keinen Erfolg haben ([13]). Und die Menschen werden den IKT nur dann vertrauen, wenn ihre Daten wirksam geschützt werden. Aus diesem Grund sollte der Datenschutz integraler Bestandteil von Technologien und Dienstleistungen sein. Ein starker Datenschutzrahmen fördert die europäische Wirtschaft, vorausgesetzt, er ist nicht nur stark, sondern auch richtig zugeschnitten. Eine weitere Harmonisierung innerhalb der EU und eine Minimierung des Verwaltungsaufwands sind unter diesem Gesichtspunkt grundlegend (siehe Kapitel 5 dieser Stellungnahme).

22. In den vergangenen Jahren war viel die Rede von der Notwendigkeit, ein Gleichgewicht zwischen Privatsphäre und Sicherheit zu schaffen, insbesondere im Hinblick auf die Instrumente zur Verarbeitung und zum Austausch von Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit ([14]). Der Datenschutz wurde häufig falsch als ein Hindernis für den vollständigen Schutz der physischen Sicherheit des Einzelnen dargestellt ([15]) oder zumindest als eine unvermeidliche Bedingung, die von den Strafverfolgungsbehörden einzuhalten ist. Dies ist allerdings noch nicht alles. Eine starker Datenschutzrahmen kann die Sicherheit erhöhen und stärken. Die Datenschutzgrundsätze — wenn sie richtig angewandt werden — verpflichten die für die Verarbeitung Verantwortlichen zu gewährleisten, dass die Informationen richtig und aktuell sind und dass überflüssige personenbezogene Daten, die für die Strafverfolgung nicht erforderlich sind, aus den Systemen entfernt werden. In diesem Zusammenhang sind auch Verpflichtungen zur Umsetzung von technologischen und

([9]) Das Stockholmer Programm - Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, (ABl. C 115 vom 4.5.2010, S. 1), auf S. 10.

([10]) Übereinkommen des Europarats Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 108, 28. Januar 1981.

([11]) OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, veröffentlicht auf http://www.oecd.org

([12]) Die Bedeutung des Datenschutzes und die Verknüpfung mit der Privatsphäre in der Charta werden durch den Gerichtshof in seinem Urteil vom 9. November 2010, verbundene Rechtssachen C-92/09 und C-93/09, *Schecke*, noch nicht veröffentlicht in der Slg., betont.

([13]) Siehe Stellungnahme des EDSB vom 18. März 2010 zur Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre, (ABl. C 280 vom 16.10.2010, S. 1), Absatz 113.

([14]) Siehe z. B. die Stellungnahme des EDSB vom 10. Juli 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger", (ABl. C 276 vom 17.9.2009, S. 8).

([15]) Sicherheit ist ein weiter gefasster Begriff als die physische Sicherheit, zur Veranschaulichung der entsprechenden Argumente wird er hier jedoch in einer stärker eingeschränkten Weise verwendet.

organisatorischen Maßnahmen erwähnenswert, um die Sicherheit der Systeme, wie der Schutzsysteme gegen unbefugte Offenlegung oder unbefugten Zugang, die im Bereich des Datenschutzes entwickelt wurden, zu gewährleisten.

23. Die Einhaltung der Datenschutzgrundsätze kann des Weiteren gewährleisten, dass die Strafverfolgungsbehörden rechtsstaatliche Verfahren einhalten, was Vertrauen in ihr Verhalten erzeugt und auf diese Weise im weiteren Sinne Vertrauen in unseren Gesellschaften fördert. Die nach Artikel 8 der EU-Charta der Grundrechte entwickelte Rechtsprechung gewährleistet, dass Polizei- und Justizbehörden sämtliche für ihre Arbeit relevanten Daten verarbeiten können, allerdings nicht ohne Einschränkungen. Der Datenschutz erfordert gegenseitige Kontrollen (siehe zu Polizei und Justiz in Kapitel 9 dieser Stellungnahme).

24. In demokratischen Gesellschaften sind die Regierungen für alle Handlungen rechenschaftspflichtig, einschließlich für die Verwendung personenbezogener Daten für die verschiedenen von ihnen bedienten öffentlichen Interessen. Dies reicht von der Veröffentlichung von Daten im Internet aus Gründen der Transparenz bis zur Verwendung von Daten zur Unterstützung politischer Maßnahmen in Bereichen wie dem Gesundheitswesen, Transport- oder Steuerwesen oder zur Überwachung von Einzelpersonen zu Zwecken der Strafverfolgung. Ein starker Datenschutzrahmen ermöglicht Regierungen die Einhaltung ihrer Verantwortung und Rechenschaftspflichten als Bestandteil einer verantwortungsvollen Staatsführung.

3.2 *Konsequenzen für den Rechtsrahmen zum Datenschutz*

3.2.1 Eine weitere Harmonisierung ist erforderlich

25. In der Mitteilung wird richtig festgestellt, dass einer der wesentlichen Mängel der derzeitigen Rahmenregelung darin besteht, dass im Hinblick auf die Umsetzung der europäischen Bestimmungen in nationales Recht zuviel dem Ermessen der Mitgliedstaaten überlassen wird. Dieser Mangel an Harmonisierung hat eine Reihe negativer Folgen in einer Informationsgesellschaft, in der die physischen Grenzen zwischen den Mitgliedstaaten zunehmend an Relevanz verlieren (siehe Kapitel 5 dieser Stellungnahme).

3.2.2 Allgemeine Datenschutzgrundsätze behalten ihre Gültigkeit

26. Ein erster und eher formaler Grund, weshalb die allgemeinen Datenschutzgrundsätze nicht verändert werden sollen und können, ist rechtlicher Natur. Diese Grundsätze sind im Übereinkommen Nr. 108 des Europarats, das für alle Mitgliedstaaten bindend ist, festgelegt. Dieses Übereinkommen ist die Grundlage für den Datenschutz in der EU. Darüber hinaus werden einige der wesentlichen Grundsätze in Artikel 8 der Charta der Grundrechte der Europäischen Union ausdrücklich erwähnt. Eine Änderung dieser Grundsätze würde folglich eine Änderung der Verträge erfordern.

27. Dies ist jedoch noch nicht alles. Es gibt ebenso inhaltliche Gründe dafür, die allgemeinen Grundsätze nicht zu ändern. Der EDSB ist davon überzeugt, dass eine Informationsgesellschaft nicht ohne einen adäquaten Schutz der Privatsphäre und der personenbezogenen Daten von Einzelpersonen funktionieren kann und sollte. Wenn mehr Informationen verarbeitet werden, ist auch ein besserer Schutz erforderlich. Eine Informationsgesellschaft, in der große Mengen von Informationen über jedermann verarbeitet werden, muss auf dem Konzept der Kontrolle durch den Einzelnen aufbauen, um diesem zu ermöglichen, als Individuum zu handeln und von seinen Rechten in einer demokratischen Gesellschaft, wie dem Recht auf freie Meinungsäußerung, Gebrauch zu machen.

28. Weiterhin ist eine Kontrolle des Einzelnen kaum ohne die Verpflichtung der für die Verarbeitung Verantwortlichen vorstellbar, die Verarbeitung gemäß den Grundsätzen der Notwendigkeit, Verhältnismäßigkeit und Zweckbindung einzuschränken. Ebenso ist eine Kontrolle durch den Einzelnen ohne die anerkannten Rechte der betroffenen Personen, wie das Recht auf Auskunft, Berichtigung, Löschung oder Sperrung der Daten, kaum vorstellbar.

3.2.3 Aus der Sichtweise der Grundrechte

29. Der EDSB betont, dass der Datenschutz als Grundrecht anerkannt wird. Dies bedeutet nicht, dass der Datenschutz stets *Vorrang vor* anderen wichtigen Rechten und Interessen einer demokratischen Gesellschaft *hat*, sondern dass er sich auf die Art und den Umfang des Schutzes auswirkt, der in einem EU-Rechtsrahmen gewährleistet werden muss, damit die Anforderungen des Datenschutzes immer *auf angemessene Weise* berücksichtigt werden.

30. Die wichtigsten Auwirkungen können folgendermaßen definiert werden:

— Der Schutz muss wirksam sein. Ein Rechtsrahmen muss die Instrumente bereitstellen, mit deren Hilfe der Einzelne seine Rechte in der Praxis ausüben kann.

— Der Rahmen muss über einen langen Zeitraum hinweg stabil bleiben.

— Der Schutz muss unter allen Umständen gewährleistet sein und darf nicht von den politischen Vorlieben während eines bestimmten Zeitraums abhängen.

— Einschränkungen der Ausübung des Rechts können erforderlich sein, müssen sich jedoch auf Ausnahmen beschränken, die ordnungsgemäß gerechtfertigt sind und nie die wesentlichen Elemente des Rechts als solches betreffen ([16]).

Der EDSB empfiehlt, dass die Kommission dies berücksichtigt, wenn sie Legislativlösungen vorschlägt.

3.2.4 Neue Rechtsvorschriften sind erforderlich

31. Die Mitteilung konzentriert sich zu Recht auf die Notwendigkeit, die rechtliche Regelungen zum Datenschutz zu verstärken. In diesem Zusammenhang ist es sinnvoll, daran zu erinnern, dass im Dokument der Artikel-29-Datenschutzgruppe über die Zukunft des Datenschutzes ([17]) die Datenschutzbehörden die Notwendigkeit einer stärkeren Rolle der unterschiedlichen Akteure im Bereich des

([16]) Siehe auch die Stellungnahme des EDSB vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie", Absatz 17, die auf der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte und des Gerichtshofs aufbaut.

([17]) Vgl. Fußnote 7.

Datenschutzes, insbesondere der betroffenen Personen, der für die Verarbeitung Verantwortlichen und der Aufsichtsbehörden selbst betonen.

32. Es scheint ein breiter Konsens zwischen den Interessengruppen zu bestehen, dass stärkere rechtliche Regelungen — mit denen die technologische Entwicklung und die Globalisierung berücksichtigt werden — der Schlüssel für einen ambitionierten und wirksamen Datenschutz auch in der Zukunft sind. Wie bereits unter Absatz 7 aufgeführt, sind dies die Kriterien, anhand derer der EDSB alle vorgeschlagenen Lösungen beurteilt.

3.2.5 Möglichst weite Ausdehnung als *Conditio sine qua non*

33. In der Mitteilung wird daran erinnert, dass die Richtlinie 95/46/EG auf sämtliche Verarbeitungen personenbezogener Daten in den Mitgliedstaaten sowohl im öffentlichen als auch im privaten Sektor anwendbar ist, mit Ausnahme von Aktivitäten außerhalb des Anwendungsbereichs des ehemaligen Gemeinschaftsrechts ([18]). Während diese Ausnahme im Rahmen des damaligen Vertrags erforderlich war, ist dies nach dem Inkrafttreten des Vertrags von Lissabon nicht mehr der Fall. Darüber hinaus steht die Ausnahme in Widerspruch zu — dem Text und in jedem Fall den Geist von — Artikel 16 AEUV.

34. Nach Ansicht des EDSB gehört ein umfassender Rechtsakt für den Datenschutz unter Einschluss der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu den wesentlichen Verbesserungen, die sich aus einem neuen Rechtsrahmen ergeben können. Dies ist eine *Conditio sine qua non* für einen wirksamen Datenschutz in der Zukunft.

35. Der EDSB betont zur Unterstützung dieser Aussage die folgenden Argumente:

— Die Unterscheidung zwischen Tätigkeiten im privaten Sektor und dem Strafverfolgungssektor ist unscharf. Einrichtungen aus dem privaten Sektor dürfen Daten verarbeiten, die letztlich zu Zwecken der Strafverfolgung verwendet werden (Beispiel: Fluggastdatensätze) ([19]), während in anderen Fällen von diesen Einrichtungen verlangt wird, Daten zu Zwecken der Strafverfolgung aufzubewahren (Beispiel: Richtlinie zur Vorratsdatenspeicherung) ([20]).

— Es besteht kein wesentlicher Unterschied zwischen Polizei- und Justizbehörden und anderen Behörden, die nach Maßgabe der Richtlinie 95/46/EG an der Strafverfolgung beteiligt sind (Steuern, Zoll, Betrugsbekämpfung, Einwanderung).

— Wie in der Mitteilung richtig dargelegt wird, ist der zum aktuellen Zeitpunkt auf die Polizei- und Justizbehörden anwendbare Rechtsakt zum Datenschutz (Rahmenbeschluss 2008/977/JI) ([21]) unzureichend.

— Die meisten Mitgliedstaaten haben die Richtlinie 95/46/EG und das Übereinkommen Nr. 108 in ihrer nationalen Gesetzgebung umgesetzt und wenden diese ebenfalls auf ihre Polizei- und Justizbehörden an.

36. Die Aufnahme von Polizei und Justiz in einen allgemeinen Rechtsakt würde den Bürgern nicht nur mehr Garantien gewähren, sondern auch die Aufgabe der Polizeibehörden vereinfachen. Die Notwendigkeit, verschiedene Regelwerke anzuwenden, ist mühsam, unnötig zeitraubend und behindert die internationale Zusammenarbeit (siehe hierzu Kapitel 9 der Stellungnahme). Dies spricht gleichfalls für die Aufnahme der Verarbeitungsaktivitäten durch nationale Sicherheitsdienste, sofern dies beim gegenwärtigen Stand des EU-Rechts möglich ist.

3.2.6 Technologische Neutralität

37. Der Zeitraum seit der Annahme der Richtlinie 95/46/EG im Jahr 1995 kann in technologischer Hinsicht als turbulent bezeichnet werden. Es werden häufig neue technologische Entwicklungen und Anwendungen eingeführt. In vielen Fällen führte dies zu grundlegenden Veränderungen in der Art und Weise, wie die personenbezogenen Daten von Einzelpersonen verarbeitet werden. Die Informationsgesellschaft kann nicht länger als eine Parallelumgebung betrachtet werden, an der Einzelpersonen auf einer freiwilligen Basis teilnehmen können, sondern ist ein integraler Bestandteil unseres Alltags geworden. Beispielsweise werden im Konzept eines Internets der Dinge ([22]) Verknüpfungen zwischen physischen Gegenständen und der mit diesen in Bezug stehenden Online-Information hergestellt.

38. Die Technologie wird sich weiterentwickeln. Dies hat Folgen für den neuen Rechtsrahmen, der für lange Jahre wirksam sein muss und gleichzeitig künftige technologische Entwicklungen nicht behindern darf. Dies erfordert technologische Neutralität der rechtlichen Regelungen. Allerdings muss die Rahmenregelung auch mehr Rechtssicherheit für Unternehmen und Einzelpersonen gewährleisten. Sie müssen verstehen, was von ihnen erwartet wird, und in der Lage sein, ihre Rechte auszuüben, weshalb die rechtlichen Regelungen präzise sein müssen.

39. Nach Ansicht des EDSB muss ein allgemeiner Rechtsakt zum Datenschutz so weit wie möglich technologisch neutral formuliert werden. Dies beinhaltet, dass die Rechte und Pflichten der verschiedenen Akteure in einer allgemeinen und neutralen Weise zu formulieren sind, so dass sie grundsätzlich gültig und rechtskräftig bleiben, unabhängig von der Technologie, die für die Verarbeitung personenbezogener Daten gewählt wird. Angesichts des heutigen schnellen technologischen Fortschritts gibt es keine andere Wahl. Der EDSB schlägt vor, zu den bestehenden Grundsätzen zum Datenschutz zusätzlich neue, „technologisch neutrale“ Rechte einzuführen, denen in der sich

([18]) Die vorliegende Stellungnahme konzentriert sich hauptsächlich auf den damaligen 3. Pfeiler (polizeiliche und justizielle Zusammenarbeit in Strafsachen), da es sich bei dem 2. Pfeiler nicht nur um einen schwierigeren Bereich des EU-Rechts handelt (was auch in Artikel 16 AEUV und Artikel 39 EU anerkannt wird), sondern dieser Bereich für die Datenverarbeitung auch weniger relevant ist.

([19]) Siehe z. B. Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer, KOM (2010) 492 endgültig.

([20]) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, (ABl. L 105 vom 13.4.2006, S. 54).

([21]) Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

([22]) Gemäß der Festlegung in „Internet der Dinge — ein Aktionsplan für Europa“, KOM(2009) 278 endgültig.

schnell verändernden elektronischen Umgebung spezielle Bedeutung zukommen könnte (siehe hauptsächlich Kapitel 6 und 7).

3.2.7 Auf lange Sicht: Rechtssicherheit für einen längeren Zeitraum

40. Die Richtlinie 95/46/EG war in den letzten 15 Jahren das Kernstück des Datenschutzes in der EU. Sie wurde in das Recht der Mitgliedstaaten umgesetzt und durch die verschiedenen Akteure angewandt. Im Lauf der Jahre profitierte die Anwendung von praktischen Erfahrungen und zusätzlicher Orientierung durch die Kommission, die Datenschutzbehörden (auf nationaler Ebene und im Rahmen der Artikel-29-Datenschutzgruppe) sowie durch nationale und europäische Gerichte.

