Artikel-29-Datenschutzgruppe

Arbeitsgruppe Polizei und Justiz

02356/09/DE
WP 168

Die Zukunft des Datenschutzes

Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten

Annahme am 1. Dezember 2009

Die Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.
Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Freiheit und Sicherheit, Direktion D (Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro LX-46 01/190.
Webseite: http://ec.europa.eu/ justice_home/fsj/privacy/index_de.htm

Die Arbeitsgruppe Polizei und Justiz wurde von der Konferenz der Datenschutzbehörden eingesetzt. Ihre Aufgabe ist es, die Entwicklungen im Bereich der Strafverfolgung zu beobachten und zu überprüfen, um so besser auf die wachsenden Herausforderungen beim Schutz personenbezogener Daten reagieren zu können.

Zusammenfassung

Am 9. Juli 2009 hat die Kommission ein Konsultationsverfahren zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, insbesondere angesichts neuer Technologien und angesichts der Globalisierung. Die Kommission erwartet Beiträge zu den Fragen, ob der aktuelle Rechtsrahmen den Herausforderungen gewachsen ist und welche zukünftigen Aktionen erforderlich sind, um die ermittelten Herausforderungen in Angriff zu nehmen. Das vorliegende Dokument enthält die gemeinsame Stellungnahme der Artikel-29-Arbeitsgruppe (WP29) und der Arbeitsgruppe Polizei und Justiz (WPPJ) zu diesem Konsultationsverfahren.

Dieser Beitrag stellt in erster Linie fest, dass die wichtigsten Grundsätze des Datenschutzes trotz der neuen Technologien und der Globalisierung nach wie vor gültig sind. Das Datenschutzniveau in der EU kann von einer besseren Anwendung der bestehenden Datenschutzgrundsätze profitieren. Das bedeutet nicht, dass keine Gesetzesänderungen erforderlich sind. Ganz im Gegenteil ist es sinnvoll, die Gelegenheit zu ergreifen, um:

- die Anwendung einiger Grundregeln und Grundsätze des Datenschutzes (wie Einwilligung und Transparenz) zu klären;
- dem Rechtsrahmen durch zusätzliche Grundsätze (wie z. B. „Privacy by Design“ und „Rechenschaftspflicht“) Neuerungen hinzuzufügen;
- die Wirksamkeit des Systems durch die Modernisierung von Bestimmungen der Richtlinie 95/46/EG zu stärken (z. B. durch eine Einschränkung der bürokratischen Hindernisse);
- die Grundsätze des Datenschutzes in einem umfassenden Rechtsrahmen zusammenzufassen, der auch bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Anwendung findet.

Kapitel 1 enthält eine Einleitung mit einem kurzen Überblick über den Hintergrund und den Kontext des Datenschutzes in der EU.

In Kapitel 2 wird die Einführung eines umfassenden Rechtsrahmens vorgeschlagen. Die Notwendigkeit spezieller Gesetze (*leges speciales*) wird erkannt, vorausgesetzt, sie passen zu dem Konzept eines umfassenden Rechtsrahmens und erfüllen die wichtigsten Grundsätze. Die wichtigsten Garantien und Grundsätze des Datenschutzes sollten auf die Datenverarbeitung in allen Sektoren Anwendung finden.

In den Kapiteln 3 und 4 werden die wichtigsten Herausforderungen an den Datenschutz diskutiert.

In Kapitel 3 zur Globalisierung wird festgestellt, dass der Datenschutz gemäß dem Gemeinschaftsrecht ein Grundrecht ist. Die EU und ihre Mitgliedstaaten sollten jedem dieses Grundrecht garantieren, insoweit es in ihre Zuständigkeit fällt. Natürliche Personen sollten die Möglichkeit haben, Schutz einzufordern, auch wenn ihre Daten außerhalb der EU verarbeitet werden. Deshalb ist die Kommission dazu aufgerufen, Initiativen zu einer weiteren Entwicklung der internationalen globalen Standards zum Schutz personenbezogener Daten zu ergreifen. Des Weiteren ist es erforderlich, das Konzept der Angemessenheit zu überdenken. Außerdem können internationale

Abkommen angemessene Instrumente für den Schutz personenbezogener Daten in einem globalen Kontext darstellen. Der zukünftige Rechtsrahmen könnte die Voraussetzungen für Abkommen mit Drittländern nennen. Die Verarbeitung von Daten außerhalb der EU kann auch durch verbindliche unternehmensinterne Datenschutzregelungen (BCR) geschützt werden. In den neuen Rechtsrahmen sollte eine gestärkte Regelung zu den BCR aufgenommen werden. Die WP29 plant, die Kommission im kommenden Jahr über das anzuwendende Recht zu beraten.

In Kapitel 4 über die technologischen Änderungen wird festgestellt, dass die Richtlinie 95/46/EG aufgrund ihrer soliden und technologisch neutralen Grundsätze und Konzepte dem Zustrom technologischer Änderungen gut standgehalten hat. Diese Grundsätze und Konzepte bleiben in der heutigen vernetzten Welt gleichermaßen maßgeblich, gültig und anwendbar. Die technologischen Änderungen haben die Risiken für die Privatsphäre des Einzelnen und für den Datenschutz erhöht. Als Gegengewicht zu diesen Risiken sollte der Grundsatz „Privacy by Design“ in den neuen Rechtsrahmen eingebracht werden: Bei der Planung von Informations- und Kommunikationstechnologien sollten der Privatsphäre und dem Datenschutz Rechnung getragen werden. Die Anwendung dieses Grundsatzes würde die Notwendigkeit zur Einführung von Technologien zum Schutz der Privatsphäre, von „Privacy by Default“-Einstellungen und der erforderlichen Tools betonen, damit die Nutzer ihre personenbezogenen Daten besser schützen können. Der Grundsatz „Privacy by Design“ sollte also nicht nur für die für die Datenverarbeitung Verantwortlichen bindend sein, sondern auch für die Entwickler und Hersteller der Technologien. Darüber hinaus sollten soweit erforderlich in Bezug auf bestimmte technologische Kontexte Verordnungen erlassen werden, welche die Verankerung von Grundsätzen des Datenschutzes und der Privatsphäre vorschreiben.

In den Kapiteln 5, 6 und 7 wird dargelegt, dass diese wichtigsten Herausforderungen an den Datenschutz eine stärkere Rolle der verschiedenen Akteure erfordern.