41. Es sollte betont werden, dass diese Entwicklungen Zeit benötigen und dass — besonders deshalb, weil wir es mit einer allgemeinen Rahmenregelung zur Verwirklichung eines Grundrechts zu tun haben — diese Zeit erforderlich ist, um Rechtssicherheit und Stabilität zu schaffen. Ein neuer allgemeiner Rechtsakt muss mit der Zielsetzung entworfen werden, dass auf diese Weise Rechtssicherheit und Stabilität für einen längeren Zeitraum geschaffen werden, wobei es zu berücksichtigen gilt, dass die künftige Entwicklung von Technologie und Globalisierung sehr schwer vorhersagbar ist. Auf jeden Fall unterstützt der EDSB uneingeschränkt das Ziel der Schaffung von Rechtssicherheit für einen längeren, mit der Perspektive der Richtlinie 95/46/EG vergleichbaren Zeitraum. Kurz gesagt: Während sich die Technologie rasch entwickelt, muss das Recht Beständigkeit aufweisen.

3.2.8 Auf kurze Sicht: Eine bessere Verwendung der vorhandenen Instrumente

42. Auf kurze Sicht ist es entscheidend, die Wirksamkeit der bestehenden rechtlichen Regelungen zu gewährleisten, und zwar in erster Linie durch Konzentration auf die Durchsetzung auf nationaler und EU-Ebene (siehe Kapitel 11 dieser Stellungnahme).

B. ELEMENTE EINER NEUEN RAHMENREGELUNG

4. Gesamtkonzept

43. Der EDSB unterstützt vorbehaltlos das Gesamtkonzept für den Datenschutz, das nicht nur der Titel, sondern auch der Ausgangspunkt der Mitteilung ist und notwendigerweise die Ausweitung der allgemeinen Datenschutzvorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen beinhaltet ([23]).

44. Allerdings stellt der EDSB zudem fest, dass die Kommission nicht beabsichtigt, sämtliche Aktivitäten im Rahmen der Datenverarbeitung in diesen allgemeinen Rechtsakt aufzunehmen. Insbesondere werden von Organen, Einrichtungen, Ämtern und Agenturen der EU durchgeführte Datenverarbeitungen nicht aufgenommen. Die Kommission führt lediglich aus, dass sie „prüfen (wird), ob andere Rechtsakte an die neue allgemeine Datenschutzregelung angepasst werden müssen."

45. Der EDSB gibt der Aufnahme von Verarbeitungen auf EU-Ebene in den allgemeinen Rechtsrahmen eindeutig den Vorzug. Er erinnert daran, dass dies die ursprüngliche Absicht des ehemaligen Artikels 286 EGV war, in dem der Datenschutz zum ersten Mal auf Vertragsebene erwähnt wurde. Artikel 286 EGV legte nur fest, dass alle Rechtsakte über die Verarbeitung personenbezogener Daten auch auf die Organe und Einrichtungen anzuwenden sind. Bedeutender ist jedoch, dass ein einziger Rechtstext Unstimmigkeiten zwischen Bestimmungen vermeiden würde und für den Datenaustausch zwischen der EU-Ebene und den privaten und öffentlichen Einrichtungen in den Mitgliedstaaten am besten geeignet wäre. So ließe sich auch das Risiko vermeiden, dass nach einer Änderung der Richtlinie 95/46/EG kein politisches Interesse mehr an einer Änderung der Verordnung (EG) Nr. 45/2001 besteht oder dieser Änderung keine ausreichende Priorität eingeräumt wird, um unterschiedliche Zeitpunkte des Inkrafttretens zu vermeiden.

46. Der EDSB fordert die Kommission — falls diese zum Schluss kommen sollte, dass eine Aufnahme der Verarbeitung auf EU-Ebene in einen allgemeinen Rechtsakt nicht durchführbar ist — nachdrücklich auf, sich zu einem Vorschlag für eine Anpassung der Verordnung (EG) Nr. 45/2001 zu verpflichten (nicht „prüfen, ob"), und zwar innerhalb einer möglichst kurzen Frist und vorzugsweise bis Ende 2011.

47. Gleichermaßen wichtig ist, dass die Kommission gewährleistet, dass andere Bereiche nicht zurückbleiben, insbesondere:

— Datenschutz in der Gemeinsamen Außen- und Sicherheitspolitik auf der Grundlage von Artikel 39 EUV ([24]).

— Sektorspezifische Datenschutzregelungen für EU-Einrichtungen wie Europol, Eurojust und informationstechnische Großsysteme, sofern diese an den neuen Rechtsakt angepasst werden müssen.

— Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG, sofern diese an den neuen Rechtsakt angepasst werden muss.

48. Schließlich kann — und muss wohl auch — ein allgemeiner Rechtsakt für den Datenschutz durch zusätzliche sektorbezogene und spezifische Vorschriften ergänzt werden, beispielsweise im Hinblick auf die polizeiliche und justizielle Zusammenarbeit, jedoch auch in anderen Bereichen ([25]). Sofern erforderlich und unter Einhaltung des Subsidiaritätsprinzips sollten diese zusätzlichen Vorschriften auf EU-Ebene angenommen werden. Die Mitgliedstaaten können in bestimmten Bereichen, in denen dies gerechtfertigt ist, zusätzliche Regelungen einführen (siehe 5.2).

([23]) Siehe S. 14 der Mitteilung und Abschnitt 3.2.5 dieser Stellungnahme.

([24]) Siehe ebenfalls die Stellungnahme des EDSB vom 24. November 2010 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat — „Politik der EU zur Terrorismusbekämpfung: wichtigste Errungenschaften und künftige Herausforderungen", Absatz 31.

([25]) Siehe auch das Dokument der Artikel-29-Datenschutzgruppe über die Zukunft des Datenschutzes (Fußnote 7), Absätze 18-21.

5. **Weitere Harmonisierung und Vereinfachung**

5.1 *Die Notwendigkeit einer Harmonisierung*

49. Eine Harmonisierung des EU-Datenschutzrechts ist von höchster Bedeutung. Die Mitteilung betont ganz richtig, dass der Datenschutz eine starke Binnenmarktdimension aufweist, da er den freien Fluss personenbezogener Daten zwischen den Mitgliedstaaten des Binnenmarkts gewährleisten muss. Allerdings wurde das im Rahmen der aktuellen Richtlinie erreichte Harmonisierungsniveau nicht als zufriedenstellend eingestuft. Die Mitteilung trägt dem Umstand Rechnung, dass dies zu den wesentlichen, immer wiederkehrenden Bedenken der Interessengruppen gehört. Insbesondere betonen die Interessengruppen die Notwendigkeit, die Rechtssicherheit zu stärken, den Verwaltungsaufwand zu reduzieren und gleiche Wettbewerbsbedingungen für die Wirtschaftsbeteiligten zu gewährleisten. Wie die Kommission zu Recht feststellt, gilt dies insbesondere für die in verschiedenen Mitgliedstaaten niedergelassenen, für die Verarbeitung Verantwortlichen, die (möglicherweise voneinander abweichende) Anforderungen nach nationalem Datenschutzrecht erfüllten müssen ([26]).

50. Die Harmonisierung ist nicht nur wichtig für den Binnenmarkt, sondern auch im Hinblick auf die Gewährleistung eines angemessenen Datenschutzes. Artikel 16 AEUV legt fest, dass „jede Person" das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Für eine tatsächliche Einhaltung dieses Rechts ist es erforderlich, ein gleichwertiges Schutzniveau in der gesamten EU zu gewährleisten. Im Dokument der Artikel-29-Datenschutzgruppe über die Zukunft des Datenschutzes wird betont, dass verschiedene Bestimmungen hinsichtlich der Stellung der betroffenen Personen nicht in allen Mitgliedstaaten umgesetzt bzw. einheitlich ausgelegt werden ([27]). In einer globalisierten und miteinander verschalteten Welt könnten diese Unterschiede den Schutz des Einzelnen untergraben oder einschränken.

51. Der EDSB ist der Ansicht, dass eine fortschreitende und bessere Harmonisierung zu den Hauptzielen des Überprüfungsprozesses gehört. Er begrüßt die in der Mitteilung ausgedrückte Bereitschaft der Kommission zu prüfen, wie eine weitere Harmonisierung des Datenschutzes auf EU-Ebene erreicht werden kann. Allerdings stellt er mit Erstaunen fest, dass in der Mitteilung auf dieser Stufe keine konkreten Möglichkeiten hierzu genannt werden. Aus diesem Grund verweist der EDSB hier auf bestimmte Bereiche, in denen eine höhere Konvergenz dringend geboten ist (siehe 5.3). Eine weitere Harmonisierung in diesen Bereichen sollte nicht nur dadurch erzielt werden, dass der Handlungsspielraum für nationales Recht eingeschränkt wird, sondern auch dadurch, dass einer falschen Umsetzung durch die Mitgliedstaaten vorgebeugt (siehe auch Kapitel 11) und eine in höherem Maße einheitlichere und koordiniertere Durchsetzung (siehe auch Kapitel 10) gewährleistet wird.

([26]) Mitteilung, S. 10.

([27]) Siehe Dokument der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes (Fußnote 7), Absatz 70. Das Dokument nimmt insbesondere Bezug auf die Haftungsbestimmungen und die Möglichkeit, immaterielle Schäden einzuklagen.

5.2 *Verringerung des Spielraums zur Umsetzung der Richtlinie*

52. Die Richtlinie enthält eine Reihe von Bestimmungen, die weit gefasst sind und aus diesem Grund allerhand Spielraum für eine unterschiedliche Umsetzung lassen. In Erwägungsgrund 9 der Richtlinie wird ausdrücklich bestätigt, dass die Mitgliedstaaten über einen gewissen Spielraum verfügen und dass im Zusammenhang mit diesem Spielraum Unterschiede bei der Umsetzung der Richtlinie auftreten können. Eine Reihe von Bestimmungen wurden von den Mitgliedstaaten unterschiedlich umgesetzt, darunter einige grundlegende Bestimmungen ([28]). Diese Situation ist nicht zufriedenstellend und es sollte eine höhere Konvergenz angestrebt werden.

53. Dies bedeutet nicht, dass Unterschiede völlig ausgeschlossen werden sollten. In bestimmten Bereichen ist u. U. Flexibilität erforderlich, um gerechtfertigte besondere Gegebenheiten, ein bedeutendes öffentliches Interesse oder die institutionelle Autonomie der Mitgliedstaaten zu bewahren. Nach Ansicht des EDSB sollten die Unterschiede zwischen den Mitgliedstaaten insbesondere auf die folgenden spezifischen Bereiche beschränkt werden:

— Recht auf freie Meinungsäußerung: Nach Maßgabe der aktuellen Regelung (Artikel 9) können die Mitgliedstaaten im Hinblick auf eine Datenverarbeitung, die zu journalistischen Zwecken oder zu Zwecken des künstlerischen oder literarischen Ausdrucks durchgeführt wird, Ausnahmen und Abweichungen gewähren. Diese Flexibilität scheint angesichts der unterschiedlichen Traditionen und kulturellen Unterschiede, die diesbezüglich in den Mitgliedstaaten bestehen, angebracht; allerdings unterliegt diese Flexibilität den durch die Charta und die EMRK auferlegten Einschränkungen. Dies würde jedoch einer möglichen Aktualisierung des derzeitigen Artikels 9 vor dem Hintergrund der Entwicklungen im Internet nicht entgegenstehen.

— Spezifisches öffentliches Interesse: Nach Maßgabe der aktuellen Regelung (Artikel 13) können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte beschränken, sofern eine solche Beschränkung für die Wahrung öffentlicher Interessen wie die nationale Sicherheit, die Verteidigung, die öffentliche Sicherheit usw. notwendig ist. Diese Befugnis der Mitgliedstaaten ist auch weiterhin gerechtfertigt. Allerdings sollte, wo immer möglich, die Auslegung der Ausnahmen weiter harmonisiert werden (siehe Abschnitt 9.1). Zudem scheint der aktuelle Umfang für Ausnahmen von Artikel 6 Absatz 1 übermäßig weit gefasst.

— Rechtsmittel, Sanktionen und Verwaltungsverfahren: Eine europäische Rahmenregelung sollte die Grundvoraussetzungen festlegen, allerdings muss nach dem aktuellen Stand des EU-Rechts die Festlegung von Sanktionen, Rechtsmitteln, Verfahrensvorschriften und Modalitäten für auf nationaler Ebene durchzuführende Inspektionen den Mitgliedstaaten überlassen bleiben.

([28]) Unterschiedliche Ansätze bestehen ebenfalls im Hinblick auf manuelle Daten.

5.3 *Bereiche für eine weitere Harmonisierung*

54. *Begriffsbestimmungen* (Artikel 2 der Richtlinie 95/46/EG). Begriffsbestimmungen sind die Grundpfeiler des Rechtssystems und sollten in allen Mitgliedstaaten ohne Spielraum für die Durchführung einheitlich ausgelegt werden. Bei der aktuellen Rahmenregelung sind Unterschiede beispielsweise hinsichtlich des Begriffs des für die Verarbeitung Verantwortlichen aufgetreten ([29]). Der EDSB empfiehlt, dass in die aktuelle Liste in Artikel 2 weitere Begriffe wie anonyme Daten, pseudonyme Daten, Justizdaten, Datenübermittlung und Datenschutzbeauftragter aufgenommen werden, um mehr Rechtssicherheit zu gewährleisten.

55. *Rechtmäßigkeit der Verarbeitung* (Artikel 5). Der neue Rechtsakt sollte im Hinblick auf die Kernelemente zur Definition der Rechtmäßigkeit der Datenverarbeitung möglichst präzise sein. Artikel 5 der Richtlinie (ebenso wie Erwägungsgrund 9), in dem die Mitgliedstaaten beauftragt werden, die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, wird daher in einer künftigen Regelung gegebenenfalls nicht mehr benötigt.

56. *Gründe für die Datenverarbeitung* (Artikel 7 und 8). Die Definition der Voraussetzungen für die Datenverarbeitung ist ein grundlegender Bestandteil einer jeden Gesetzgebung zum Datenschutz. Den Mitgliedstaaten sollte nicht gestattet werden, zusätzliche oder abgewandelte Gründe für die Verarbeitung einzuführen oder irgendwelche Gründe auszuschließen. Die Möglichkeit von Abweichungen sollte ausgeschlossen oder eingeschränkt werden (insbesondere im Hinblick auf sensible Daten) ([30]). In einem neuen Rechtsakt sollten die Gründe für die Datenverarbeitung klar formuliert und auf diese Weise der Ermessensspielraum für die Um- bzw. Durchsetzung verringert werden. Insbesondere der Begriff der Einwilligung sollte konkretisiert werden (siehe Abschnitt 6.5). Darüber hinaus lässt der Grund, der sich auf das berechtigte Interesse des für die Verarbeitung Verantwortlichen stützt (Artikel 7 Buchstabe f), wegen seines flexiblen Charakters weit voneinander abweichende Auslegungen zu. Eine Konkretisierung ist erforderlich. Eine weitere Bestimmung, die wohl geändert werden muss, ist in Artikel 8 Absatz 2 Buchstabe b ausgeführt. Hier wird eine Verarbeitung sensibler Daten gestattet, wenn diese erforderlich ist, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen ([31]).

57. *Rechte der betroffenen Person* (Artikel 10-15). Dies ist einer der Bereiche, in denen von den Mitgliedstaaten noch nicht alle Elemente der Richtlinie auf einheitliche Weise umgesetzt und ausgelegt wurden. Die Rechte der betroffenen Personen sind ein zentrales Element eines wirksamen Datenschutzes. Aus diesem Grund sollte der Spielraum deutlich verringert werden. Der EDSB empfiehlt, dass die Informationen, die von dem für die Verarbeitung Verantwortlichen für die betroffenen Personen bereitgestellt werden, innerhalb der EU einheitlich sein sollten.

58. *Internationale Übermittlungen* (Artikel 25-26). Dies ist ein Bereich, an dem sich auf Grund einer fehlenden einheitlichen Handhabung innerhalb der EU breite Kritik entzündet hat. Die Interessengruppen kritisierten, dass die Beschlüsse der Kommission zur Angemessenheit von den Mitgliedstaaten sehr unterschiedlich ausgelegt und umgesetzt werden. Verbindliche unternehmensinterne Vorschriften sind ein weiteres Element, für das der EDSB eine weitere Harmonisierung empfiehlt (siehe Kapitel 9).

59. *Nationale Datenschutzbehörden* (Artikel 28). Die nationalen Datenschutzbehörden unterstehen in den 27 Mitgliedstaaten weit voneinander abweichenden Vorschriften, insbesondere im Hinblick auf ihre Rechtsstellung, ihre Ressourcen und ihre Befugnisse. Artikel 28 hat auf Grund seiner mangelhaften Klarheit ([32]) teilweise zu diesen Abweichungen beigetragen und sollte daher in Übereinstimmung mit dem Urteil des Europäischen Gerichtshofs im Fall C-518/07 ([33]) (siehe auch Kapitel 10) klarer formuliert werden.

5.4 *Vereinfachung des Meldesystems*

60. Die Meldeanforderungen (Artikel 18-21 der Richtlinie 95/46/EG) sind ein weiterer Bereich, in dem den Mitgliedstaaten bisher bedeutende Freiheiten gewährt wurden. In der Mitteilung wird zu Recht festgestellt, dass ein harmonisiertes System sowohl die Kosten als auch den Verwaltungsaufwand, der den für die Verarbeitung Verantwortlichen entsteht, senken würde ([34]).