Die Änderungen im Verhalten und in der Rolle der betroffenen Personen sowie die Erfahrungen mit der Richtlinie 95/46/EG machen eine stärkere Position der Betroffenen in dem Datenschutzrechtsrahmen erforderlich. Kapitel 5 enthält Vorschläge, wie die Betroffenen gestärkt werden können, so dass sie eine aktivere Rolle spielen. Dies erfordert unter anderem eine Verbesserung des Rechtsschutzes: mehr Möglichkeiten für die Betroffenen, ihre Rechte auszuüben und geltend zu machen, einschließlich der Einführung von Sammelklagen; einfacher zugängliche, wirkungsvollere und kostengünstigere Beschwerdeverfahren sowie alternative Verfahren zur Streitbeilegung. Darüber hinaus sollte der neue Rechtsrahmen alternative Lösungen zur Erhöhung der Transparenz bereitstellen sowie die generelle Meldung von Datenschutzverletzungen einführen. Die „Einwilligung“ ist eine wichtige Grundlage für die Verarbeitung, die dem Betroffenen unter bestimmten Umständen eine stärkere Position geben könnte. Derzeit wird die Einwilligung jedoch häufig fälschlicherweise als maßgeblicher Grund für die Verarbeitung angegeben, da die Voraussetzungen für die Einwilligung nicht vollumfänglich erfüllt werden. Deshalb sollten die Voraussetzungen für eine „Einwilligung“ in dem neuen Rechtsrahmen genauer festgelegt werden. Außerdem muss die Harmonisierung verbessert werden, da die Stärkung der Rolle des Betroffenen derzeit durch eine fehlende Harmonisierung der innerstaatlichen Gesetze, mit denen die Richtlinie 95/46/EG umgesetzt wird, untergraben wird. Ein weiteres Problem ist die Rolle der Betroffenen im Internet. Angesichts des neuen Rechtsrahmens sollte hier eine weitere Klärung erfolgen. Jedenfalls sollte jeder, der Privatpersonen Dienste anbietet,

dazu verpflichtet sein, für die Sicherheit und in angemessenem Rahmen für die Vertraulichkeit der durch die Nutzer hochgeladenen Informationen bestimmte Garantien zu geben, unabhängig davon, ob der Kunde für die Datenverarbeitung verantwortlich ist oder nicht.

Kapitel 6 zielt auf eine Stärkung der Verantwortung der für die Datenverarbeitung Verantwortlichen ab. Der Datenschutz sollte zuallererst in Organisationen verankert werden. Er sollte Teil der gemeinsamen Werte und Praktiken von Organisationen werden, und es sollten ausdrücklich für den Datenschutz Verantwortliche benannt werden. Dies wird auch die nationalen Datenschutzbehörden bei ihren Kontroll- und Durchsetzungsaufgaben unterstützen und so die Wirksamkeit des Schutzes der Privatsphäre stärken. Die für die Datenverarbeitung Verantwortlichen müssen verschiedene proaktive und reaktive Maßnahmen ergreifen, die in diesem Kapitel genannt werden. Darüber hinaus wäre es angemessen, in den umfassenden Rechtsrahmen den Grundsatz der Rechenschaftspflicht einzuführen, so dass die für die Datenverarbeitung Verantwortlichen zur Durchführung der Maßnahmen verpflichtet sind, mit denen sichergestellt werden kann, dass die wesentlichen Grundsätze und Verpflichtungen gemäß der geltenden Richtlinie bei der Bearbeitung der personenbezogenen Daten beachtet werden. Die für die Datenverarbeitung Verantwortlichen sollten auch dazu verpflichtet werden, die erforderlichen internen Mechanismen einzuführen, mit denen gegenüber externen Stellen, einschließlich der Datenschutzbehörde, die Einhaltung der Grundsätze und Verpflichtungen nachgewiesen werden kann. Die Meldungen von Datenverarbeitungsoperationen an nationale Datenschutzbehörden könnten vereinfacht oder eingeschränkt werden. Es sollte untersucht werden, ob und in welchem Ausmaß die Meldungen auf diejenigen Fälle beschränkt werden könnten, in denen eine ernstzunehmende Gefahr für den Datenschutz besteht. Dies würde den Datenschutzbehörden die Möglichkeit geben, selektiver vorzugehen und ihre Anstrengungen auf die vorgenannten Fälle zu konzentrieren sowie auf Wege zur Rationalisierung der Meldungen.

Kapitel 7a sieht eine stärkere und eindeutigere Rolle der nationalen Datenschutzbehörden vor. Derzeit bestehen große Unterschiede zwischen den Mitgliedstaaten, unter anderem bezüglich der Position, den Ressourcen und den Befugnissen der einzelnen Datenschutzbehörden. Die neuen Herausforderungen an den Datenschutz machen eine strikte, einheitlichere und effektive Überwachung durch die Datenschutzbehörden erforderlich. Der neue Rechtsrahmen sollte folglich hochrangig und richtunggebend einheitliche Standards in Bezug auf Unabhängigkeit und effektive Befugnisse garantieren sowie den Datenschutzbehörden eine beratende Rolle im Gesetzgebungsverfahren geben sowie die Möglichkeit, die Geschäftsordnung selbst festzulegen, insbesondere durch das Setzen von Prioritäten bei der Behandlung von Beschwerden.

In Kapitel 7b wird dargelegt, wie die Zusammenarbeit zwischen den Datenschutzbehörden verbessert werden sollte. Die europäischen Datenschutzbehörden sind in der WP29 zusammengefasst. Als erste Priorität sollte sichergestellt werden, dass alle Fragen bezüglich der Verarbeitung personenbezogener Daten insbesondere im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in die Maßnahmen der aktuellen WP29 eingeschlossen werden. Darüber hinaus sollten die Arbeitsmethoden der WP29 weiter verbessert werden. Soweit erforderlich, sollten die Mitglieder der WP29 zur Umsetzung der Ansichten der WP29 in den jeweiligen Mitgliedstaaten in die Praxis aufgefordert werden. Die Beziehungen zwischen der WP29 und der Kommission, die die Sekretariatsgeschäfte für die WP29 wahrnimmt, können

durch das Festlegen der wichtigsten Rollen der beiden Akteure in einem Memorandum of Understanding weiter verbessert werden. Die WP29 wird im Jahr 2010 mit der Kommission Beratungen zu diesem Memorandum aufnehmen.

Kapitel 8 schließlich beschäftigt sich mit den Datenschutzherausforderungen im Bereich der Strafverfolgung, die ein ganz spezielles Problemfeld darstellen. Der Kontext im Bereich Strafverfolgung hat sich in der EU mit dem Inkrafttreten des Vertrags von Lissabon geändert. Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, kann als erster Schritt zu einem allgemeinen Rechtsrahmen in der ehemaligen dritten Säule angesehen werden. Dieser Schritt ist jedoch noch lange nicht abgeschlossen. In den letzten Jahren gab es einen dramatischen Anstieg bei der Speicherung und dem Austausch personenbezogener Daten in Bezug auf die Tätigkeiten im Polizei- und Justizbereich. Denn um den neuen Bedrohungen entgegenzutreten, die aus dem Terrorismus und dem organisierten Verbrechen entstanden sind, gibt es - gefördert durch die technologischen Entwicklungen - einen wachsenden Bedarf an der Nutzung dieser Daten. Vor diesem Hintergrund sind die Herausforderungen an den Datenschutz immens und sollten in dem zukünftigen Rechtsrahmen angesprochen werden. Kapitel 8 legt die Bedingungen für die Rechtsetzung und Politikgestaltung in Bezug auf den Datenschutz im Bereich der Strafverfolgung dar: eine einheitliche Strategie als Grundlage des Informationsaustauschs; regelmäßige Bewertung der bestehenden Maßnahmen, der Rechtsinstrumente und ihrer Anwendung; Transparenz und Auskunfts- und Berichtigungsrechte im grenzüberschreitenden Kontext; Transparenz und demokratische Kontrolle im Gesetzgebungsverfahren; die Architektur der Systeme für die Speicherung und den Austausch der personenbezogenen Daten; ein eindeutiger Rechtsrahmen als Grundlage für die Beziehungen mit Drittländern, der für alle Parteien bindend ist und auf dem Konzept der Angemessenheit basiert; besondere Aufmerksamkeit auf die groß angelegten Informationssysteme in der EU; richtiges Herangehen an eine unabhängige Kontrolle, an die justizielle Aufsicht und an die Rechtsmittel; Stärken der Zusammenarbeit zwischen den Datenschutzbehörden.

1. Einleitung

Die Konsultation

1. Am 9. Juli 2009 hat die Kommission ein Konsultationsverfahren zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, insbesondere angesichts neuer Technologien und angesichts der Globalisierung. Die Kommission erwartet Beiträge zu den Fragen, ob der aktuelle Rechtsrahmen den Herausforderungen gewachsen ist und welche zukünftigen Aktionen erforderlich sind, um die ermittelten Herausforderungen in Angriff zu nehmen.

2. Dieses Papier enthält die gemeinsame Stellungnahme der Artikel-29-Arbeitsgruppe (WP29) und der Arbeitsgruppe Polizei und Justiz (WPPJ) zu diesem Konsultationsverfahren.

Hintergrund und Kontext

3. Das Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108)[1] kann als erster europäischer Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten angesehen werden. Das Recht auf Datenschutz ist eng verbunden mit dem Anspruch auf Achtung des Privatlebens gemäß Artikel 8 der Europäischen Menschenrechtskonvention, ist jedoch nicht identisch mit diesem. Das Recht auf Datenschutz wird in Artikel 8 der Charta der Grundrechte der Europäischen Union als eigenständiges Grundrecht anerkannt.

4. Die Grundsätze des Übereinkommens 108 wurden in der Richtlinie 95/46/EG[2] weiterentwickelt, die den Grundbaustein des Datenschutzrechts in der EU bildet. Das hauptsächliche Ziel des Konsultationsverfahrens der Kommission ist die (zukünftige) Wirksamkeit der Richtlinie. Weitere Rechtsakte der EU für den Datenschutz sind die Verordnung (EG) Nr. 45/2001[3], anwendbar bei der Datenverarbeitung durch Organe und Einrichtungen der EU, Richtlinie 2002/58/EC[4] über die Privatsphäre und die elektronische Kommunikation und Rahmenbeschluss 2008/977/JI[5] über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.

5. Mit dem Vertrag von Lissabon hat der Datenschutz signifikant an Bedeutung gewonnen. Es wurde nicht nur die EU-Grundrechtecharta bindend, sondern es wurde auch Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) als neue Rechtsgrundlage für den Datenschutz eingeführt, die bei jeglicher Verarbeitung personenbezogener Daten im privaten und im öffentlichen Bereich anzuwenden ist sowie bei der Verarbeitung von Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit und bei der gemeinsamen Außen- und Sicherheitspolitik. Artikel 16 gibt dem Datenschutz neue Impulse.

6. In diesem Zusammenhang muss auch das „Stockholmer Programm" erwähnt werden. Dieses Mehrjahresprogramm der EU widmet dem Datenschutz und damit dem Schutz der Bürger in einem Raum der Freiheit, der Sicherheit und des Rechts viel Aufmerksamkeit.[6]

---

1 STE Nr. 108, 28.1.1981.

2 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, ABl. 1995, L 281, S. 31.

3 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, ABl. 2001, L 8, S. 1.

4 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002, L 201, S. 37, in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung.

5 Rahmenbeschluss 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008, L 350, S. 60, der bis zum 27. November 2010 in innerstaatliches Recht umgesetzt sein muss.

6 Das Stockholmer Programm: ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, durch den Europäischen Rat im Dezember 2009 anzunehmen.

Hauptaussage

7. Das Konsultationsverfahren der Kommission wird angesichts der wichtigen neuen Herausforderungen durch die neuen Technologien und durch die Globalisierung sowie angesichts des Vertrags von Lissabon zum passenden Zeitpunkt durchgeführt.

8. In erster Linie ist festzustellen, dass die wichtigsten Grundsätze des Datenschutzes trotz dieser wichtigen Herausforderungen nach wie vor gültig sind. Das Datenschutzniveau in der EU kann von einer besseren Anwendung der bestehenden Datenschutzgrundsätze profitieren. Das bedeutet nicht, dass keine Gesetzesänderungen erforderlich sind. Ganz im Gegenteil ist es sinnvoll, die Gelegenheit zu ergreifen, um:

   - die Anwendung einiger Grundregeln und Grundsätze des Datenschutzes (wie Einwilligung und Transparenz) zu klären;
   - dem Rechtsrahmen durch zusätzliche Grundsätze (wie z. B. „Privacy by Design" und „Rechenschaftspflicht") Neuerungen hinzuzufügen;
   - die Wirksamkeit des Systems durch die Modernisierung von Bestimmungen der Richtlinie 95/46/EG zu stärken (z. B. durch eine Einschränkung der bürokratischen Hindernisse);
   - die Grundsätze des Datenschutzes in einem umfassenden Rechtsrahmen zusammenzufassen, der auch bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Anwendung findet.