61. Dies ist ein Bereich, in dem eine Vereinfachung das Hauptziel sein sollte. Die Überprüfung des Datenschutzrahmens bietet eine einmalige Gelegenheit für eine weitere Vereinfachung bzw. Verringerung des Umfangs der aktuellen Meldeanforderungen. In der Mitteilung wird anerkannt, dass zwischen den Interessengruppen ein allgemeiner Konsens darüber besteht, dass das aktuelle Meldesystem eher kompliziert ist und als solches keinen zusätzlichen Nutzen für den Schutz personenbezogener Daten bietet ([35]). Der EDSB begrüßt daher die Bereitschaft der Kommission, verschiedene Möglichkeiten zur Vereinfachung des derzeitigen Meldesystems zu prüfen.

62. Nach Ansicht des EDSB besteht der Ausgangspunkt für diese Vereinfachung in einer Verlagerung von einem System, in dem Meldungen, falls dies nicht anderweitig geregelt ist (z. B. „Freistellungssystem"), die Regel sind, zu einem zielgerichteteren System. Das Freistellungssystem hat sich als ineffizient erwiesen, weil es in den Mitgliedstaaten nicht einheitlich umgesetzt wurde ([36]). Der EDSB empfiehlt die Erwägung der folgenden Alternativen:

([29]) Siehe die Stellungnahme 1/2010 zu den Konzepten der Artikel-29-Datenschutzgruppe im Hinblick auf den „für die Verarbeitung Verantwortlichen" und den „Verarbeiter" (WP 169).

([30]) Artikel 8 Absatz 4 und Absatz 5 gestatten den Mitgliedstaaten unter bestimmten Voraussetzungen weitere Abweichungen im Hinblick auf sensible Daten.

([31]) Siehe den weiter oben zitierten ersten Bericht der Kommission zur Durchführung der Datenschutzrichtlinie, S. 14.

([32]) Dokument der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes, Absatz 87.

([33]) Fall C-518/07, *Kommission/Deutschland,* noch nicht in der Slg. veröffentlicht.

([34]) Vgl. Fußnote 26.

([35]) Vgl. Fußnote 26.

([36]) Bericht der Artikel-29-Datenschutzgruppe über die Pflicht zur Meldung bei den nationalen Kontrollstellen, die bestmögliche Nutzung der Ausnahmen und der Vereinfachung und die Rolle der Datenschutzbeauftragten in der Europäischen Union, WP 106, 2005, S. 7.

— Beschränkung der Meldepflicht auf bestimmte, mit spezifischen Risiken verbundene Verarbeitungen (diese Meldungen könnten weitere Schritte, beispielsweise eine Vorabkontrolle der Verarbeitung, zur Folge haben).

— Eine einfache Pflicht zur Registrierung für die für die Verarbeitung Verantwortlichen (im Gegensatz zu einer umfassenden Registrierung sämtlicher Datenverarbeitungen).

Zusätzlich könnte ein paneuropäisches Standard-Meldeformular eingeführt werden, um harmonisierte Vorgehensweisen im Hinblick auf die erforderlichen Informationen zu gewährleisten.

63. Die Überprüfung des derzeitigen Meldesystems sollte einer Verbesserung der Verpflichtung zur Vorabkontrolle für bestimmte Verarbeitungen, die eventuell bestimmte Risiken aufweisen (etwa informationstechnische Großsysteme), nicht entgegenstehen. Der EDSB befürwortet die Aufnahme einer nicht erschöpfenden Liste von Fällen, für die eine solche Vorabkontrolle erforderlich ist, in den neuen Rechtsakt. Die Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr stellt ein nützliches Modell für diesen Zweck dar ([37]).

5.5 *Eine Verordnung anstelle einer Richtlinie*

64. Schließlich ist der EDSB der Ansicht, dass der Überprüfungsprozess eine Gelegenheit bietet, die Art des Rechtsakts zum Datenschutz zu überprüfen. Eine Verordnung, ein einziges Instrument, das direkt in den Mitgliedstaaten anwendbar ist, stellt das wirksamste Mittel zum Schutz des grundlegenden Rechts auf Datenschutz und zur Schaffung eines realen Binnenmarkts dar, in dem der freie Verkehr personenbezogener Daten gewährleistet ist und das Schutzniveau unabhängig vom Land oder dem Sektor, in dem die Daten verarbeitet werden, gleich ist.

65. Eine Verordnung würde den Raum für widersprüchliche Auslegungen und ungerechtfertigte Unterschiede bei der Umsetzung und Anwendung des Rechts einschränken. Auf diese Weise wäre auch die Festlegung des auf die Verarbeitung innerhalb der EU anwendbaren Rechts weniger bedeutsam - einer der besonders kontroversen Aspekte des aktuellen Systems (siehe Kapitel 9).

66. Im Bereich des Datenschutzes ist eine Verordnung umso gerechtfertigter, da

— Artikel 16 AEUV das Recht auf den Schutz personenbezogener Daten auf die Ebene des Vertrags aufgewertet hat und ein einheitliches Schutzniveau für den Einzelnen innerhalb der EU vorsieht — bzw. sogar vorschreibt;

— die Datenverarbeitung in einem elektronischen Umfeld stattfindet, in dem die Binnengrenzen zwischen den Mitgliedstaaten an Bedeutung verloren haben.

67. Die Wahl einer Verordnung als allgemeinem Rechtsakt gestattet ferner, dass Bestimmungen, bei denen Flexibilität erforderlich ist, direkt an Mitgliedstaaten gerichtet werden. Eine Verordnung wirkt sich zudem nicht auf die Befugnis der Mitgliedstaaten aus, gegebenenfalls in Übereinstimmung mit dem EU-Recht zusätzliche Vorschriften für den Datenschutz anzunehmen.

6. **Stärkung der Rechte des Einzelnen**

6.1 *Die Notwendigkeit einer Stärkung der Rechte*

68. Der EDSB unterstützt uneingeschränkt den in der Mitteilung unterbreiteten Vorschlag, die Rechte des Einzelnen zu stärken, da die bestehenden Rechtsakte nicht in vollem Umfang den wirksamen Schutz gewährleisten, der in einer zunehmend komplexen, digitalisierten Welt erforderlich ist.

69. Einerseits beinhaltet die Entwicklung einer digitalen Welt eine rapide Zunahme der Erhebung, Verwendung und Weiterübermittlung personenbezogener Daten auf eine extrem komplexe und nicht transparente Weise. Einzelpersonen sind sich dessen oft nicht bewusst oder verstehen nicht, auf welche Weise dies erfolgt, wer ihre Daten erhebt oder wie sie Kontrolle ausüben können. Veranschaulichen lässt sich dieses Phänomen durch die Überwachung der Webbrowsing-Aktivitäten von Einzelpersonen durch Anzeigenservice-Netzwerkbetreiber, die Cookies und Ähnliches für eine gezielte Werbung verwenden. Wenn Benutzer auf Websites zugreifen, erwarten sie nicht, dass ein unsichtbarer Dritter diese Besuche protokolliert und anhand von Informationen zu ihrem Lebensstil oder ihren Vorlieben und Abneigungen Datensätze zu Benutzern erstellt.

70. Andererseits animiert diese Entwicklung Einzelpersonen dazu, persönliche Informationen anderen von sich aus mitzuteilen, beispielsweise innerhalb sozialer Netzwerke. Junge Menschen sind zunehmend Mitglieder in sozialen Netzwerken und wirken auf Gleichaltrige ein. Es ist fraglich, ob (junge) Menschen sich der Breite dieser Offenlegung und der langfristigen Auswirkungen ihrer Handlungen bewusst sind.

6.2 *Mehr Transparenz*

71. Der Transparenz kommt in allen Datenschutzvorschriften eine überragende Bedeutung zu, und zwar nicht nur aufgrund ihres Wertes an sich, sondern auch, weil andere Datenschutzgrundsätze gestützt auf die Transparenz angewandt werden können. Nur dann, wenn Einzelpersonen von der Datenverarbeitung Kenntnis haben, sind sie in der Lage, ihre Rechte auszuüben.

72. Mehrere Bestimmungen der Richtlinie 95/46/EG beschäftigen sich mit der Transparenz. Artikel 10 und 11 enthalten eine Verpflichtung, Einzelpersonen über die Erhebung ihrer personenbezogenen Daten zu informieren. Darüber hinaus wird in Artikel 12 das Recht festgeschrieben, eine Kopie der eigenen personenbezogenen Daten in verständlicher Form (Recht auf Auskunft) zu erhalten. In Artikel 15 wird das Recht auf Auskunft über die Logik anerkannt, auf deren Grundlage automatisierte Entscheidungen, die rechtliche Folgen nach sich ziehen, getroffen werden. Schließlich beinhaltet Artikel 6 Absatz 1 Buchstabe a, in dem eine Verarbeitung nach Treu und Glauben verlangt wird, ebenfalls die Forderung nach Transparenz. Personenbezogene Daten dürfen nicht für versteckte oder geheime Zwecke verarbeitet werden.

([37]) Siehe Artikel 27 der Verordnung, (ABl. L 8 vom 12.1.2001, S. 1).

73. In der Mitteilung wird vorgeschlagen, einen allgemeinen Grundsatz der Transparenz hinzuzufügen. Als Reaktion auf diesen Vorschlag betont der EDSB, dass der Begriff der Transparenz bereits integraler Bestandteil des aktuellen Rechtsrahmens für den Datenschutz darstellt, wenn auch auf implizite Weise. Dies kann aus den unterschiedlichen Bestimmungen, die sich mit der Transparenz beschäftigen und die im vorhergehenden Absatz erwähnt wurden, abgeleitet werden. Der EDSB ist der Ansicht, dass ein zusätzlicher Nutzen durch die Aufnahme eines *ausdrücklichen* Grundsatzes der Transparenz erzielt werden könnte, unabhängig davon, ob dieser mit der bestehenden Bestimmung einer Verarbeitung nach Treu und Glauben verknüpft ist oder nicht. Dies würde die Rechtssicherheit erhöhen und auch bekräftigen, dass der für die Verarbeitung Verantwortliche personenbezogene Daten unter allen Umständen auf transparente Weise zu verarbeiten hat, nicht nur auf Anfrage oder wenn er aufgrund einer konkreten rechtlichen Bestimmungen hierzu verpflichtet ist.

74. Allerdings ist es möglicherweise wichtiger, die bestehenden Bestimmungen zur Transparenz, wie die bestehenden Artikel 10 und 11 der Richtlinie 95/46/EG, zu stärken. Diese Bestimmungen nennen die bereitzustellenden Informationselemente, präzisieren jedoch nicht die Modalitäten hierfür. Der EDSB schlägt konkret vor, die bestehenden Bestimmung folgendermaßen zu stärken:

— Eine Verpflichtung des für die Verarbeitung Verantwortlichen, Informationen über die Datenverarbeitung auf leicht zugängliche und verständliche Weise sowie in klarer und einfacher Sprache bereitzustellen ([38]). Die Informationen sollten klar, deutlich und leicht auffindbar sein. Die Bestimmung sollte überdies die Verpflichtung beinhalten, ein leichtes Verständnis der Information zu gewährleisten. Aufgrund dieser Verpflichtung würden undurchsichtige oder schwer verständliche Datenschutzbestimmungen rechtswidrig.

— Eine Verpflichtung zur einfachen und direkten Bereitstellung der Informationen an die betroffenen Personen. Die Informationen sollten zudem dauerhaft zugänglich sein und nicht nach einer sehr kurzen Zeit von einem elektronischen Medium verschwinden. Dies würde es den Nutzern erleichtern, unter der Gewährleistung einer dauerhaften Auskunft Informationen in der Zukunft zu speichern und zu reproduzieren.

6.3 *Unterstützung einer Verpflichtung zur Meldung von Sicherheitsverletzungen*

75. Der EDSB unterstützt die Einführung einer Bestimmung zur Meldung von Sicherheitsverletzungen im Hinblick auf personenbezogene Daten im allgemeinen Rechtsakt, durch die die Verpflichtung, die in die überarbeitete Datenschutzrichtlinie für elektronische Kommunikation für bestimmte Diensteanbieter aufgenommen wurde, auf alle für die Datenverarbeitung Verantwortlichen ausgeweitet wird, wie in der Mitteilung vorgeschlagen. Im Rahmen der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikation ist die Verpflichtung ausschließlich auf Anbieter von elektronischen Kommunikationsdiensten (Anbieter von Telefondiensten (einschließlich VoIP) und Internetzugang) anwendbar. Andere für die Datenverarbeitung Verantwortliche unterliegen nicht dieser Verpflichtung. Eine solche Verpflichtung ist auch bei den für die Datenverarbeitung Verantwortlichen außerhalb von elektronischen Kommunikationsdiensten voll und ganz gerechtfertigt.

76. Die Meldung von Sicherheitsverletzungen dient verschiedenen Zwecken und Zielen. Der offenkundigste, in der Mitteilung betonte, Zweck besteht darin, in der Funktion als Informationsinstrument Einzelpersonen dafür zu sensibilisieren, welche Risiken sie gewärtigen müssen, wenn ihre personenbezogenen Daten gefährdet sind. Dies kann sie dabei unterstützen, die erforderlichen Maßnahmen zur Abschwächung solcher Risiken zu ergreifen. Wenn Einzelpersonen beispielsweise über Verletzungen im Hinblick auf ihre Finanzinformationen informiert werden, können sie unter anderem Passwörter austauschen oder ihre Konten auflösen. Zusätzlich tragen Meldungen über Sicherheitsverletzungen zur wirksamen Anwendung anderer Grundsätze und Verpflichtungen der Richtlinie bei. Beispielsweise werden durch die Anforderung, Sicherheitsverletzungen zu melden, Anreize für die für die Datenverarbeitung Verantwortlichen geschaffen, zur Vorbeugung derartiger Verletzungen stärkere Sicherheitsmaßnahmen einzuführen. Meldungen über Sicherheitsverletzungen sind auch ein Instrument zur Stärkung der Verantwortung der für die Verarbeitung Verantwortlichen und insbesondere zur Verbesserung der Rechenschaftspflicht (siehe Kapitel 7). Schließlich dienen sie als Instrument zur Durchsetzung für die Datenschutzbehörden. Die Meldung einer Verletzung an eine Datenschutzbehörde kann zur Untersuchung der allgemeinen Praktiken eines für die Verarbeitung Verantwortlichen führen.

77. Die spezifischen Vorschriften zu Sicherheitsverletzungen in der geänderten Datenschutzrichtlinie für elektronische Kommunikation wurden im Vorfeld der Annahme dieser Richtlinie in der parlamentarischen Phase der Regelung auf breiter Ebene diskutiert. Bei dieser Diskussion wurden die Ansichten der Artikel-29-Datenschutzgruppe und des EDSB zusammen mit den Standpunkten anderer Interessengruppen berücksichtigt. Die Vorschriften spiegeln die Ansichten verschiedener Interessengruppen wider. Sie stellen ein Interessengleichgewicht dar: während die Kriterien zur Auslösung der Meldepflicht in der Regel für den Schutz des Einzelnen angemessen sind, erfüllen sie diesen Zweck, ohne übermäßig komplizierte, wenig nützliche Anforderungen aufzuerlegen.

6.4 *Bessere Regelung der Einwilligung*

78. Artikel 7 der Datenschutzrichtlinie listet sechs Rechtsgrundlagen für die Verarbeitung personenbezogener Daten auf. Die Einwilligung der betroffenen Person ist eine davon. Für die Verarbeitung Verantwortliche sind berechtigt, personenbezogene Daten in dem Maß zu verarbeiten, wie die betroffenen Personen ihre in Kenntnis der Sachlage erfolgte Einwilligung zur Erhebung und Weiterverarbeitung ihrer Daten erteilt haben.

79. In der Praxis verfügen Benutzer oft über eine begrenzte Kontrolle über ihre Daten, insbesondere in technologischen Umgebungen. Eine der Methoden, die zuweilen verwendet wird, besteht in der impliziten Einwilligung, das heißt eine Einwilligung, auf die geschlossen wurde. Auf die Einwilligung kann aufgrund einer Handlung des Einzelnen geschlossen werden (z. B. wenn die Handlung in der Verwendung einer Website besteht und dies als Einwilligung betrachtet wird, die Daten des Benutzers zu Marketingzwecken zu protokollieren). Auf eine Einwilligung kann

([38]) Siehe Mitteilung, S. 6.

auch aufgrund von Stillschweigen oder Untätigkeit geschlossen werden (wird das Häkchen in einem entsprechenden Feld nicht entfernt, wird dies als Einwilligung betrachtet).

80. Gemäß der Richtlinie muss die Einwilligung, um gültig zu sein, in Kenntnis der Sachlage, ohne Zwang und für den konkreten Fall erteilt werden. Es muss sich um eine in Kenntnis der Sachlage erfolgte Angabe der Absicht einer Person handeln, mit der diese ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten erteilt. Die Einwilligung muss auf eindeutige Weise erteilt werden.

81. Eine Einwilligung, auf die durch eine Handlung oder insbesondere durch Stillschweigen oder Untätigkeit geschlossen wird, ist oft keine eindeutige Einwilligung. Allerdings ist nicht immer klar, wodurch sich eine echte, eindeutige Einwilligung auszeichnet. Bestimmte für die Verarbeitung Verantwortliche nutzen diese Ungewissheit aus und stützen sich auf Methoden, die für die Erteilung einer echten, eindeutigen Einwilligung nicht geeignet sind.