2. Ein umfassender Rechtsrahmen

Der aktuelle Rechtsrahmen

9. Der Datenschutz wurde als binnenmarktbezogenes Thema in den Rechtsrahmen der Europäischen Union eingebracht. Die Richtlinie 95/46/EG basiert auf Artikel 95 EG-Vertrag. Die Richtlinie verfolgt zwei Zwecke. Für das Errichten und das Funktionieren eines Binnenmarkts müssen personenbezogene Daten frei von einem Mitgliedstaat in einen anderen übertragen werden können, während gleichzeitig ein hohes Schutzniveau in Bezug auf die Grundrechte der natürlichen Personen gewährleistet sein sollte.

10. Richtlinie 95/46/EG ist als allgemeiner Rechtsrahmen gedacht, der für bestimmte Sektoren durch besondere Regelungen zum Datenschutz ergänzt werden kann. Bis jetzt wurde eine einzige Sonderregelung angenommen, nämlich im Bereich des Datenschutzes bei der elektronischen Kommunikation (derzeit Richtlinie 2002/58/EG). Außerdem enthalten einige sektorbezogene Rechtsvorschriften besondere Bestimmungen zur Verarbeitung personenbezogener Daten ([7]zur Geldwäsche, Zollvorschriften oder Vorschriften zu VIS, EURODAC oder SIS II)

11. Die Anwendung von Artikel 95 EG-Vertrag hat sich auf den Anwendungsbereich der Richtlinie 95/46/EG ausgewirkt. Obwohl die Richtlinie als allgemeiner Rechtsrahmen für den Datenschutz gedacht war und in vielen Aspekten auch als

[7] Z. B. Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. 2005, L 309, S. 15 und verschiedene Rechtsinstrumente für die groß angelegten Informationssysteme SIS, VIS und EURODAC.

solcher funktioniert, deckt sie weder die Datenverarbeitung durch Einrichtungen der Gemeinschaft ab, noch Verarbeitungen, die außerhalb des Bereichs der ehemals ersten Säule (hauptsächlich die ehemalige dritte Säule) fallen. Für die Verarbeitung durch Einrichtungen der Gemeinschaft (insofern sie sich innerhalb der ersten Säule bewegen) wurde die Verordnung 45/2001 angenommen, die der Richtlinie 95/46/EG in großen Abschnitten ähnelt. Die derzeitige Situation in Bezug auf die ehemals dritte Säule kann als Stückwerk von Datenschutzregelungen beschrieben werden, die in unterschiedlichen Situationen anzuwenden sind. Einige Unterschiede zwischen diesen Regelungen haben ihren Ursprung in den Besonderheiten des abgedeckten Bereichs, andere sind lediglich die Folgen der unterschiedlichen gesetzlichen Hintergründe. Der Rahmenbeschluss 2008/977/JI kann als erster Schritt zu einem allgemeineren Rechtsrahmen gesehen werden.

12. Die Situation ist insbesondere für die dritte Säule nicht zufriedenstellend:

- Der Datenschutz wird inzwischen in zunehmendem Maße als allgemeines Anliegen der Europäischen Union erkannt und ist nicht mehr zwangsläufig ein rein binnenmarktbezogenes Thema. Dies zeigt sich z. B. in Artikel 8 der Charta der Grundrechte der Europäischen Union.
- In den vergangenen Jahren und sicherlich nach den Terroranschlägen in den USA vom 11.9.2001 wurde der Austausch personenbezogener Daten unter den Mitgliedstaaten ein wesentlicher Bestandteil der polizeilichen und justiziellen Zusammenarbeit, der natürlich einen angemessenen Schutz erforderlich macht.
- Die ehemalige Aufteilung zwischen den Säulen spiegelt nicht die Realität des Datenschutzes wider, in der die personenbezogenen Daten in säulenübergreifenden Situationen genutzt werden. Dies wird durch die Entscheidungen des Europäischen Gerichtshofs zu den PNR und zu der Vorratsdatenspeicherung an Fällen gezeigt, in denen Daten, die ursprünglich in einem Wirtschaftskontext erhoben wurden, für die Strafverfolgung genutzt wurden.

Die Notwendigkeit eines neuen Rechtsrahmens

13. Die Unzulänglichkeiten des aktuellen Systems erfordern das Nachdenken über „einen umfassenden und einheitlichen Rechtsrahmen zum Datenschutz, der für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt".[8] Der Vertrag von Lissabon sieht eine neue horizontale Herangehensweise an den Datenschutz und den Schutz der Privatsphäre vor und stellt die erforderliche Rechtsgrundlage (Art. 16 AEUV)[9] bereit, um die bestehenden Unterschiede und Abweichungen abzuschaffen, die einen nahtlosen, einheitlichen und wirkungsvollen Schutz aller natürlichen Personen beeinträchtigen.

14. Die wichtigsten Garantien und Grundsätze sollten auf die Datenverarbeitung in allen Sektoren angewendet werden und ein ganzheitliches Vorgehen sowie einen nahtlosen, einheitlichen und wirkungsvollen Schutz sicherstellen.

---

[8] Wortlaut der Kommission in KOM 262 endgültig.

[9] Artikel 16 AEUV erstreckt sich – insoweit als die Einrichtungen der Gemeinschaft personenbezogene Daten verarbeiten - nicht nur auf die dritte, sondern auch auf die zweite Säule (gemeinsame Außen- und Sicherheitspolitik). Artikel 39 EU-Vertrag sorgt für eine besondere Rechtsgrundlage für die Datenverarbeitung in der zweiten Säule durch die Mitgliedstaaten. Das ist z. B. wichtig in Bezug auf die Terroristenlisten, die durch die EU und die Mitgliedstaaten erstellt wurden. Dieser Punkt wird in dem vorliegenden Kapitel jedoch nicht näher angesprochen.

15. Richtlinie 95/46/EG sollte als Richtschnur für einen umfassenden Rechtsrahmen dienen, dessen Hauptziele Wirksamkeit und ein wirkungsvoller Schutz des Einzelnen sind. Die bestehenden Grundsätze des Datenschutzes müssen bestätigt und mit Maßnahmen ergänzt werden, um diese Grundsätze auf eine wirkungsvollere Weise zu erfüllen (und um einen wirkungsvolleren Schutz der personenbezogenen Daten der Bürger sicherzustellen).

16. Die wichtigsten Grundsätze des Datenschutzes sollten das Rückgrat eines umfassenden Rechtsrahmens sein: Schlüsselbegriffe (wer/für die Datenverarbeitung Verantwortlicher – was/personenbezogene Daten) und Grundsätze sollten bestätigt werden, darunter insbesondere die Grundsätze der Rechtmäßigkeit, Billigkeit, Verhältnismäßigkeit, Zweckbindung und Transparenz, die Rechte der betroffenen Personen sowie eine unabhängige Kontrolle durch die Behörden. Das Überdenken des Rechtsrahmens ist also auch eine Gelegenheit zur Klärung der Anwendung einiger Kernkonzepte wie:

    - Einwilligung: Unübersichtlichkeit zwischen Opt-in und Opt-out sollte vermieden werden sowie die Verwendung der Einwilligung in Situationen, in denen sie nicht die angemessene Rechtsgrundlage darstellt (siehe auch Kapitel 5);
    - Transparenz: Sie ist eine Voraussetzung für eine faire Verarbeitung. Es muss klar sein, dass Transparenz nicht unbedingt zur Einwilligung führt, aber eine Voraussetzung für eine gültige Einwilligung und die Ausübung der Rechte der Betroffenen ist (siehe auch Kapitel 5).

    Das Ziel sollte sein, den Datenschutz auf internationaler Ebene im Einklang mit den in der Richtlinie 95/46/EG niedergelegten Grundsätzen und Rechten zu verbessern, während gleichzeitig das aktuelle Schutzniveau aufrechterhalten wird (siehe auch Kapitel 3).

17. Die Annahme eines umfassenden Rechtsrahmens würde auch einige nützliche Erneuerungen der geltenden Bestimmungen ermöglichen. Dies könnte auch die Einführung des allgemeinen Grundsatzes „Privacy by Design“ als Ausweitung der geltenden Bestimmungen zu den organisatorischen und technischen Sicherheitsmaßnahmen (siehe auch Kapitel 4) bedeuten und des allgemeinen Grundsatzes der Rechenschaftspflicht (siehe auch Kapitel 6).

Die Architektur eines umfassenden Rechtsrahmens

18. Ein umfassender Rechtsrahmen – gemäß dem Vertrag von Lissabon basierend auf einer einzigen Rechtsgrundlage – bedeutet nicht unbedingt, dass es innerhalb des Geltungsbereichs des allgemeinen Rechtsrahmens keinen Raum für Flexibilität und Unterschiede zwischen den Sektoren und den Mitgliedstaaten gibt. Spezielle Gesetze (*leges speciales*) könnten als Ergänzung dienen und das Schutzniveau verbessern, vorausgesetzt, dass sie zu dem Konzept eines umfassenden Rechtsrahmens passen und die vorgenannten wichtigsten Grundsätze erfüllen.

19. Es könnten zusätzliche sektorbezogene Vorschriften und Sondervorschriften vorgesehen werden, so z. B. in Bezug auf:

- bestimmte Sektoren, wie z. B. das Gesundheitswesen, die Beschäftigung oder intelligente Verkehrssysteme;
- Privacy Tools und Leistungen, wie z. B. Gütesiegel und Audits (siehe auch Kapitel 4 und 6);
- Sicherheitsverletzungen (als Ergänzung des Grundsatzes der Sicherheit; siehe auch Kapitel 5 und 6);
- polizeiliche und justizielle Zusammenarbeit, wie sie ausdrücklich in der Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon vorgesehen ist (siehe auch Kapitel 8);
- innerstaatliche Sicherheitspolitik, wie ausdrücklich vorgesehen in der Erklärung Nr. 20 im Anhang zum Vertrag von Lissabon.

20. Es könnten zusätzliche innerstaatliche Verordnungen ins Auge gefasst werden, die den kulturellen Unterschieden und der innerstaatlichen Organisation der Mitgliedstaaten Rechnung tragen, vorausgesetzt, sie beeinträchtigen die Harmonisierung nicht, die in einer Europäischen Union ohne Binnengrenzen benötigt wird.

21. Als Teil eines eindeutigen und unmissverständlichen Rechtsrahmens wird eine weitere Harmonisierung benötigt. Dies schließt jedoch nicht aus, dass ein gewisses Maß an Flexibilität zusätzlichen Wert haben kann. Dies wird derzeit unter der Richtlinie 95/46/EG anerkannt, wenn dies z. B. aufgrund von kulturellen Unterschieden erforderlich ist. Es könnte auch Raum gelassen werden für innerstaatliches Recht, um die Zuweisung der Verantwortlichkeiten und die Anerkennung der unterschiedlichen Rollen des öffentlichen und des privaten Sektors festzulegen.

3. Globalisierung

Kontext und derzeitiger Rechtsrahmen

22. Im EU-Recht ist der Datenschutz ein Grundrecht, das gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union geschützt wird (siehe auch Kapitel 1). In anderen Teilen der Welt ist die Notwendigkeit des Datenschutzes weitgehend anerkannt, dieser hat aber nicht unbedingt den Status eines Grundrechts.

23. Die EU und die Mitgliedstaaten sollten jedem dieses Grundrecht garantieren, sofern sie zuständig sind. In einer globalisierten Welt bedeutet das, dass natürliche Personen auch dann Schutz fordern können, wenn ihre Daten außerhalb der Europäischen Union verarbeitet werden.

24. Richtlinie 95/46/EG behandelt diesen Schutzbedarf in Artikel 4. Die Richtlinie ist überall bei der Datenverarbeitung anzuwenden und folglich auch außerhalb der EU[10] (a) wenn der für die Datenverarbeitung Zuständige seinen Sitz in der EU hat und (b) wenn der für die Datenverarbeitung Zuständige seinen Sitz außerhalb der EU hat, aber Ausrüstung innerhalb der EU nutzt.

25. Darüber hinaus enthalten Artikel 25 und 26 der Richtlinie 95/46/EG eine Sonderregelung für die Übermittlung personenbezogener Daten an Drittländer. Die

[10] In diesem Kontext versteht sich EU einschließlich der EFTA-Länder.