82. Vor dem Hintergrund des weiter oben Gesagten unterstützt der EDSB die Kommission im Hinblick auf die Notwendigkeit, die Grenzen der Einwilligung zu klären und sicherzustellen, dass nur eine Einwilligung, die auf haltbare Weise ausgelegt wird, auch als solche behandelt wird. In diesem Zusammenhang unterbreitet der EDSB die folgenden Empfehlungen ([39]):

— Es könnte erwogen werden, die Situationen, in denen eine ausdrückliche Einwilligung erforderlich ist und die aktuell auf sensible Daten beschränkt sind, auszuweiten.

— Annahme zusätzlicher Vorschriften zur Einwilligung in der Online-Umgebung.

— Annahme zusätzlicher Vorschriften zur Einwilligung für die Datenverarbeitung zu sekundären Zwecken (d. h., die Verarbeitung ist gegenüber der Hauptverarbeitung sekundär oder nicht offenkundig).

— In einem zusätzlichen Rechtsinstrument, das von der Kommission nach Maßgabe von Artikel 290 AEUV oder anderweitig angenommen werden kann, Festlegung der Art der erforderlichen Einwilligung, z. B. die Ebene der Einwilligung für die Verarbeitung von Daten aus RFID-Etiketten auf Konsumgütern oder für andere spezifische Techniken.

6.5 *Datenübertragbarkeit und das Recht auf Vergessen*

83. Die Datenübertragbarkeit und das Recht auf Vergessen sind zwei miteinander verknüpfte Konzepte, die in der Mitteilung zur Stärkung der Rechte der betroffenen Personen dargelegt werden. Sie sind eine Ergänzung zu den bereits in der Richtlinie erwähnten Grundsätzen, die die betroffenen Personen mit dem Recht zur Verweigerung einer Weiterverarbeitung ihrer personenbezogenen Daten ausstatten und dem für die Verarbeitung Verantwortlichen die Verpflichtung auferlegen, Informationen zu löschen, sobald diese für den Zweck der Verarbeitung nicht weiter erforderlich sind.

([39]) Die Artikel-29-Datenschutzgruppe arbeitet aktuell an einer Stellungnahme zur „Einwilligung". Aus dieser Stellungnahme könnten sich weitere Empfehlungen ergeben.

84. Diese beiden neuen Begriffe haben den größten zusätzlichen Nutzen im Zusammenhang mit einer Informationsgesellschaft, in der zunehmend Daten automatisch gespeichert und für unbegrenzte Zeiträume aufbewahrt werden. Die Praxis zeigt, dass sogar dann, wenn Daten von der betroffenen Person selbst hochgeladen werden, die Kontrolle, die diese Person über ihre personenbezogenen Daten hat, in der Praxis sehr beschränkt ist. Dies gilt umso mehr angesichts des gigantischen Speichers, den das Internet heute darstellt. Abgesehen davon ist es unter wirtschaftlichen Gesichtspunkten für einen für die Datenverarbeitung Verantwortlichen kostspieliger, Daten zu löschen, anstatt sie im Speicher zu belassen. Die Ausübung der Rechte des Einzelnen ist deshalb dem natürlichen wirtschaftlichen Trend entgegengerichtet.

85. Sowohl die Datenübertragbarkeit als auch das Recht auf Vergessen könnten dazu beitragen, das Gleichgewicht zugunsten der betroffenen Person zu verschieben. Das Ziel der Datenübertragbarkeit besteht darin, dem Einzelnen eine stärkere Kontrolle über seine Daten zu geben, während das Recht auf Vergessen gewährleisten würde, dass die Informationen automatisch nach einem bestimmten Zeitraum verschwinden, sogar dann, wenn die betroffene Person keine Handlung vornimmt oder sich nicht einmal bewusst ist, dass ihre Daten gespeichert wurden.

86. Insbesondere wird die Datenübertragbarkeit als Möglichkeit des Benutzers betrachtet, die Präferenzen im Hinblick auf die Verarbeitung ihrer Daten zu ändern, insbesondere im Zusammenhang mit den Dienstleistungen im Bereich der neuen Technologien. Dies gilt zunehmend für Dienste, in deren Rahmen Informationen, einschließlich personenbezogener Daten, gespeichert werden, wie z. B. Mobilfunk und Dienste, die Bilder, E-Mails und andere Informationen, teilweise unter Verwendung von Cloud-Computing, speichern.

87. Einzelpersonen müssen in der Lage sein, einfach und frei den Diensteanbieter zu wechseln und ihre personenbezogenen Daten an einen anderen Diensteanbieter zu übermitteln. Der EDSB ist der Ansicht, dass die bestehenden, in der Richtlinie 95/46/EG ausgeführten Rechte gestärkt werden könnten, indem ein Recht auf Übertragbarkeit insbesondere im Kontext von Dienstleistungen für die Informationsgesellschaft eingeführt wird. Auf diese Weise werden Einzelpersonen darin unterstützt, sicherzustellen, dass Anbieter und andere relevante, für die Verarbeitung Verantwortliche ihnen Auskunft über ihre personenbezogenen Informationen erteilen, während gleichzeitig gewährleistet wird, dass die ehemaligen Anbieter oder für die Verarbeitung Verantwortlichen diese Informationen löschen, und zwar auch dann, wenn sie diese lieber für ihre eigenen rechtmäßigen Zwecke aufbewahren würden.

88. Ein neu festgeschriebenes „Recht auf Vergessen" würde die Löschung personenbezogener Daten oder das Verbot gewährleisten, diese weiter zu verwenden, ohne dass die betroffene Person tätig werden muss, jedoch unter der Bedingung, dass diese Daten bereits während eines bestimmten Zeitraums gespeichert waren. Den Daten würde mit anderen Worten eine Art Verfallsdatum zugeordnet. Dieses Prinzip wurde bereits in nationalen Gerichtsfällen

bestätigt oder in spezifischen Bereichen, beispielsweise Polizeiakten, Strafregisterauszügen oder Disziplinarakten, angewandt: Im Rahmen einiger nationaler Gesetzgebungen werden Informationen zu Einzelpersonen automatisch gelöscht oder nicht weiterverwendet oder weiterverbreitet, insbesondere nach Ablauf einer bestimmten festgelegten Frist, ohne dass vorab eine Analyse von Fall zu Fall erforderlich ist.

89. In diesem Sinne sollte ein neues „Recht auf Vergessen" mit der Datenübertragbarkeit verknüpft werden. Der auf diese Weise entstehende zusätzliche Nutzen besteht darin, dass von Seiten der betroffenen Person keine Anstrengungen oder Forderungen zur Löschung der Daten erforderlich sind, da dies auf objektive und automatische Weise erfolgen sollte. Nur unter sehr spezifischen Umständen, wenn eine konkrete Notwendigkeit zur Aufbewahrung der Daten für einen längeren Zeitraum geltend gemacht werden kann, sollte ein für die Datenverarbeitung Verantwortlicher berechtigt sein, die Daten weiterhin aufzubewahren. Dieses „Recht auf Vergessen" würde folglich die Beweislast vom Einzelnen auf den für die Datenverarbeitung Verantwortlichen verlagern und einen „eingebauten Datenschutz" für die Verarbeitung personenbezogener Daten darstellen.

90. Der EDSB ist der Ansicht, dass das Recht auf Vergessen sich insbesondere im Kontext der Dienstleistungen für die Informationsgesellschaft als nützlich erweisen könnte. Eine Verpflichtung zur Löschung oder Nichtweiterverbreitung von Informationen nach Ablauf einer festgelegten Frist ist insbesondere im Hinblick auf die Medien oder das Internet und ganz besonders bei sozialen Netzwerken sinnvoll. Es wäre ebenfalls sinnvoll, wo Endgeräte betroffen sind: Auf mobilen Geräten oder Computern gespeicherte Daten würden nach Ablauf einer festgelegten Frist automatisch gelöscht oder gesperrt, wenn sie nicht mehr im Besitz des Einzelnen sind. In diesem Sinne kann das Recht auf Vergessen in eine Verpflichtung zum „eingebauten Datenschutz" übersetzt werden.

91. Insgesamt ist der EDSB der Ansicht, dass die Datenübertragbarkeit und das Recht auf Vergessen nützliche Konzepte sind. Es wäre sinnvoll, sie in den Rechtsakt aufzunehmen, allerdings wohl mit einer Beschränkung auf das elektronische Umfeld.

6.6 *Verarbeitung personenbezogener Daten in Bezug auf Kinder*

92. Die Richtlinie 95/46/EG enthält keine spezifischen Vorschriften zur Verarbeitung personenbezogener Daten von Kindern. Hiermit wird der Notwendigkeit eines gezielten Schutzes von Kindern unter spezifischen Umständen aufgrund ihrer Verletzlichkeit nicht Rechnung getragen; dies zieht rechtliche Unsicherheiten insbesondere in den folgenden Bereichen nach sich:

— Die Erhebung der Daten von Kindern und die Art und Weise, in der diese über die Erhebung zu informieren sind;

— die Art und Weise, wie die Einwilligung von Kindern eingeholt wird. Da keine klaren Vorschriften bestehen, auf welche Weise die Einwilligung von Kindern einzuholen ist und bis zu welchem Alter Kinder als solche zu betrachten sind, wird dieser Sachverhalt nach Maßgabe der nationalen Gesetzgebung, die von Mitgliedstaat zu Mitgliedstaat unterschiedlich ist, gehandhabt ([40]);

— die Art und Weise und die Voraussetzungen, unter denen Kinder oder ihre gesetzlichen Vertreter ihre Rechte im Rahmen der Richtlinie wahrnehmen können.

93. Der EDSB ist der Ansicht, dass die spezifischen Interessen von Kindern besser geschützt wären, wenn der neue Rechtsakt zusätzliche Bestimmungen enthielte, die sich speziell auf die Erhebung und Weiterverarbeitung der Daten von Kindern beziehen. Solche spezifischen Bestimmungen würden auch Rechtssicherheit in diesem Bereich herstellen und könnten den für die Datenverarbeitung Verantwortlichen von Nutzen sein, da diese gegenwärtig unterschiedliche gesetzliche Anforderungen erfüllen müssen.

94. Der EDSB schlägt vor, die folgenden Bestimmungen in den Rechtsakt aufzunehmen:

— Eine Anforderung, die Informationen an Kinder insoweit anzupassen, wie dies das Verständnis der Kinder dafür erleichtern würde, was es bedeutet, wenn ihre Daten erhoben werden.

— Weitere, kindgerechte Informationsanforderungen, Anforderungen hinsichtlich der Art und Weise, wie die Informationen bereitzustellen sind und ggf. auch im Hinblick auf den Inhalt.

— Eine gezielte Bestimmung zum Schutz von Kindern vor verhaltensorientierter Werbung.

— Der Grundsatz der Zweckbindung sollte gestärkt werden, wenn Daten von Kindern betroffen sind.

— Bestimmte Datenkategorien sollten von Kindern nie erhoben werden.

— Eine Altersgrenze. Unter dieser Altersgrenze sollten Informationen von Kindern ausschließlich mit der ausdrücklichen und überprüfbaren Einwilligung der Eltern erhoben werden.

— Falls die Einwilligung der Eltern erforderlich ist, wäre es notwendig, Vorschriften aufzustellen, auf welche Weise das Alter des Kindes ermittelt werden kann - mit anderen Worten, wie ermittelt wird, dass es sich bei dem Kind um einen Minderjährigen handelt und wie die Einwilligung der Eltern überprüft wird. Dies

([40]) Die Einwilligung ist in der Regel an das Alter geknüpft, ab dem Kinder Vertragsverpflichtungen eingehen können. Dies ist das Alter, in dem Kinder mutmaßlich einen bestimmten Reifegrad erreicht haben. Beispielsweise fordert die spanische Gesetzgebung die Einwilligung der Eltern zur Erhebung der Daten von Kindern, die noch nicht 14 Jahre alt sind. Ab diesem Alter werden die Kinder als in der Lage gesehen, ihre Einwilligung zu erteilen. Im Vereinigten Königreich wird im Datenschutzgesetz kein bestimmtes Alter bzw. keine bestimmte Grenze vorgesehen. Allerdings ist die Datenschutzbehörde im Vereinigten Königreich zu der Auslegung gekommen, dass Kinder über 12 Jahren ihre Einwilligung erteilen können. Umgekehrt können Kinder unter 12 ihre Einwilligung nicht erteilen, und um ihre personenbezogenen Daten zu erhalten, ist es zunächst erforderlich, die Einwilligung eines Elternteils oder Vormunds einzuholen.

ist ein Bereich, in dem die EU Anregungen aus anderen Ländern, wie etwa den Vereinigten Staaten, aufgreifen kann. ([41])

6.7 *Kollektive Rechtsbehelfsverfahren*

95. Eine substanzielle Stärkung der Rechte des Einzelnen wäre bei gleichzeitigem Fehlen wirksamer Verfahrensmechanismen zur Durchsetzung dieser Rechte zwecklos. In diesem Zusammenhang empfiehlt der EDSB die Aufnahme eines kollektiven Rechtsbehelfsverfahrens im Hinblick auf Verletzungen der Datenschutzvorschriften in das EU-Recht. Insbesondere kollektive Rechtsbehelfsverfahren, mit denen Bürgergruppen in die Lage versetzt werden, ihre Forderungen in einer Sammelklage zusammenzufassen, könnten ein äußerst wirksames Instrument zur Durchsetzung der Datenschutzvorschriften darstellen ([42]). Diese Neuerung wird ebenfalls von den Datenschutzbehörden im Dokument der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes unterstützt.

96. In Fällen mit einer geringeren Auswirkung ist es unwahrscheinlich, dass die Opfer einer Verletzung von Datenschutzvorschriften in Anbetracht der Kosten, Fristen, Ungewissheiten, Risiken und Lasten, denen sie ausgesetzt wären, eine Klage gegen die für die Verarbeitung Verantwortlichen einlegen. Diese Schwierigkeiten können überwunden oder wesentlich gemindert werden, wenn ein System für kollektive Rechtbehelfe bestünde, in dessen Rahmen die Opfer von Verletzungen ihre individuellen Forderungen in einer Sammelklage zusammenfassen könnten. Der EDSB befürwortet ferner die Befugnis qualifizierter Rechtsträger, wie z. B. Verbraucherverbänden oder öffentlichen Einrichtungen, zur Geltendmachung von Schadensersatzklagen im Namen der Opfer von Datenschutzverletzungen. Diese Klagen sollten keine Beeinträchtigung des Rechts der betroffenen Personen zur Einlegung individueller Klagen nach sich ziehen.

97. Sammelklagen sind nicht nur für die Gewährleistung einer vollständigen Entschädigung oder einer anderen Abhilfe von Bedeutung, sie dienen indirekt auch einer verstärkten Abschreckung. Das Risiko, im Rahmen solcher Klagen kostspieligen kollektiven Schadenersatz leisten zu müssen, würde die Motivation der für die Verarbeitung Verantwortlichen, die Einhaltung der Regeln zu gewährleisten, um ein Vielfaches erhöhen. In dieser Hinsicht wäre eine verbesserte Durchsetzung auf der Ebene von Privatpersonen mittels kollektiver Rechtsbehelfsmechanismen eine Ergänzung der öffentlichen Durchsetzung.

98. Die Mitteilung nimmt zu diesem Punkt nicht Stellung. Der EDSB ist sich der fortdauernden Diskussion über die Einführung eines kollektiven Rechtsbehelfs für Verbraucher auf europäischer Ebene bewusst. Er ist sich gleichfalls der Gefahr des Ausuferns bewusst, die diese Mechanismen nach den Erfahrungen in anderen Rechtssystemen mit sich bringen können. Allerdings stellen diese Faktoren seiner Ansicht nach keine ausreichenden Argumente dar, um die Aufnahme in die Datenschutzvorschriften vor dem Hintergrund der hiermit verbundenen Vorteile abzulehnen oder zu verschieben ([43]).

7. **Stärkung der Rolle von Organisationen/der für die Verarbeitung Verantwortlichen**

7.1 *Allgemeines*

99. Der EDSB ist der Ansicht, dass ein moderner Rechtsakt zum Datenschutz zusätzlich zu der Stärkung der Rechte des Einzelnen die notwendigen Instrumente zur Förderung der Verantwortung der für die Datenverarbeitung Verantwortlichen enthalten muss. Insbesondere muss die Rahmenregelung den für die Datenverarbeitung Verantwortlichen im privaten oder öffentlichen Sektor Anreize bieten, Maßnahmen zum Datenschutz vorausschauend in ihre Geschäftsprozesse aufzunehmen. Diese Instrumente wären in erster Linie hilfreich, weil — wie bereits weiter oben erwähnt — technologische Entwicklungen zu einem starken Anstieg der Erhebung, Verwendung und Weiterübermittlung personenbezogener Daten geführt haben, wodurch das Risiko für den Schutz der Privatsphäre und personenbezogener Daten Einzelner erhöht wird, was auf wirksame Weise ausgeglichen werden sollte. Zweitens sind in der aktuellen Regelung — mit Ausnahme weniger, klar festgelegter Bestimmungen (siehe weiter unten) — solche Instrumente nicht vorhanden und die für die Datenverarbeitung Verantwortlichen können gegenüber dem Schutz der Privatsphäre und dem Datenschutz eine *reagierende* Haltung einnehmen und erst tätig werden, wenn ein Problem bereits entstanden ist. Eine solche Vorgehensweise kommt in Statistiken zum Ausdruck, in denen mangelhafte Praktiken zur Einhaltung der Regeln und Datenverluste als wiederkehrende Probleme auftauchen.