Grundregel von Artikel 25 sieht vor, dass die Übermittlung nur an solche Drittländer zulässig ist, die ein angemessenes Schutzniveau gewährleisten. Artikel 26 sieht eine Reihe von Ausnahmen zu dieser Vorschrift vor. Bekannte Konzepte wie die verbindlichen Unternehmensregelungen (BCR) und Standardvertragsklauseln setzen diese Vorschrift um.

Anzuwendendes Recht

26. Der genaue Geltungsbereich der Richtlinie 95/46/EG ist jedoch nicht ausreichend klar. Es ist nicht immer eindeutig, ob EG-Recht anzuwenden ist, welches Recht der Mitgliedstaaten anzuwenden ist und welche Rechtsvorschrift(en) im Falle mehrerer Niederlassungen eines multinationalen Unternehmens in verschiedenen Mitgliedstaaten anzuwenden wäre(n). Artikel 4 der Richtlinie, der festlegt, wann die Richtlinie in Bezug auf die Datenverarbeitung anzuwenden ist, lässt hier Raum für unterschiedliche Auslegungen.

27. Darüber hinaus gibt es Situationen, die außerhalb des Anwendungsbereichs der Richtlinie liegen. Das ist der Fall, wenn ein nicht in der EU niedergelassener für die Datenverarbeitung Verantwortlicher Daten von EU-Bürgern verarbeitet und das zur Erhebung und Weiterverarbeitung von personenbezogenen Daten führt. Das ist z. B. bei Online-Verkäufern und dergleichen der Fall, die bestimmte Werbungen mit Lokalkolorit verwenden oder Webseiten, die sich direkt an EU-Bürger wenden (indem sie die Landessprache verwenden usw.). Wenn sie dies tun, ohne technisches Gerät in der EU zu verwenden, findet die Richtlinie 95/46/EG keine Anwendung.

28. Derzeit schreibt die WP29 eine Stellungnahme zu dem Konzept des anzuwendenden Rechts. Die WP29 plant, die Europäische Kommission im kommenden Jahr zu dieser Frage zu beraten. Dieser Rat könnte weitere Empfehlungen für den zukünftigen Rechtsrahmen enthalten.

Internationale Normen und die Madrid-Resolution

29. Weltweite Normen zum Datenschutz werden unverzichtbar. Weltweite Normen würden auch die grenzüberschreitenden Datenströme erleichtern, die aufgrund der Globalisierung eher zur Regel werden, statt eine Ausnahme zu sein. Solange keine weltweiten Standards existieren, bleibt die Diversität bestehen. Grenzüberschreitende Datenströme müssen erleichtert werden, während gleichzeitig ein hohes Schutzniveau für die personenbezogenen Daten sichergestellt wird, wenn diese in Drittländer übermittelt und dort verarbeitet werden.

30. Die “Madrid-Resolution”, ein konzertierter Vorschlag zu internationalen Normen für den Schutz der Privatsphäre, der am 6. November 2009 durch die Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre angenommen wurde, verdient Unterstützung. Der konzertierte Vorschlag enthält den Entwurf für eine weltweite Norm und bündelt alle möglichen Ansätze für den Schutz personenbezogener Daten und der Privatsphäre, wobei er die Rechtsprechung von fünf Kontinenten integriert. Er umfasst eine Reihe von Grundsätzen, Rechten und Verpflichtungen, die die Grundlage für den Datenschutz in allen Rechtssystemen in der ganzen Welt sein sollten und demonstriert, dass weltweite Normen, die ein angemessenes Schutzniveau bieten, zur gegebenen Zeit möglich sind.

31. Die Kommission wird dazu aufgerufen:

- Initiativen für die weitere Entwicklung internationaler globaler Normen bezüglich des Schutzes personenbezogener Daten mit der Absicht zu ergreifen, einen internationalen Rechtsrahmen für den Datenschutz zu fördern und folglich den grenzüberschreitenden Datenstrom zu erleichtern, während gleichzeitig ein angemessenes Schutzniveau der Betroffenen gewährleistet wird. Diese Initiativen sollten eine Prüfung der Durchführbarkeit eines bindenden internationalen Rechtsrahmens umfassen.
- in Ermangelung von globalen Normen die Entwicklung von Rechtsvorschriften zum Datenschutz, die ein angemessenes Schutzniveau bieten, sowie die Gründung unabhängiger Datenschutzbehörden in Ländern, die nicht der Europäischen Union angehören, zu fördern. Die wichtigsten Datenschutzgrundsätze, so wie sie in der „Madrid-Resolution" niedergelegt wurden, sollten die allgemeine Grundlage dieser Rechtsvorschriften bilden.

In dem zukünftigen Rechtsrahmen sollten diese besonderen Aufgaben der Kommission aufgeführt werden.

Verbesserung der Entscheidungen zur Angemessenheit

32. In dem globalisierten Umfeld finden immer mehr Verarbeitungsvorgänge personenbezogener Daten statt. Es wird immer wichtiger, sicherzustellen, dass die Ströme personenbezogener Daten frei fließen und gleichzeitig das Schutzniveau der Rechte des Einzelnen zu garantieren. Deshalb ist es erforderlich, den Prozess der Angemessenheit umzugestalten:

    - Präzisere Definition der Kriterien zur rechtlichen Verankerung des Grundsatzes der "Angemessenheit". Hierbei sollte gebührende Aufmerksamkeit auf das Vorgehen der WP29[11] gerichtet werden sowie auf die verschiedenen anderen Ansätze zum Datenschutz in der ganzen Welt und insbesondere auf die Rechte und Grundsätze, die im konzertierten Vorschlag zu Internationalen Normen für den Schutz der Privatsphäre niedergelegt wurden;
    - Rationalisieren der Analyseverfahren in Bezug auf die Rechtssysteme von Drittländern, damit mehr Entscheidungen zur Angemessenheit des Schutzniveaus getroffen werden können.

Der zukünftige Rechtsrahmen sollte diese Themen näher darlegen.

Internationale Abkommen

33. Die Aktivitäten der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten wurden zur Kenntnis genommen. Diese Aktivitäten könnten zu einem transatlantischen Abkommen mit gemeinsamen Grundsätzen zur Privatsphäre und zum Datenschutz führen, das bei einem Informationsaustausch mit den Vereinigten Staaten im Kampf gegen den Terrorismus und die transnationale Schwerkriminalität anzuwenden wäre.[12]

---

[11] Siehe insbesondere Arbeitspapier 12 der WP 29: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, angenommen am 24. Juli 1998.