100. Nach Ansicht des EDSB reicht die bestehende Regelung für einen wirksamen Schutz personenbezogener Daten unter den gegenwärtigen und zukünftigen Bedingungen nicht aus. Je höher die Risiken, desto größer die Notwendigkeit zur Durchführung von konkreten Maßnahmen, um Informationen in der Praxis zu schützen und einen wirksamen Schutz zu gewährleisten. Solange diese vorausschauenden Maßnahmen *de facto* nicht umgesetzt sind, werden Fehler, Pannen und Fahrlässigkeit wohl weiterhin die Privatsphäre des Einzelnen in dieser zunehmen digitalen Gesellschaft gefährden. Diesbezüglich schlägt der EDSB die folgenden Maßnahmen vor.

7.2 *Mehr Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen*

101. Der EDSB empfiehlt, eine neue Bestimmung in den Rechtsakt aufzunehmen, mit der die für die Datenverarbeitung Verantwortlichen verpflichtet werden, geeignete und wirksame Maßnahmen zur Umsetzung der im Rechtsakt formulierten Grundsätze und Pflichten durchzuführen und dies auf Verlangen nachzuweisen.

([41]) In den Vereinigten Staaten verlangt das Datenschutzgesetz für Kinder COPPA von den Betreibern gewerblicher Websites oder Onlinedienstleistungen, die sich an Kinder unter 13 richten, die Einwilligung der Eltern, bevor personenbezogene Informationen erhoben werden. Betreiber von gewerblichen Websites mit einer allgemeinen Zielgruppe müssen berücksichtigen, dass es sich bei einigen Besuchern um Kinder handelt.

([42]) Siehe auch die Stellungnahme des EDSB vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“, (ABl. C 255 vom 27.10.2007, S. 10).

([43]) Einige nationale Gesetzgebungen sehen bereits ähnliche Mechanismen vor.

102. Diese Art von Bestimmung ist nicht ganz neu. Artikel 6 Absatz 2 der Richtlinie 95/46/EG bezieht sich auf die Grundsätze im Hinblick auf die Datenqualität und führt aus: „Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen." Ebenso werden die für die Datenverarbeitung Verantwortlichen in Artikel 17 Absatz 1 aufgefordert, sowohl technische als auch organisatorische Maßnahmen durchzuführen. Diese Bestimmungen zeichnen sich jedoch durch einen begrenzten Anwendungsbereich aus. Die Aufnahme einer allgemeinen Bestimmung zur Rechenschaftspflicht würde die für die Verarbeitung Verantwortlichen anhalten, vorausschauende Maßnahmen zu ergreifen, um die Einhaltung sämtlicher Elemente der Datenschutzvorschriften zu erzielen.

103. Eine Bestimmung zur Rechenschaftspflicht hätte zur Folge, dass die für die Datenverarbeitung Verantwortlichen interne Mechanismen und Kontrollsysteme umsetzen müssten, um eine Einhaltung der Grundsätze und Verpflichtungen der Rahmenregelung zu gewährleisten. Dies würde beispielsweise erfordern, dass die oberste Führungsebene in die Datenschutzpolitik eingebunden wird, dass Verfahren zur Gewährleistung einer genauen Ermittlung aller Operationen zur Datenverarbeitung ausgearbeitet werden, dass eine verpflichtende Datenschutzpolitik bereitsteht, die Gegenstand einer fortlaufenden Überprüfung und Aktualisierung ist, damit neue Operationen zur Datenverarbeitung integriert werden können, dass Übereinstimmung mit den Grundsätzen der Datenqualität, der Meldung, Sicherheit und Auskunft erzielt wird usw. Dies würde ferner erfordern, dass die für die Verarbeitung Verantwortlichen Nachweise führen, um die Einhaltung der Regeln gegenüber den Behörden auf Verlangen nachweisen zu können. Ein Nachweis der Einhaltung von Regeln gegenüber der breiten Öffentlichkeit sollte in bestimmten Fällen ebenfalls zwingend vorgeschrieben werden. Dies könnte beispielsweise dadurch erfolgen, dass die für die Verarbeitung Verantwortlichen verpflichtet werden, den Datenschutz in öffentliche (Jahres-)berichte aufzunehmen, wenn solche Berichte aus anderen Gründen zwingend vorgeschrieben sind.

104. Selbstverständlich müssen die Kategorien der durchzuführenden internen und externen Maßnahmen geeignet sein und auf dem Sachverhalt und den Umständen eines jeden einzelnen Falls basieren. Es ist ein Unterschied, ob ein für die Verarbeitung Verantwortlicher mehrere Hundert nur aus Namen und Anschriften bestehende Kundendaten verarbeitet oder ob es sich bei der Verarbeitung um Daten von Millionen Patienten, einschließlich ihrer Krankengeschichte, handelt. Dasselbe gilt für die konkrete Art und Weise, in der die Wirksamkeit der Maßnahmen zu beurteilen ist. Es besteht Bedarf an Skalierbarkeit.

105. Der allgemeine umfassende Rechtsakt zum Datenschutz sollte nicht die konkreten Anforderungen an die Rechenschaftspflicht festlegen, sondern lediglich die wesentlichen Elemente. Die Mitteilung sieht bestimmte Elemente zur Stärkung der Verantwortung der für die Datenverarbeitung Verantwortlichen vor, was selbstverständlich begrüßt wird. Insbesondere unterstützt der EDSB in vollem Umfang, dass Datenschutzbeauftragte und Datenschutzfolgenabschätzungen unter bestimmten Schwellenbedingungen zwingend vorgeschrieben werden.

106. Darüber hinaus empfiehlt der EDSB die Ausstattung der Kommission mit Befugnissen nach Artikel 290 AEUV, um die für die Einhaltung des Rechenschaftsstandards erforderlichen Grundanforderungen zu ergänzen. Die Ausübung dieser Befugnisse würde die Rechtssicherheit der für die Datenverarbeitung Verantwortlichen stärken und die Einhaltung der Regeln innerhalb der EU harmonisieren. Bei der Entwicklung solch konkreter Instrumente sollten die Artikel-29-Datenschutzgruppe und der EDSB konsultiert werden.

107. Schließlich könnten die konkreten, von den für die Datenverarbeitung Verantwortlichen hinsichtlich der Rechenschaftspflicht durchzuführenden Maßnahmen auch durch die Datenschutzbehörden im Rahmen ihrer Durchsetzungsbefugnisse auferlegt werden. Hierzu könnten die Datenschutzbehörden mit neuen Befugnissen ausgestattet werden, die sie in die Lage versetzen, Abhilfemaßnahmen zu ergreifen oder Sanktionen aufzuerlegen. Beispiele sollten die Einrichtung interner Programme zur Einhaltung der Regeln, zur Durchführung des eingebauten Datenschutzes bei bestimmten Produkten und Dienstleistungen usw. umfassen. Abhilfemaßnahmen sollten nur insofern auferlegt werden, als diese angemessen, verhältnismäßig und wirksam sind, um die Einhaltung geltender und durchsetzbarer gesetzlicher Standards zu gewährleisten.

7.3 *Eingebauter Datenschutz*

108. Der eingebaute Datenschutz bezieht sich auf die Integration des Schutzes von Daten und der Privatsphäre von Beginn an bei neuen Produkten, Dienstleistungen und Verfahren, die eine Verarbeitung personenbezogener Daten beinhalten. Nach Ansicht des EDSB ist der eingebaute Datenschutz ein Element der Rechenschaftspflicht. Folglich wären die für die Datenverarbeitung Verantwortlichen auch verpflichtet, nachzuweisen, dass sie den eingebauten Datenschutz umgesetzt haben, wo dies angemessen ist. Kürzlich nahm die 32. Internationale Datenschutzkonferenz eine Entschließung an, die den eingebauten Datenschutz als wesentlichen Bestandteil des fundamentalen Datenschutzes anerkennt ([44]).

109. Die Richtlinie 95/46/EG enthält zwar mehrere Bestimmungen zur Förderung des eingebauten Datenschutzes ([45]), allerdings erkennt sie eine diesbezügliche Verpflichtung nicht ausdrücklich an. Der EDSB begrüßt die Unterstützung des eingebauten Datenschutzes durch die Kommission als Instrument zur Gewährleistung der Einhaltung der Datenschutzvorschriften. Er schlägt vor, eine verbindliche Bestimmung mit einer Verpflichtung zum „eingebauten Datenschutz" einzuführen, die auf

([44]) Entschließung zum eingebauten Datenschutz, angenommen von der 32. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 27. bis 29. Oktober 2010 in Jerusalem.

([45]) Die Richtlinie enthält Bestimmungen, die indirekt in verschiedenen Situationen die Umsetzung des eingebauten Datenschutzes fordern. Insbesondere wird in Artikel 17 verlangt, dass die für die Datenverarbeitung Verantwortlichen angemessene technische und organisatorische Maßnahmen treffen, um einer unrechtmäßigen Verarbeitung personenbezogener Daten vorzubeugen. Die Datenschutzrichtlinie für elektronische Kommunikation ist diesbezüglich explitziter. In Artikel 14 Absatz 3 wird ausgeführt: „Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist".

dem Wortlaut von Erwägungsgrund 46 der Richtlinie 95/46/EG aufbauen könnte. Insbesondere sollte die Bestimmung von den für die Datenverarbeitung Verantwortlichen ausdrücklich die Durchführung von technischen und organisatorischen Maßnahmen verlangen, und zwar sowohl zum Zeitpunkt der Konzeption des Verarbeitungssystems, als auch zum Zeitpunkt der Verarbeitung selbst, um insbesondere den Schutz personenbezogener Daten zu gewährleisten und einer unrechtmäßigen Verarbeitung vorzubeugen ([46]).

110. Auf der Grundlage einer solchen Bestimmung wären die für die Datenverarbeitung Verantwortlichen unter anderem verpflichtet, zu gewährleisten, dass die Systeme zur Datenverarbeitung so konzipiert sind, dass sie so wenig personenbezogene Daten wie möglich verarbeiten, um den eingebauten Datenschutz, beispielsweise in sozialen Netzwerken, umzusetzen, die Profile von Einzelnen gegenüber anderen standardmäßig geheim zu halten und Instrumente einzusetzen, mit deren Hilfe Benutzer ihre personenbezogenen Daten besser schützen können (z. B. Zugriffskontrollen, Verschlüsselung).

111. Die Vorteile einer ausdrücklicheren Bezugnahme auf den eingebauten Datenschutz können folgendermaßen zusammengefasst werden:

— Die Bedeutung des Grundsatzes *per se* würde betont, und zwar als Instrument zur Gewährleistung, dass die Verfahren, Produkte und Dienstleistungen von Beginn an unter Berücksichtigung des Datenschutzes konzipiert werden.

— Der Datenmissbrauch würde verringert und die unnötige Erhebung von Daten würde minimiert; Einzelpersonen würden hinsichtlich ihrer personenbezogenen Daten mit einer echten Wahlmöglichkeit ausgestattet.

— Nachträgliches „Flickwerk" zur Behebung von Problemen, die nur schwierig bis gar nicht zu beseitigen sind, würde vermieden.

— Überdies würde eine wirksame Anwendung und Durchsetzung dieses Grundsatzes durch die Datenschutzbehörden ermöglicht.

112. Eine solche Verpflichtung würde eine stärkere Nachfrage von Produkten und Dienstleistungen mit eingebautem Datenschutz nach sich ziehen, wodurch der Industrie Anreize zur Befriedigung dieser Nachfrage gegeben würden. Es sollte darüber hinaus erwogen werden, eine separate Verpflichtung für die Designer und Hersteller von neuen Produkten und Dienstleistungen zu schaffen, die sich auf den Datenschutz und den Schutz der Privatsphäre auswirken dürften. Der EDSB empfiehlt die Aufnahme einer solchen separaten Verpflichtung, die den für die Datenverarbeitung Verantwortlichen die Einhaltung ihrer eigenen Verpflichtung ermöglichen würde.

113. Die Festschreibung des eingebauten Datenschutzes könnte durch eine in Übereinstimmung mit diesem Grundsatz anzunehmende Bestimmung ergänzt werden, die generelle, auf alle Sektoren, Produkte und Dienstleistungen anzuwendende Anforderungen an den eingebauten Datenschutz vorschreibt, etwa die Gewährleistung von Maßnahmen zum „Empowerment" der Benutzer.

114. Zusätzlich empfiehlt der EDSB in Übereinstimmung mit Artikel 290 AEUV die Übertragung von Befugnissen an die Kommission, um gegebenenfalls die Grundanforderungen an den eingebauten Datenschutz für ausgewählte Produkte und Dienstleistungen zu ergänzen. Die Ausübung dieser Befugnisse würde die Rechtssicherheit der für die Datenverarbeitung Verantwortlichen erhöhen und die Einhaltung der Regeln innerhalb der EU harmonisieren. Zur Entwicklung dieser spezifischen Instrumente sollten die Artikel-29-Datenschutzgruppe und der EDSB konsultiert werden (siehe ebenfalls Absatz 106 zur Rechenschaftspflicht).

115. Schließlich sollten die Datenschutzbehörden mit der Befugnis ausgestattet werden, unter ähnlich restriktiven Voraussetzungen, wie sie bereits in Absatz 107 erwähnt wurden, Abhilfemaßnahmen zu ergreifen oder Sanktionen aufzuerlegen, falls die für die Verarbeitung Verantwortlichen eindeutig versäumt haben, konkrete Schritte in Fällen zu unternehmen, wo dies erforderlich gewesen wäre.

7.4 *Zertifizierungsdienste*

116. In der Mitteilung wird die Notwendigkeit anerkannt, die Schaffung von EU-Zertifizierungsregelungen für Produkte und Dienstleistungen zu untersuchen, die aus Sicht des Datenschutzes unbedenklich sind. Der EDSB unterstützt dieses Ziel vorbehaltlos und empfiehlt, eine Bestimmung, die zu einem späteren Zeitpunkt in zusätzlichen Rechtsvorschriften weiterentwickelt werden kann, zur Schaffung solcher Regelungen und ihrer denkbaren Auswirkungen innerhalb der EU aufzunehmen. Die Bestimmung sollte die Bestimmungen zur Rechenschaftspflicht und zum eingebauten Datenschutz ergänzen.

117. Freiwillige Zertifizierungsregelungen würden die Überprüfung ermöglichen, dass ein für die Datenverarbeitung Verantwortlicher Maßnahmen zur Einhaltung des Rechtsakts ergriffen hat. Darüber hinaus erzielen für die Datenverarbeitung Verantwortliche — oder sogar Produkte oder Dienstleistungen —, die einen Zertifizierungsnachweis besitzen, wahrscheinlich einen Wettbewerbsvorteil gegenüber anderen. Derartige Regelungen würden auch die Datenschutzbehörden bei ihrer Aufsichts- und Durchsetzungsfunktion unterstützen.

8. **Globalisierung und anwendbares Recht**

8.1 *Eine klare Notwendigkeit für einen einheitlicheren Schutz*

118. Wie bereits in Kapitel 2 erwähnt, ist die Übermittlung personenbezogener Daten über die EU-Grenzen hinaus als Folge der Entwicklung neuer Technologien, der Rolle multinationaler Unternehmen und des gestiegenen Einflusses von Regierungen auf die Verarbeitung und gemeinsame Nutzung personenbezogener Daten im internationalen Maßstab exponentiell gestiegen. Dies ist einer der Hauptgründe, die die Überprüfung des aktuellen Rechtsrahmens rechtfertigen. Folglich ist dies einer der Bereiche, für den der EDSB Ehrgeiz und Wirksamkeit fordert, weil eine klare Notwendigkeit für einen einheitlicheren Datenschutz besteht, wenn Daten außerhalb der EU verarbeitet werden.

([46]) Im Rahmen der gegenwärtigen Regelung wird die Durchführung solcher Maßnahmen durch die für die Verarbeitung Verantwortlichen in Erwägungsgrund 46 unterstützt, allerdings ist ein Erwägungsgrund nicht rechtsverbindlich.

8.2 *Engagement für internationale Vorschriften*

119. Nach Ansicht des EDSB ist mehr Engagement bei der Ausarbeitung internationaler Vorschriften vonnöten. Eine weitere Harmonisierung im Hinblick auf das weltweite Schutzniveau personenbezogener Daten könnte die Eckpunkte der einzuhaltenden Grundsätze und die Voraussetzungen für Datenübermittlungen beträchtlich klären. Diese globalen Vorschriften müssten die Anforderung an einen hohen Datenschutzstandard — einschließlich der Kernelemente aus dem EU-Datenschutz — mit regionalen Besonderheiten in Einklang bringen.

120. Der EDSB unterstützt die zielgerichtete Arbeit, die bisher im Rahmen der internationalen Konferenz der Beauftragten für den Datenschutz zur Entwicklung und Verbreitung der sogenannten „Madrider Standards" geleistet wurde, mit der Absicht, diese in ein verbindliches Instrument zu integrieren und möglicherweise eine intergouvernementale Konferenz einzusetzen. ([47]) Er ruft die Kommission dazu auf, die entsprechenden Initiativen zu ergreifen, um die Erreichung dieses Ziels zu erleichtern.

121. Nach Ansicht des EDSB ist es zudem wichtig, die Stimmigkeit zwischen diesen Inititativen zu internationalen Standards, der gegenwärtigen Überprüfung des EU-Datenschutzrahmens und anderen Entwicklungen, wie der gegenwärtigen Überprüfung der OECD-Datenschutzrichtlinien und des Übereinkommens Nr. 108 des Europarats, das von Drittländern unterzeichnet werden kann, zu gewährleisten (siehe auch Absatz 17). Der EDSB ist der Ansicht, dass die Kommission in diesem Zusammenhang eine klare Rolle zu spielen hat, indem sie festlegt, wie sie diese Stimmigkeit in den Verhandlungen mit der OECD und dem Europarat fördern will.

8.3 *Klärung der Kriterien des anwendbaren Rechts*

122. Da eine vollständige Einheitlichkeit nicht einfach zu erreichen ist, wird — zumindest in der nahen Zukunft — eine gewisse Uneinheitlichkeit zwischen den Gesetzen innerhalb der EU und umso mehr über die Grenzen der EU hinaus bestehen bleiben. Der EDSB ist der Ansicht, dass in einem neuen Rechtsakt die Kriterien zur Festlegung des anwendbaren Rechts und vereinfachte Mechanismen für den Datenfluss sowie die Rechenschaftspflicht der in den Datenfluss eingebundenen Akteure festgelegt werden müssen.

123. Der Rechtsakt sollte in erster Linie gewährleisten, dass die EU-Rechtsvorschriften bei der Verarbeitung personenbezogener Daten außerhalb der Grenzen der EU anwendbar sind, wo die Anwendung von EU-Recht gerechtfertigt ist. Das Beispiel von nicht-europäischen Cloud-Computing-Dienstleistungen, die auf EU-Bürger abzielen, zeigt, warum dies erforderlich ist. In einer Umgebung, in der Daten nicht physisch gespeichert und an einem bestimmten Standort verarbeitet werden und in der die in verschiedenen Ländern ansässigen Anbieter von Dienstleistungen und Benutzer einen erheblichen Einfluss auf die Daten ausüben, ist es sehr schwierig, festzustellen, wer für die Einhaltung der Datenschutzgrundsätze verantwortlich ist. Insbesondere die Datenschutzbehörden stellen Leitlinien bereit, wie die Richtlinie 95/46/EG in solchen Fällen auszulegen und anzuwenden ist, aber Leitlinien alleine sind nicht ausreichend, um Rechtssicherheit in diesem neuen Umfeld zu gewährleisten.

124. Was das Gebiet der EU anbelangt, wurde die Notwendigkeit von mehr Klarheit im neuen Rechtsrahmen sowie für ein vereinfachtes Kriterium zur Festlegung des anwendbaren Rechts von der Artikel-29-Datenschutzgruppe in einer kürzlich angenommenen Stellungnahme betont ([48]).

125. Nach Ansicht des EDSB besteht die bevorzugte Option in der Annahme des Rechtsakts in Form einer Verordnung, die identische, in allen Mitgliedstaaten anwendbare Vorschriften zur Folge hätte. Eine Verordnung würde die Notwendigkeit verringern, das anwendbare Recht festzulegen. Dies ist einer der Gründe dafür, dass der EDSB die Annahme einer Verordnung vorzieht. Allerdings könnte auch eine Verordnung einigen Spielraum für die Mitgliedstaaten lassen. Sollte im neuen Rechtsakt ein bedeutender Spielraum gewahrt werden, unterstützt der EDSB die Empfehlung der Artikel-29-Datenschutzgruppe, eine Verlagerung von der parallelen Anwendung verschiedener nationaler Gesetzgebungen zu einer zentralisierten Anwendung einer einzelnen Gesetzgebung in allen Mitgliedstaaten, in denen ein für die Verarbeitung Verantwortlicher ansässig ist, zu vollziehen. Der EDSB setzt sich auch für eine verstärkte Zusammenarbeit und Koordination zwischen den Datenschutzbehörden in transnationalen Fällen und Beschwerden ein (siehe Kapitel 10).

8.4 *Vereinfachung der Mechanismen für die Datenflüsse*

126. Die Notwendigkeit der Einheitlichkeit und hoher Maßstäbe muss nicht nur in Anbetracht der globalen Grundsätze zum Datenschutz, sondern auch mit Blick auf internationale Übermittlungen berücksichtigt werden. Der EDSB unterstützt uneingeschränkt das Ziel der Kommission, die aktuellen Verfahren für internationale Übermittlungen zu vereinfachen und eine einheitlichere und kohärentere Vorgehensweise gegenüber Drittländern und internationalen Organisationen zu gewährleisten.

127. Der Mechanismus der Datenflüsse umfasst sowohl Übermittlungen des privaten Sektors, insbesondere im Rahmen von Vertragsklauseln oder verbindlichen unternehmensinternen Vorschriften, als auch des öffentlichen Sektors sowie Übermittlung zwischen Behörden. Verbindliche unternehmensinterne Vorschriften gehören zu den Elementen, bei denen eine kohärentere und vereinfachte Vorgehensweise wünschenswert wäre. Der EDSB empfiehlt, die Voraussetzungen für verbindliche unternehmensinterne Vorschriften im neuen Rechtsakt ausdrücklich zu festzulegen ([49]), und zwar wie folgt:

— Ausdrückliche Anerkennung von verbindlichen unternehmensinternen Vorschriften als Instrument zur Bereitstellung von angemessenen Garantien;

— Bereitstellung der wesentlichen Elemente/Voraussetzungen für die Annahme von verbindlichen unternehmensinternen Vorschriften;

([47]) Nach Maßgabe der Empfehlung in der Entschließung zum eingebauten Datenschutz, angenommen von der 32. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 27. bis 29. Oktober 2010 in Jerusalem.

([48]) Stellungnahme der Artikel-29-Datenschutzgruppe 8/2010 zum anwendbaren Recht, WP 179.

([49]) Zu internationalen Übermittlungen siehe auch Kapitel 8 der Stellungnahme.

— Darlegung der Verfahren zur Zusammenarbeit für die Annahme von verbindlichen unternehmensinternen Vorschriften, einschließlich der Kriterien für die Auswahl einer leitenden Aufsichtsbehörde (zentrale Anlaufstelle).

9. **Der Bereich Polizei und Justiz**

9.1 *Der allgemeine Rechtsakt*

128. Die Kommission betonte wiederholt die Bedeutung einer Stärkung des Datenschutzes im Zusammenhang mit der Strafverfolgung und der Vorbeugung von Kriminalität als Bereiche, in denen der Austausch und die Verwendung personenbezogener Informationen stark zugenommen hat. Das vom Europäischen Rat angenommene Stockholmer Programm nimmt ebenfalls Bezug auf ein starkes Datenschutzsystem als Hauptvoraussetzung für eine EU-Strategie zum Informationsmanagement in diesem Bereich ([50]).

129. Die Überprüfung des allgemeinen Datenschutzrahmens ist eine ideale Gelegenheit, um diesbezüglich Fortschritte zu machen, zumal der Rahmenbeschluss 2008/977/JI in der Mitteilung zu Recht als unzureichend beschrieben wird ([51]).

130. Der EDSB hat in Abschnitt 3.2.5 dieser Stellungnahme dargelegt, warum der Bereich der polizeilichen und justiziellen Zusammenarbeit in einen allgemeinen Rechtsakt aufgenommen werden sollte. Die Aufnahme von Polizei und Justiz bietet eine Reihe zusätzlicher Vorteile. Dies bedeutet, dass die Vorschriften nicht länger nur für den grenzübergreifenden Datenaustausch ([52]), sondern auch für die Verarbeitung im Inland gelten. Ein angemessener Schutz beim Austausch personenbezogener Daten mit Drittländern wird so auch im Hinblick auf internationale Vereinbarungen besser gewährleistet. Darüber hinaus werden die Datenschutzbehörden über dieselben umfassenden und harmonisierten Befugnisse gegenüber den Polizei- und Justizbehörden verfügen, wie anderen für die Datenverarbeitung Verantwortlichen gegenüber. Schließlich wird der jetzige Artikel 13, der den Mitgliedstaaten die Befugnis verleiht, Rechtsvorschriften zur Einschränkung von Verpflichtungen und Rechten im Rahmen des allgemeinen Rechtsakts für bestimmte öffentliche Interessen anzunehmen, in derselben restriktiven Weise wie in anderen Bereichen anzuwenden sein. Insbesondere sind die spezifischen Garantien, die in diesem Bereich in einem allgemeinen Rechtsakt bereitgestellt werden, ebenfalls von der nationalen Gesetzgebung, die für den Bereich der polizeilichen und justiziellen Zusammenarbeit verabschiedet wird, zu berücksichtigen.

9.2 *Zusätzliche spezifische Vorschriften für Polizei und Justiz*

131. Allerdings schließt eine solche Einbindung spezielle Vorschriften und Abweichungen, die die Besonderheiten dieses Sektors im Einklang mit der dem Vertrag von Lissabon angefügten Erklärung 21 gebührend berücksichtigen, nicht aus. Einschränkungen der Rechte der betroffenen Personen können festgelegt werden, allerdings müssen sie notwendig und verhältnismäßig sein und dürfen die wesentlichen Elemente des Rechts an sich nicht verändern. In diesem Zusammenhang ist zu betonen, dass die Richtlinie 95/46/EG, einschließlich Artikel 13, gegenwärtig auf verschiedene Bereiche der Strafverfolgung anwendbar ist (z. B. Steuern, Zoll, Betrugsbekämpfung), die sich nicht grundlegend von vielen Tätigkeiten im Bereich Polizei und Justiz unterscheiden.

132. Darüber hinaus müssen auch bestimmte Garantien eingesetzt werden, um die betroffenen Personen durch einen zusätzlichen Schutz in einem Bereich, in dem die Verarbeitung personenbezogener Daten eine einschneidendere Wirkung hat, zu entschädigen.

133. Vor dem Hintergrund der weiter oben gemachten Ausführungen ist der EDSB der Ansicht, dass der neue Rechtsakt im Einklang mit dem Übereinkommen Nr. 108 und der Empfehlung Nr. R (87) 15 zumindest die folgenden Elemente beinhalten sollte:

— Eine Unterscheidung zwischen verschiedenen Daten- und Dateikategorien nach ihrer Richtigkeit und Zuverlässigkeit, ausgehend von dem Prinzip, dass auf Sachverhalten basierende Daten von Daten unterschieden werden sollten, die auf Meinungen oder persönlicher Beurteilung beruhen.

— Eine Unterscheidung zwischen verschiedenen Kategorien betroffener Personen (mutmaßliche Straftäter, Opfer, Zeugen usw.) und Dateien (zeitlich befristete, zeitlich unbefristete und nachrichtendienstliche Dateien). Spezifische Bedingungen und Garantien müssen für die Verarbeitung von Daten von Personen festgelegt werden, bei denen es sich nicht um Verdächtigte handelt.

— Mechanismen zur Gewährleistung einer regelmäßig stattfindenden Überprüfung und Berichtigung zur Sicherstellung der Qualität der zu verarbeitenden Daten.

— Spezifische Bestimmungen und/oder Garantien können im Hinblick auf die (zunehmend bedeutsame) Verarbeitung biometrischer und genetischer Daten im Bereich der Strafverfolgung verfügt werden. Ihre Verwendung sollte ausschließlich auf Fälle beschränkt werden, in denen keine anderen, weniger stark eingreifenden Mittel verfügbar sind, mit denen sich der gleiche Zweck erreichen ließe ([53]).

— Bedingungen für die Übermittlung personenbezogener Daten an nicht zuständige Behörden und private Stellen sowie Bedingungen für die Auskunft und Weiterverwendung personenbezogener, von privater Seite erhobener Daten durch Strafverfolgungbehörden.

([50]) Siehe diesbezüglich die Stellungnahme des EDSB vom 30. September 2010 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat — „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht", Absätze 9-19.

([51]) Siehe Abschnitt 3.2.5 weiter oben.

([52]) Dies ist gegenwärtig der beschränkte Anwendungsbereich des Rahmenbeschlusses 2008/977/JI.

([53]) In dieser Hinsicht siehe Dokument der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes, Absatz 112.

9.3 *Sektorspezifische Datenschutzvorschriften*

134. In der Mitteilung wird ausgeführt: „Zudem ersetzt der Rahmenbeschluss nicht die auf EU-Ebene erlassenen sektorspezifischen Vorschriften über die polizeiliche und justizielle Zusammenarbeit in Strafsachen, insbesondere nicht die Rechtsakte über Europol, Eurojust, das Schengener Informationssystem (SIS) und das Zollinformationssystem (ZIS), die entweder spezielle Datenschutzvorschriften enthalten und/oder auf die Datenschutzübereinkommen des Europarates verweisen".

135. Nach Ansicht des EDSB sollte ein neuer Rechtsrahmen möglichst klar, einfach und kohärent sein. Während eine zunehmende Zahl unterschiedlicher Vorschriften beispielsweise auf Europol, Eurojust, SIS und Prüm anwendbar sind, bleibt die Einhaltung der Vorschriften kompliziert oder wird immer noch komplizierter. Dies ist einer der Gründe dafür, warum der EDSB einen umfassenden Rechtsakt für alle Bereiche befürwortet.

136. Der EDSB ist sich allerdings bewusst, dass eine Angleichung der Vorschriften aus den verschiedenen Systemen beträchtliche Arbeit erfordert, die sorgfältig ausgeführt werden muss. Der EDSB ist der Ansicht, dass die in der Mitteilung erwähnte Schritt-für-Schritt-Vorgehensweise so lange einen Sinn ergibt, wie die Verpflichtung zur Gewährleistung eines hohen Datenschutznivaus auf kohärente und wirksame Weise klar und sichtbar bleibt. Konkreter gesagt:

— In einer ersten Phase sollte der allgemeine Rechtsakt zum Datenschutz für alle Verarbeitungen im Bereich der polizeilichen und justiziellen Zusammenarbeit anwendbar gemacht werden, einschließlich der Anpassungen für Polizei und Justiz (wie in 9.2 ausgeführt).

— In einer zweiten Phase sollten die sektorspezifischen Datenschutzvorschriften an diesen allgemeinen Rechtsakt angeglichen werden. Die Kommission sollte sich selbst dazu verpflichten, innerhalb eines kurzen und klar abgesteckten Zeitraums Vorschläge für diese zweite Phase anzunehmen.

10. **Datenschutzbehörden und die Zusammenarbeit zwischen Datenschutzbehörden**

10.1 *Stärkung der Rolle der Datenschutzbehörden*

137. Der EDSB unterstützt uneingeschränkt das Ziel der Kommission, die Frage der Rechtsstellung der Datenschutzbehörden zu klären und insbesondere ihre Unabhängigkeit, Ressourcen und Durchsetzungsbefugnisse zu stärken.

138. Der EDSB besteht überdies auf der Notwendigkeit, im Rahmen des neuen Rechtsakts den grundlegenden Begriff der Unabhängigkeit der Datenschutzbehörden zu klären. Der Europäische Gerichtshof hat kürzlich zu diesem Problem ein Urteil im Fall C-518/07 ([54]) gesprochen, in dem betont wird, dass die Unabhängigkeit die Abwesenheit von äußeren Einflüssen beinhaltet. Eine Datenschutzbehörde darf weder um Weisungen ersuchen noch Weisungen entgegennehmen. Der EDSB empfiehlt ausdrücklich, diese Elemente der Unabhängigkeit rechtlich zu verankern.

139. Zur Wahrnehmung ihrer Aufgaben müssen die Datenschutzbehörden mit ausreichend Personal und finanziellen Mitteln ausgestattet werden. Der EDSB schlägt vor, diese Anforderung in den Rechtsakt aufzunehmen ([55]). Schließlich betont der EDSB die Notwendigkeit, sicherzustellen, dass die Behörden über vollständig harmonisierte Befugnisse im Hinblick auf die Ermittlung und die Auferlegung ausreichender Maßnahmen zur Abschreckung und Abhilfe sowie Sanktionen verfügen. Dies würde auch die Rechtssicherheit für die betroffenen Personen und die für die Datenverarbeitung Verantwortlichen verbessern.

140. Eine Stärkung der Unabhängigkeit, der Ressourcen und der Befugnisse der Datenschutzbehörden sollte mit einer verstärkten Zusammenarbeit auf mulitlateraler Ebene einhergehen, insbesondere angesichts der zunehmenden Zahl von Datenschutzproblemen auf europäischer Ebene. Hauptakteur bei dieser Zusammenarbeit wird offensichtlicherweise die Artikel-29-Datenschutzgruppe sein.

10.2 *Stärkung der Rolle der Artikel-29-Datenschutzgruppe*

141. Wie die Vergangenheit zeigt, hat sich die Funktionsweise der Gruppe seit ihrer Gründung 1997 entwickelt. Sie ist in eine stärkere Unabhängigkeit hineingewachsen und in der Praxis nicht nurmehr eine einfache, beratende Arbeitsgruppe für die Kommission. Der EDSB empfiehlt weitere Verbesserungen der Funktionsweise der Artikel-29-Datenschutzgruppe, einschließlich ihrer Ausstattung und Unabhängigkeit.