[12] In dieser Hinsicht bleibt das transatlantische Problem hinsichtlich des Rechtsschutzes zu lösen.

34. Internationale Abkommen sind angemessene Instrumente zum Schutz personenbezogener Daten in einem globalen Kontext, vorausgesetzt, dass das gewährte Schutzniveau den vorgenannten globalen Normen mindestens entspricht und dass jede natürliche Person einen einfachen und wirkungsvollen Zugang zu Rechtsmitteln hat, einschließlich des gerichtlichen Rechtsbehelfs. Es müssen besondere Garantien in Bezug auf den Zweck, für den die personenbezogenen Daten herangezogen werden, bestehen.

35. Unter diesen Bedingungen könnte das vorhergesehene transatlantische Abkommen als Modell für den Austausch mit anderen Drittländern und für andere Zwecke dienen. Der zukünftige Rechtsrahmen könnte die Bedingungen für Abkommen mit Drittländern aufführen.

36. Darüber hinaus sollte die EU die Zusammenarbeit zwischen internationalen Datenschutzbehörden ermutigen, zum Beispiel auf transatlantischer Ebene. Eine solche Zusammenarbeit ist ein erfolgreiches Mittel zur Förderung des Datenschutzes außerhalb der EU.

Verbindliche unternehmensinterne Datenschutzregelungen / Rechenschaftspflicht

37. Die Verarbeitung von Daten außerhalb der EU kann auch durch verbindliche unternehmensinterne Datenschutzregelungen (BCR), also internationale Verhaltenskodizes für multinationale Unternehmen, geschützt werden, die die weltweite Übertragung innerhalb eines multinationalen Unternehmens gestatten. Die WP29 hat BCR im Jahr 2003 eingeführt. Sowohl Datenschutzbehörden als auch multinationale Unternehmen sind der Ansicht, dass BCR ein gutes Mittel zur Vereinfachung der internationalen Datenströme sind und gleichzeitig den Schutz der personenbezogenen Daten gewährleisten. Die Richtlinie 95/46/EG hat die BCR jedoch nicht wirklich berücksichtigt. Infolgedessen erfordert der Prozess für die Genehmigung der BCR, der auf Artikel 26 Absatz 2 der Richtlinie 95/46/EG basiert, die Zustimmung aller durch eine BCR betroffenen Mitgliedstaaten. Folglich benötigt die Bewertung und die Genehmigung der BCR viel Zeit. Die WP29 hat beträchtliche Anstrengungen unternommen, die Anwendung und die Genehmigung der BCR in dem gültigen Rechtsrahmen zu fördern und zu vereinfachen. Zur Verbesserung des Prozesses haben bislang neunzehn Datenschutzbehörden einem „gegenseitige Anerkennung“ genannten Verfahren zur Anerkennung von BCR zugestimmt.

38. Vor diesem Hintergrund sollte eine Vorschrift zu den BCR weiter gestärkt und in den neuen Rechtsrahmen eingefügt werden. Dies würde mehrere Zwecke erfüllen:

    - Anerkennung der BCR als passendes Mittel zur Bereitstellung angemessener Schutzmaßnahmen;
    - Definieren der wichtigsten materiell- und verfahrensrechtlichen Elemente der BCR in Anlehnung an die diesbezügliche Stellungnahme der WP29.

39. Allgemein gesehen, könnte dem neuen Rechtsrahmen eine neue Vorschrift hinzugefügt werden, nach welcher die für die Datenverarbeitung Verantwortlichen für die personenbezogenen Daten, die sie verarbeiten, rechenschaftspflichtig und verantwortlich bleiben, selbst wenn diese an andere für die Datenverarbeitung Verantwortliche außerhalb der EU übermittelt wurden (siehe „Rechenschaftspflicht“ allgemeiner in Kapitel 6).

Abschließende Bemerkung

40. Im vorliegenden Kapitel wird die Globalisierung an sich diskutiert. Auf die eine oder andere Weise behandeln aber alle Kapitel dieses Beitrags dieses Thema. Wenn man an „Globalisierung“ denkt, denkt man häufig an Wirtschaft. In einer globalisierten Welt finden aber immer mehr Verarbeitungen von personenbezogenen Daten statt. Auch wenn der Einzelne häufig ein örtlich begrenztes Leben führt, kann er immer häufiger online angetroffen werden, und dort werden seine Daten global verarbeitet. Globalisierung ist folglich mit Technologie verknüpft (Kapitel 4), mit der Stellung der betroffenen Personen (Kapitel 5), dem für die Datenverarbeitung Verantwortlichen (Kapitel 6), den Datenschutzbehörden / der WP29 (Kapitel 7) und der Strafverfolgung (Kapitel 8).

4. Technologische Änderungen; Privacy by Design als neuer Grundsatz

41. Die grundlegenden Konzepte der Richtlinie 95/46/EG wurden in den Siebzigerjahren entwickelt, als Datenverarbeitung von Karteikästen, Lochkarten und Großrechnern geprägt war. Heute sind Computer allgegenwärtig, global und vernetzt. IT-Geräte werden zunehmend kleiner und mit Netzkarten, Wi-Fi oder sonstigen Funkschnittstellen ausgerüstet. In fast allen Büros und Familien können die Nutzer global über das Internet kommunizieren. Web 2.0-Dienste und Cloud Computing verschleiern die Unterscheidung zwischen für die Datenverarbeitung Verantwortlichen, Auftragsverarbeitern und betroffenen Personen.

42. Richtlinie 95/46/EG hat dem Zustrom technologischer Änderungen aufgrund ihrer soliden und technologisch neutralen Grundsätze und Konzepte gut standgehalten. Diese Grundsätze und Konzepte bleiben in der heutigen vernetzten Welt gleichermaßen maßgeblich, gültig und anwendbar.

43. Während es zwar klar ist, dass die oben beschriebenen technologischen Entwicklungen gut für die Gesellschaft sind, haben sie dennoch die Risiken für die Privatsphäre des Einzelnen und für den Datenschutz erhöht. Um diese Risiken auszugleichen, sollte der Rechtsrahmen zum Datenschutz ergänzt werden. Als Erstes sollte dem Rechtsrahmen der Grundsatz “Privacy by Design” beigefügt werden. Als Zweites sollten soweit erforderlich in Bezug auf bestimmte technologische Kontexte Verordnungen erlassen werden, welche die Verankerung von Grundsätzen des Datenschutzes und der Privatsphäre in diese Kontexte vorschreiben.