142. Der EDSB ist der Ansicht, dass die Stärke dieser Gruppe untrennbar mit der Unabhängigkeit und den Befugnissen ihrer Mitglieder verknüpft ist. Die Autonomie der Artikel-29-Datenschutzgruppe sollte in dem neuen Rechtsrahmen gemäß den Kriterien gewährleistet werden, die für eine vollständige Unabhängigkeit der Datenschutzbehörden durch den Europäischen Gerichtshof im Fall C-518/07 aufgestellt wurden. Der EDSB ist der Ansicht, dass die Artikel-29-Datenschutzgruppe ferner mit ausreichenden Ressourcen und einem entsprechenden Haushalt für ein verstärktes Sekretariat ausgestattet werden sollte, um ihren Beitrag zu unterstützen.

143. Im Hinblick auf das Sekretariat der Artikel-29-Datenschutzgruppe wertschätzt der EDSB, dass dieses in das Referat Datenschutz der Generaldirektion Justiz integriert ist, was den Vorteil hat, dass die Artikel-29-Datenschutzgruppe von den effizienten und flexiblen Kontakten und aktuellen Information zu Datenschutzentwicklungen profitieren kann. Andererseits stellt der EDSB die Tatsache in Frage, dass die Kommission (und insbesondere das Referat) gleichzeitig Mitglied, Sekretariat und Empfänger der Stellungnahmen der Datenschutzgruppe ist. Dies würde eine größere Unabhängigkeit des Sekretariats rechtfertigen. Der EDSB ermutigt die Kommission, in enger Absprache mit den Interessengruppen zu prüfen, wie diese Unabhängigkeit am besten gewährleistet werden kann.

([54]) Fall C-518/07, *Kommission/Deutschland,* noch nicht veröffentlicht in der Slg.

([55]) Siehe beispielsweise Artikel 43 Absatz 2 der Verordnung (EG) Nr. 45/2001, die solche Anforderungen an den EDSB enthält.

144. Schließlich erfordert eine Stärkung der Befugnisse der Datenschutzbehörden auch stärkere Befugnisse der Artikel-29-Datenschutzgruppe, mit einer Struktur, die bessere Vorschriften und Garantien und mehr Transparenz bietet. Dies gilt es gleichermaßen für die beratende und die durchsetzende Rolle der Artikel-29-Datenschutzgruppe auszugestalten.

10.3 *Die beratende Rolle der Artikel-29-Datenschutzgruppe*

145. Die Standpunkte der Artikel-29-Datenschutzgruppe müssen im Rahmen der beratenden Rolle gegenüber der Kommission wirksam umgesetzt werden, insbesondere hinsichtlich der Auslegung und Anwendung der Grundsätze der Richtlinie und anderer Datenschutzinstrumente. Mit anderen Worten, der verbindliche Charakter der Standpunkte der Datenschutzgruppe muss gewährleistet sein. Zwischen den Datenschutzbehörden besteht weiterer Diskussionsbedarf, um festzulegen, wie dies in den Rechtsakt aufgenommen werden soll.

146. Der EDSB empfiehlt Lösungen, durch die die Stellungnahmen der Datenschutzgruppe verbindlicher würden, ohne ihre Funktionsweise wesentlich zu verändern. Der EDSB empfiehlt, auf der Grundlage des für die Standpunkte des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) ([56]) angenommenen Modells für die Datenschutzbehörden und die Kommission eine Verpflichtung einzuführen, den Stellungnahmen und gemeinsamen Standpunkten, die von der Datenschutzgruppe angenommen wurden, weitestgehend Rechnung zu tragen. Darüber hinaus könnte der neue Rechtsakt die Artikel-29-Datenschutzgruppe mit der ausdrücklichen Aufgabe betrauen, „Empfehlungen zur Auslegung" zu erteilen. Diese alternativen Lösungen würden den Standpunkten der Artikel-29-Datenschutzgruppe eine stärkere Rolle, auch bei Gericht, verleihen.

10.4 *Koordinierte Durchsetzung durch die Artikel-29-Datenschutzgruppe*

147. In der gegenwärtigen Rahmenregelung ist die Durchsetzung der Datenschutzgesetzgebung in den Mitgliedstaaten den 27 Datenschutzbehörden überlassen, mit wenig Koordination hinsichtlich der Handhabung spezifischer Fälle. Wenn mehr als ein Mitgliedstaat an einem Fall beteiligt ist oder bei Fällen mit einer eindeutig globalen Dimension werden auf diese Weise die Kosten, die bei verschiedenen Behörden für dieselbe Tätigkeit anfallen, vervielfacht und das Risiko einer uneinheitlichen Anwendung nimmt zu: in Extremfällen können dieselben Tätigkeiten im Rahmen einer Verarbeitung von einer Datenschutzbehörde als rechtmäßig und von einer anderen als unzulässig betrachtet werden.

148. Manche Fälle haben eine strategische Dimension, die auf zentralisierte Weise behandelt werden sollte. Die Artikel-29-Datenschutzgruppe stellt Koordinierung und Durchsetzungsmaßnahmen zwischen den Datenschutzbehörden ([57]) bei größeren Datenschutzproblemen mit internationaler Dimension bereit. Dies war bei sozialen Netzwerken und Suchmaschinen ([58]) und bei koordinierten Inspektionen der Fall, die in verschiedenen Mitgliedstaaten im Hinblick auf Probleme in der Telekommunikation und der Krankenversicherung durchgeführt wurden.

149. Allerdings gibt es Grenzen für die Durchsetzungsmaßnahmen, die die Artikel-29-Datenschutzgruppe im gegenwärtigen Rahmen ergreifen kann. Die Datenschutzgruppe kann zwar gemeinsame Standpunkte verabschieden, es gibt jedoch kein Instrument, um zu gewährleisten, dass diese Standpunkte tatsächlich in die Praxis umgesetzt werden.

150. Der EDSB schlägt vor, in den Rechtsakt zusätzliche Bestimmungen aufzunehmen, die eine koordinierte Durchsetzung unterstützen könnten, und zwar insbesondere:

— Eine Verpflichtung zur Gewährleistung, dass die Datenschutzbehörden und die Kommission den Stellungnahmen und gemeinsamen Standpunkten, die von der Artikel-29-Datenschutzgruppe angenommen wurden, weitestgehend Rechnung tragen ([59]).

— Eine Verpflichtung für die Datenschutzbehörden zu einer zuverlässigen Zusammenarbeit untereinander sowie mit der Kommission und der Artikel-29-Datenschutzgruppe ([60]). Zur praktischen Veranschaulichung einer zuverlässigen Zusammenarbeit könnte ein Verfahren eingesetzt werden, in dessen Rahmen die Datenschutzbehörden im Fall von nationalen Durchsetzungsmaßnahmen mit einem grenzübergreifenden Element die Kommission oder die Datenschutzgruppe informieren, analog zu dem Verfahren, das in der aktuellen Rahmenregelung im Hinblick auf Entscheidungen der nationalen Angemessenheit anwendbar ist.

— Eine Präzisierung der Abstimmungsregeln für mehr Verpflichtungszusagen der Datenschutzbehörden, die Entscheidungen der Datenschutzgruppe umzusetzen. Es könnte festgelegt werden, dass die Artikel-29-Datenschutzgruppe eine Entscheidung auf der Grundlage eines Konsenses vorsieht, und - falls ein Konsens nicht erzielt werden kann - eine Durchsetzung nur mit einer qualifizierten Mehrheit erfolgt. Zusätzlich hierzu könnte ein Erwägungsgrund vorsehen, dass

([56]) Verordnung (EG) Nr. 1211/2009 des Europäischen Parlaments und des Rates vom 25. November 2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros, (ABl. L 337, 18.12.2009, S. 1).

([57]) Neben der Artikel-29-Datenschutzgruppe hat die Europäische Konferenz der Beauftragten für den Datenschutz vor ungefähr zehn Jahren einen dauerhaften Arbeitskreis geschaffen, der auf die Behandlung von grenzübergreifenden Beschwerden auf koordinierte Weise abzielt. Obwohl dieser Arbeitskreis unbestreitbar einen zusätzlichen Nutzen im Hinblick auf den Austausch zwischen dem Personal der Datenschutzbehörden darstellt und ein zuverlässiges Netzwerk an Kontaktstellen anbietet, kann er nicht als Koordinierungsmechanismus für die Entscheidungsfindung betrachtet werden.

([58]) Siehe die Schreiben der Artikel-29-Datenschutzgruppe vom 12. Mai 2010 und 26. Mai 2010, veröffentlicht auf der Website der Datenschutzgruppe (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Wie weiter oben erwähnt, ist in Verordnung (EG) Nr. 1211/2009 eine ähnliche Verpflichtung ausgeführt, mit der die Rolle des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) festgelegt wird.

([60]) Siehe diesbezüglich Artikel 3 der weiter oben zitierten Verordnung (EG) Nr. 1211/2009.

Datenschutzbehörden, die für ein Dokument stimmen, eine Verpflichtung eingehen bzw. eine Verpflichtungszusage abgeben, dies auf nationaler Ebene durchzuführen.

151. Der EDSB hat Vorbehalte gegen die Einführung weiterreichenderer Maßnahmen, wie eine Rechtsverbindlichkeit der Standpunkte der Artikel-29-Datenschutzgruppe. Hierdurch würde der unabhängige Status der einzelnen Datenschutzbehörden untergraben, der durch die Mitgliedstaaten unter nationalem Recht gewährleistet werden muss. Falls die Entscheidungen der Datenschutzgruppe eine direkte Auswirkung auf Dritte wie für die Datenverarbeitung Verantwortliche hätten, sollten neue Verfahren, einschließlich Garantien wie Transparenz und Rechtsbehelfe, und einschließlich möglicher Rechtsbehelfe vor dem Europäischen Gerichtshof, festgelegt werden.

10.5 *Zusammenarbeit zwischen dem EDSB und der Artikel-29-Datenschutzgruppe*

152. Die Art und Weise der Zusammenarbeit zwischen dem EDSB und der Artikel-29-Datenschutzgruppe könnte ebenfalls besser aufeinander abgestimmt werden. Der EDSB ist ein Mitglied der Datenschutzgruppe und trägt innerhalb der Gruppe zu den Standpunkten hinsichtlich der wesentlichen strategischen EU-Entwicklungen bei und gewährleistet gleichzeitig die Stimmigkeit mit seinen eigenen Standpunkten. Der EDSB stellt eine wachsende Anzahl von Datenschutzproblemen sowohl im privaten als auch im öffentlichen Sektor fest, die sich auf nationaler Ebene in vielen Mitgliedstaaten auswirken und bei denen die Datenschutzgruppe eine bestimmte Rolle spielen muss.

153. Der EDSB hat eine ergänzende Aufgabe, die in der Beratung zu Entwicklungen im Kontext der EU besteht und beibehalten werden sollte. Als europäische Einrichtung übt er diese Beratungsbefugnis gegenüber den EU-Organen in derselben Weise aus, wie nationale Datenschutzbehörden ihre Regierungen beraten.

154. Der EDSB und die Artikel-29-Datenschutzgruppe agieren aus einer unterschiedlichen, jedoch sich ergänzenden Position heraus. Aus diesem Grund besteht die Notwendigkeit zur Beibehaltung und möglicherweise zur Verbesserung der Zusammenarbeit zwischen der Artikel-29-Datenschutzgruppe und dem EDSB, um zu gewährleisten, dass sie sich gemeinsam mit den wichtigsten Datenschutzproblemen befassen, beispielsweise durch die regelmäßige Koordinierung der Tagesordnung ([61]) und die Sicherstellung von Transparenz bei Problemen mit einem stärker nationalen oder spezifischen EU-Aspekt.

155. Eine Koordinierung wird in der gegenwärtigen Richtlinie aus dem einfachen Grund nicht erwähnt, dass der EDSB zum Zeitpunkt der Annahme der Richtlinie noch nicht existierte; allerdings ist nach einem sechsjährigen Bestehen der ergänzende Charakter des EDSB und der Artikel-29-Datenschutzgruppe sichtbar und könnte formal anerkannt werden. Der EDSB erinnert ferner daran, dass er nach Maßgabe der Verordnung (EG) Nr. 45/2001 verpflichtet ist, mit den nationalen Datenschutzbehörden zusammenzuarbeiten und an den Arbeiten der Artikel-29-Datenschutzgruppe teilzunehmen. Der EDSB empfiehlt, die Zusammenarbeit im neuen Rechtsakt ausdrücklich zu erwähnen und gegebenenfalls zu strukturieren, beispielsweise durch Festlegung eines Verfahrens zur Zusammenarbeit.

10.6 *Zusammenarbeit zwischen dem EDSB und den Datenschutzbehörden zur Aufsicht über EU-Systeme*

156. Diese Erwägungen beziehen sich auch auf Bereiche, in denen die Aufsicht zwischen der europäischen und der nationalen Ebene koordiniert werden muss. Dies ist der Fall bei EU-Einrichtungen, die große, von nationalen Behörden bereitgestellte Datenmengen verarbeiten, oder bei informationstechnischen Großsystemen mit einer europäischen und einer nationalen Komponente.

157. Das bei einigen EU-Einrichtungen und informationstechnischen Großsystemen bestehende System — beispielsweise verfügen Europol, Eurojust und die erste Generation des Schengener Informationssystems (SIS) über eine gemeinsame Kontrollinstanz mit Vertretern der nationalen Datenschutzbehörden — ist ein Überbleibsel der Zusammenarbeit zwischen Regierungen aus der Ära vor Lissabon und berücksichtigt nicht die institutionelle Struktur der EU, in die Europol und Eurojust nun fest eingebunden sind und in die auch der „Schengen-Besitzstand" integriert wurde ([62]).

158. In der Mitteilung wird angekündigt, dass die Kommission 2011 eine Konsultation der interessierten Kreise zur Überprüfung dieser Aufsichtssysteme einleitet. Der EDSB fordert die Kommission nachdrücklich auf, so bald wie möglich (innerhalb einer kurzen und festgelegten Frist, siehe weiter oben) einen Standpunkt in der fortlaufenden Diskussion über die Aufsicht zu einzunehmen. Der EDSB vertritt — in dieser Diskussion — die folgende Sichtweise:

159. Zunächst sollte gewährleistet werden, dass alle Aufsichtsgremien die unabdingbaren Kriterien der Unabhängigkeit, Ressourcen und Durchsetzungsbefugnis erfüllen. Darüber hinaus sollte sichergestellt werden, dass die auf der EU-Ebene bestehenden Standpunkte und das Know-how berücksichtigt werden. Dies bedeutet, dass eine Zusammenarbeit nicht nur zwischen den nationalen Behörden, sondern auch mit der europäischen Datenschutzbehörde (aktuell dem EDSB) stattfinden sollte. Der EDSB hält es für erforderlich, einem Modell zu folgen, das diese Anforderungen erfüllt ([63]).

160. In den vergangenen Jahren wurde das Modell der „koordinierten Aufsicht" entwickelt. Dieses Aufsichtsmodell, das nun für Eurodac und teilweise im Zollinformationssystem angewendet wird, soll bald auf das Visa-Informationssystem (VIS) und die zweite Generation des Schengener Informationssystems (SIS II) ausgeweitet werden. Dieses Modell ist dreischichtig: (1) die Aufsicht auf der nationalen Ebene wird durch die Datenschutzbehörden gewährleistet; (2) die Aufsicht auf EU-Ebene wird durch den EDSB gewährleistet; (3) die Koordinierung wird durch regelmäßige, durch den EDSB einberufene Sitzungen gewährleistet,

([61]) Beispielsweise auf der Grundlage des jährlich veröffentlichten und regelmäßig aktualisierten Bestandsverzeichnisses der Gesetzgebungstätigkeiten, das auf der Website des EDSB zur Verfügung steht.

([62]) Nach Maßgabe der Verordnung (EG) Nr. 45/2001 ist der EDSB verpflichtet, mit diesen Einrichtungen zusammenzuarbeiten.

([63]) Für Eurojust sollte das Modell zudem berücksichtigen, dass die Datenschutzaufsicht der Unabhängigkeit der Justiz Rechnung trägt, sofern Eurojust Daten im Zusammenhang mit Strafverfahren verarbeitet.

wobei der EDSB als Sekretariat dieses Koordinierungmechanismus fungiert. Dieses Modell hat sich als erfolgreich und wirksam erwiesen und sollte künftig für andere Informationssysteme in Betracht gezogen werden.

C. WIE KANN DIE ANWENDUNG DER AKTUELLEN RAHMENREGELUNG VERBESSERT WERDEN?

11. Auf kurze Sicht

161. Während der Überprüfungsprozess weitergeführt wird, sollten Anstrengungen zur Gewährleistung der vollständigen und wirksamen Umsetzung der aktuellen Vorschriften unternommen werden. Diese Vorschriften werden bis zur Annahme der künftigen Rahmenregelung und ihrer Umsetzung in das nationale Recht der Mitgliedstaaten weiter anwendbar sein. Diesbezüglich können verschiedene Tätigkeitsfelder abgesteckt werden.

162. Zunächst sollte die Kommission fortfahren, die Einhaltung der Richtlinie 95/46/EG durch die Mitgliedstaaten zu überwachen und gegebenenfalls ihre Befugnisse im Rahmen von Artikel 258 AEUV wahrzunehmen. Kürzlich wurden aufgrund einer nicht korrekten Umsetzung von Artikel 28 der Richtlinie hinsichtlich der erforderlichen Unabhängigkeit der Datenschutzbehörden Vertragsverletzungsverfahren eingeleitet ([64]). In anderen Bereichen muss eine vollständige Einhaltung der Regeln ebenfalls überwacht und durchgesetzt werden ([65]). Der EDSB begrüßt folglich die Zusage in der Mitteilung der Kommission, eine aktive Vertragsverletzungsstrategie zu verfolgen. Die Kommission sollte überdies den strukturellen Dialog mit den Mitgliedstaaten über die Durchführung fortsetzen ([66]).

163. Zweitens muss die Durchsetzung auf nationaler Ebene unterstützt werden, um die praktische Anwendung der Datenschutzvorschriften auch mit Blick auf neue technologische Phänomene und globale Akteure zu gewährleisten. Die Datenschutzbehörden sollten von ihren Ermittlungs- und Sanktionsbefugnissen in vollem Umfang Gebrauch machen. Ebenso wichtig ist, dass die bestehenden Rechte der betroffenen Personen, insbesondere das Recht auf Auskunft, vollständig in die Praxis umgesetzt werden.

164. Drittens scheint eine stärkere Koordinierung der Durchsetzung auf kurze Sicht notwendig zu sein. Die Rolle der Artikel-29-Datenschutzgruppe und ihrer Dokumente zur Auslegung ist hier von entscheidender Bedeutung, aber auch die Datenschutzbehörden sollten ihr Möglichstes tun, um diese in die Praxis umzusetzen. Abweichende Ergebnisse bei EU-weiten oder globalen Fällen müssen vermieden werden und gemeinsame Vorgehensweisen sollten und können innerhalb der Datenschutzgruppe erzielt werden. EU-weite koordinierte Untersuchungen unter der Federführung der Artikel-29-Datenschutzgruppe können ebenfalls einen bedeutenden zusätzlichen Nutzen bringen.

165. Viertens sollten die Datenschutzgrundsätze vorausschauend in neue Verordnungen, die sich direkt oder indirekt auf den Datenschutz auswirken können, „eingebaut" werden. Auf EU-Ebene unternimmt der EDSB erhebliche Anstrengungen, um zu besseren europäischen Rechtsvorschriften beizutragen, und diese Anstrengungen müssen auch auf nationaler Ebene erfolgen. Die Datenschutzbehörden sollten aus diesem Grund in vollem Umfang von ihrer Beratungsbefugnis Gebrauch machen, um eine solche vorausschauende Vorgehenseise zu gewährleisten. Die Datenschutzbehörden und der EDSB können auch bei der Überwachung technologischer Entwicklungen eine vorausschauende Rolle übernehmen. Eine Überwachung ist wichtig, um sich abzeichnende Trends in einem frühen Stadium zu ermitteln, mögliche Auswirkungen auf den Datenschutz aufzuzeigen, datenschutzfreundliche Lösungen zu unterstützen und Interessengruppen weiter zu sensibilisieren.

166. Schließlich muss die künftige Zusammenarbeit zwischen den verschiedenen Akteuren auf internationaler Ebene aktiv verfolgt werden. Aus diesem Grund ist es wichtig, die internationalen Instrumente der Zusammenarbeit zu stärken. Initiativen wie die Madrider Standards und die fortlaufende Arbeit mit dem Europarat und der OECD verdienen uneingeschränkte Unterstützung. In diesem Zusammenhang ist es sehr positiv, dass die Kartellbehörde der Vereinigten Staaten nun in die Gruppe der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im Rahmen der internationalen Konferenz der Datenschutzbeauftragten eingetreten ist.

D. SCHLUSSFOLGERUNGEN

ALLGEMEINE BEMERKUNGEN

167. Der EDSB begrüßt die Mitteilung der Kommission im Allgemeinen, da er davon überzeugt ist, dass eine Überprüfung des aktuellen Rechtsrahmens für den Datenschutz erforderlich ist, um einen wirksamen Schutz in einer sich weiterentwickelnden und globalisierten Informationsgesellschaft zu gewährleisten.

168. Die Mitteilung legt die wesentlichen Probleme und Herausforderungen dar. Der EDSB teilt die Ansicht der Kommission, dass in der Zukunft ein starkes Datenschutzsystem benötigt wird, das auf dem Verständnis basiert, dass die bestehenden allgemeinen Datenschutzgrundsätze in einer Gesellschaft, die eine grundlegende Wandlungen durchmacht, immer noch Gültigkeit besitzen. Der EDSB teilt die in der Mitteilung vertretene Ansicht, dass die Herausforderungen gewaltig sind, und unterstreicht die Schlussfolgerung, dass die vorgeschlagenen Lösungen entsprechend ehrgeizig sein und die Wirksamkeit des Schutzes verstärken sollten. Aus diesem Grund fordert er eine ehrgeizigere Vorgehensweise im Hinblick auf verschiedene Punkte.

169. Der EDSB unterstützt die umfassende Herangehensweise an den Datenschutz. Er bedauert allerdings, dass in der Mitteilung bestimmte Bereiche, etwa die Datenverarbeitung durch Organe und Einrichtungen der EU, aus dem allgemeinen Rechtsakt ausgeklammert werden. Sollte

([64]) Siehe den weiter oben zitierten Fall C-518/07 und die Presseerklärung der Kommission vom 28. Oktober 2010 (IP/10/1430).

([65]) Die Kommission eröffnete ein Vertragsverletzungsverfahren gegen das Vereinigte Königreich aufgrund einer mutmaßlichen Verletzung verschiedener Datenschutzbestimmungen, einschließlich der notwendigen Vertraulichkeit elektronischer Kommunikation im Zusammenhang mit verhaltensorientierter Werbung. Siehe Presseerklärung der Kommission vom 9. April 2009 (IP/09/570).

([66]) Siehe den weiter oben zitierten ersten Bericht der Kommission über die Durchführung der Datenschutzrichtlinie, S. 26 ff.

die Kommission beschließen, diese Bereiche auszuklammern, fordert der EDSB die Kommission nachdrücklich auf, innerhalb kürzester Frist, jedoch vorzugsweise vor Ende 2011, einen Vorschlag für die EU-Ebene anzunehmen.

WESENTLICHE GESICHTSPUNKTE

170. Die Ausgangspunkte für den Überprüfungsprozess stellen sich für den EDSB folgendermaßen dar:

— Vorkehrungen zum Datenschutz müssen so weit wie möglich andere rechtmäßige Interessen (beispielsweise die europäische Wirtschaft, die Sicherheit von Einzelpersonen und die Rechenschaftspflicht von Regierungen) aktiv unterstützen, anstatt diese zu behindern.

— Die allgemeinen Grundsätze des Datenschutzes sollten und können nicht geändert werden.

— Eine weitere Harmonisierung sollte eines der wesentlichen Ziele der Überprüfung sein.

— Die Berücksichtigung der Grundrechte sollte im Zentrum des Überprüfungsprozesses stehen. Ein Grundrecht ist darauf ausgerichtet, die Bürger unter allen Umständen zu schützen.

— Der neue Rechtsakt muss den Bereich Polizei und Justiz einschließen.

— Der neue Rechtsakt muss so weit wie möglich auf eine technologisch neutrale Weise formuliert werden und auf die Schaffung langfristiger Rechtssicherheit abzielen.

ELEMENTE EINER NEUEN REGELUNG

Harmonisierung und Vereinfachung

171. Der EDSB begrüßt die in der Mitteilung ausgedrückte Bereitschaft, die Mittel für eine weitere Harmonisierung des Datenschutzes auf EU-Ebene zu prüfen. Der EDSB legt Bereiche fest, in denen eine künftige und bessere Harmonisierung dringend erforderlich ist: Begriffsbestimmungen, Gründe für die Datenverarbeitung, die Rechte der betroffenen Personen, internationale Übermittlungen und die Datenschutzbehörden.

172. Der EDSB empfiehlt, die folgenden Alternativen zur Vereinfachung und/oder Verringerung des Umfangs der Meldeanforderungen zu berücksichtigen:

— Beschränkung der Meldepflicht auf bestimmte Verarbeitungen, die bestimmte Risiken beinhalten.

— Eine einfache Verpflichtung zur Registrierung für die für die Verarbeitung Verantwortlichen (im Gegensatz zu einer umfassenden Registrierung sämtlicher Datenverarbeitungen).

— Die Einführung eines paneuropäischen Standard-Meldeformulars.

173. Nach Ansicht des EDSB ist eine Verordnung, ein einziger Rechtsakt, der in den Mitgliedstaaten direkt anwendbar ist, das wirksamste Mittel zum Schutz des Grundrechts auf Datenschutz und zur Erzielung einer weiteren Konvergenz des Binnenmarktes.

Stärkung der Rechte des Einzelnen

174. Der EDSB unterstützt die Mitteilung insofern, als diese die Stärkung der Rechte des Einzelnen fordert. Er unterbreitet die folgenden Empfehlungen:

— Ein Transparenzgrundsatz könnte rechtlich verankert werden. Allerdings ist es wichtiger, die bestehenden Bestimmungen zur Transparenz (wie die bestehenden Artikel 10 und 11 der Richtlinie 95/46/EG) zu stärken.

— Eine Bestimmung zur Meldung von Verletzungen des Schutzes personenbezogener Daten, mit der die in der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikation für bestimmte Anbieter enthaltene Verpflichtung auf alle für die Datenverarbeitung Verantwortlichen ausgeweitet wird, sollte in den allgemeinen Rechtsakt aufgenommen werden.

— Die Grenzen der Einwilligung sollten geklärt werden. Eine Ausweitung der Fälle, in denen eine ausdrückliche Einwilligung erforderlich ist, sollte ebenso wie die Annahme zusätzlicher Vorschriften für die Online-Umgebung in Erwägung gezogen werden.

— Zusätzliche Rechte wie die Datenübertragbarkeit und das Recht auf Vergessen sollten eingeführt werden, insbesondere für die im Internet erbrachten Dienstleistungen für die Informationsgesellschaft.

— Die Interessen von Kindern sollten mit einer Reihe zusätzlicher Bestimmungen, die sich insbesondere auf die Erhebung und Weiterverarbeitung der Daten von Kindern beziehen, besser geschützt werden.

— Kollektive Rechtsbehelfsverfahren bei Verletzung von Datenschutzvorschriften sollten in die EU-Rechtsvorschriften aufgenommen werden, um den hierzu befugten Einrichtungen die Möglichkeit zu verschaffen, Klagen im Namen von Gruppen oder Einzelpersonen einzureichen.

Stärkung der Verpflichtungen von Unternehmen/für die Verarbeitung Verantwortlichen

175. Die neue Rahmenregelung muss Anreize für die für die Datenverarbeitung Verantwortlichen enthalten, Maßnahmen zum Datenschutz vorausschauend in ihre Geschäftsprozesse aufzunehmen. Der EDSB schlägt die Aufnahme von allgemeinen Bestimmungen zur Rechenschaftspflicht und dem „eingebauten Datenschutz“ vor. Eine Bestimmung zu einem Zertifizierungssystem im Hinblick auf den Datenschutz sollte ebenfalls eingeführt werden.

Globalisierung und anwendbares Recht

176. Der EDSB unterstützt die zielgerichtete Arbeit, die im Rahmen der internationalen Konferenz der Beauftragten für den Datenschutz zur Entwicklung der sogenannten „Madrider Standards“ durchgeführt wurde, mit der Absicht, diese in ein verbindliches Instrument zu integrieren und möglicherweise eine regierungsübergreifende Konferenz einzusetzen. Der EDSB ruft die Kommission dazu auf, in enger Zusammenarbeit mit der OECD und dem Europarat konkrete Schritte in diese Richtung zu unternehmen.

177. Ein neuer Rechtsakt muss die Kriterien zur Festlegung des anwendbaren Rechts klären. Es sollte gewährleistet sein, dass außerhalb der EU-Grenzen verarbeitete Daten der EU-Rechtssprechung unterliegen, wo die Anwendung von EU-Recht gerechtfertigt ist. Hätte der Rechtsrahmen die Form einer Verordnung, bestünden identische Vorschriften in allen Mitgliedstaaten, und die Festlegung des anwendbaren Rechts (innerhalb der EU) wäre weniger bedeutsam.

178. Der EDSB unterstützt vorbehaltlos das Ziel, eine einheitlichere und kohärentere Vorgehensweise gegenüber Drittländern und internationalen Organisationen zu gewährleisten. Verbindliche unternehmensinterne Vorschriften sollten in den Rechtsakt aufgenommen werden.

Der Bereich Polizei und Justiz

179. Ein umfassender Rechtsakt, in den Polizei und Justiz einbezogen sind, kann konkreten Vorschriften Rechnung tragen, mit denen die Besonderheiten in diesem Sektor im Einklang mit der dem Vertrag von Lissabon angefügten Erklärung 21 gebührend berücksichtigt werden. Es müssen bestimmte Garantien eingesetzt werden, um die betroffenen Personen durch einen zusätzlichen Schutz in einem Bereich, in dem die Verarbeitung personenbezogener Daten eine naturgemäß einschneidendere Wirkung hat, zu entschädigen.

180. Der neue Rechtsrahmen sollte möglichst klar, einfach und kohärent sein. Eine Weiterverbreitung verschiedener Regelungen, die beispielsweise auf Europol, Eurojust, SIS und Prüm anwendbar sind, sollte vermieden werden. Der EDSB ist sich bewusst, dass eine Angleichung der Vorschriften aus den verschiedenen Systemen sorgfältig und schrittweise durchgeführt werden muss.

Datenschutzbehörden und die Zusammenarbeit zwischen Datenschutzbehörden

181. Der EDSB unterstützt uneingeschränkt das Ziel der Kommission, die Frage der Rechtsstellung der Datenschutzbehörden zu klären und ihre Unabhängigkeit, Ressourcen und Durchsetzungsbefugnisse zu stärken. Er empfiehlt:

— Verankerung des grundlegenden Konzepts der Unabhängigkeit der Datenschutzbehörden gemäß der Festlegung durch den Europäischen Gerichtshof im neuen Rechtsakt.

— Festlegung im Rechtsakt, dass die Datenschutzbehörden über ausreichende Ressourcen verfügen müssen.

— Harmonisierte Ermittlungs- und Sanktionsbefugnissen für die Behörden.

182. Der EDSB empfiehlt eine weitere Verbesserung der Funktionsweise der Artikel-29-Datenschutzgruppe, einschließlich ihrer Ausstattung und Unabhängigkeit. Die Datenschutzgruppe sollte ferner mit ausreichenden Ressourcen und einem verstärkten Sekretariat ausgestattet werden.

183. Der EDSB empfiehlt eine verstärkte Beraterrolle der Datenschutzgruppe durch die Einführung einer Verpflichtung für die Datenschutzbehörden und die Kommission, *den Stellungnahmen und gemeinsamen Standpunkten*, die von der Artikel-29-Datenschutzgruppe angenommen wurden, *weitestgehend Rechnung zu tragen*. Der EDSB befürwortet nicht, den Standpunkten der Artikel-29-Datenschutzgruppe Rechtsverbindlichkeit zu verleihen, insbesondere angesichts der Unabhängigkeit der einzelnen Datenschutzbehörden. Der EDSB empfiehlt, dass die Kommission konkrete Bestimmungen zur Verbesserung der Zusammenarbeit mit dem EDSB im Rahmen des neuen Rechtsakts einführt.

184. Der EDSB fordert die Kommission nachdrücklich auf, so schnell wie möglich Position zur Aufsicht über die EU-Einrichtungen und zu informationstechnischen Großsystemen zu beziehen, wobei zu berücksichtigen ist, dass alle Aufsichtsgremien die unabdingbaren Kriterien der Unabhängigkeit, ausreichender Ressourcen und Durchsetzungsbefugnisse erfüllen sollten und gewährleistet sein sollte, dass der EU-Standpunkt gut vertreten wird. Der EDSB unterstützt das Modell der „koordinierten Aufsicht".

Verbesserungen im Rahmen des gegenwärtigen Systems:

185. Der EDSB ermutigt die Kommission zu folgenden Maßnahmen:

— Die Kommission sollte fortfahren, die Einhaltung der Richtlinie 95/46/EG durch die Mitgliedstaaten zu überwachen und gegebenenfalls ihre Durchsetzungsbefugnisse im Rahmen von Artikel 258 AEUV wahrzunehmen.

— Unterstützung der Durchsetzung auf nationaler Ebene sowie der Koordinierung der Durchsetzung.

— Vorausschauender Einbau von Datenschutzgrundsätzen in neue Verordnungen, die sich direkt oder indirekt auf den Datenschutz auswirken können.

— Aktive Verfolgung einer weiteren Zusammenarbeit zwischen den verschiedenen Akteuren auf internationaler Ebene.

Geschehen zu Brüssel den 14. Januar 2011.

Peter HUSTINX

Europäischer Datenschutzbeauftragter