Grundsatz “Privacy by Design”

44. Die Idee, in Informations- und Kommunikationstechnologien („IKT”) Datenschutzmaßnahmen zu integrieren, ist nicht ganz neu. Richtlinie 95/46/EG enthält bereits verschiedene Bestimmungen, gemäß denen die für die Datenverarbeitung Verantwortlichen verpflichtet sind, bei der Planung und dem Einsatz von IKT Sicherheitstechniken zu integrieren. So legt Artikel 17 die Verpflichtung des für die Datenverarbeitung Verantwortlichen fest, angemessene technische und organisatorische Maßnahmen durchzuführen. Erwägungsgrund Nr. 46 fordert, dass diese Maßnahmen sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt des eigentlichen Verarbeitens getroffen werden. Artikel 16 legt die Vertraulichkeit der Verarbeitung fest. Dieser Grundsatz hat in den einschlägigen Verordnungen zur IT-Sicherheit seinen Niederschlag gefunden bzw. wird durch diese ergänzt. Abgesehen von diesen

Artikeln finden auch die Grundsätze in Bezug auf die Datenqualität Anwendung, die in Artikel 6 niedergelegt sind (Rechtmäßigkeit und Billigkeit, Zweckbindung, Erheblichkeit, sachliche Richtigkeit, Begrenzung der Speicherdauer, Verantwortung).

45. Während die vorgenannten Bestimmungen der Richtlinie „Privacy by Design" unterstützen, haben sie in der Praxis nicht ausgereicht, um sicherzustellen, dass der Schutz der Privatsphäre in IKT verankert wird. Die Nutzer von IKT-Diensten – Unternehmen, der öffentliche Sektor und ganz sicher Einzelpersonen – sind nicht dazu in der Lage, die erforderlichen Sicherheitsmaßnahmen selbst zu ergreifen, um ihre eigenen und die personenbezogenen Daten anderer zu schützen. Deshalb sollten diese Dienste und Technologien mit „Privacy by Default"-Voreinstellungen ausgestattet werden.

46. Aus diesem Grund muss der neue Rechtsrahmen eine Bestimmung enthalten, die die geltenden, eng gefassten Anforderungen in den breiteren und einheitlichen Grundsatz Privacy by Design umwandelt. Dieser Grundsatz sollte sowohl für die Entwickler und Hersteller der Technologien, als auch für die für die Datenverarbeitung Verantwortlichen, die über den Erwerb und die Nutzung der IKT zu entscheiden haben, verbindlich sein. Sie sollten dazu verpflichtet sein, bereits in der Planungsphase der Informations- und Kommunikationsverfahren und -systeme Technologien zum Datenschutz zu berücksichtigen. Sowohl die Anbieter solcher Systeme oder Dienstleistungen als auch die für die Datenverarbeitung Verantwortlichen sollten zeigen, dass sie alle erforderlichen Maßnahmen ergriffen haben, um diese Anforderungen zu erfüllen.

47. Dieser Grundsatz sollte die Umsetzung des Datenschutzes bei IKT („Privacy by Design" oder „PbD") erforderlich machen, die für die Verarbeitung personenbezogener Daten geplant sind oder für diese genutzt werden. Er sollte die Anforderung enthalten, dass IKT nicht nur die Sicherheit aufrechterhalten, sondern auch so geplant und entwickelt werden sollten, dass sie die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich halten oder deren Verarbeitung ganz vermeiden. Dies entspricht der kürzlich in Deutschland ergangenen Rechtsprechung.[13]

48. Die Anwendung eines solchen Grundsatzes würde die Notwendigkeit für den Einsatz von Technologien zum Schutz der Privatsphäre (PET), von "Privacy by Default"-Voreinstellungen und der erforderlichen Tools unterstreichen, die die Nutzer dazu befähigen, ihre personenbezogenen Daten besser zu schützen (z. B. Zugangskontrollen, Verschlüsselung). Dies sollte eine wesentliche Anforderung an Produkte und Dienstleistungen sein, die Dritten und Einzelkunden bereitgestellt werden (z. B. WiFi-Router, soziale Netzwerke und Suchmaschinen). Dies würde den

[13] Eine neuere Entscheidung des Deutschen Bundesverfassungsgerichts (Entscheidung vom 27. Februar 2008 – 1 BvR 370/07; 1 BvR 595/07 –) hat ein Verfassungsrecht in Bezug auf die Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Systeme, die dazu in der Lage sind, sensible personenbezogene Daten zu schaffen, zu verarbeiten oder zu speichern, sind besonders zu schützen. Dieser Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme ist anzuwenden bei Systemen, die allein oder in ihrer technischen Vernetzung personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen wesentlichen Einblick in das Privatleben einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Zu diesen Systemen zählen z. B. Personal Computer und Laptops, Handys und elektronische Kalender.

Datenschutzbehörden im Gegenzug mehr Befugnisse bei der tatsächlichen Durchsetzung solcher Maßnahmen geben.

49. Ein solcher Grundsatz sollte auf eine *technologisch neutrale* Weise definiert werden, damit er in einem sich schnell ändernden technologischen und sozialen Umfeld lange Bestand hat. Er sollte auch *flexibel* genug sein, damit die für die Datenverarbeitung Verantwortlichen und die Datenschutzbehörden die Möglichkeit haben, ihn je nach Fall in konkrete Datenschutzmaßnahmen umzusetzen.

50. Der Grundsatz sollte wie der geltende Erwägungsgrund Nr. 46 die Notwendigkeit betonen, dass ein solcher Grundsatz *so früh wie möglich* angewendet wird: „zum Zeitpunkt der Planung des Verarbeitungssystems und zum Zeitpunkt der eigentlichen Verarbeitung“. Schutzmaßnahmen, die in einer späten Phase umgesetzt werden, sind in Bezug auf die Forderung nach einem wirkungsvollen Schutz der Rechte und Freiheiten der betroffenen Personen inkonsistent und unzureichend.

51. Software- und Hardwareentwickler sollten während der Phase der Systemanalyse technologische Standards entwickeln und berücksichtigen, so dass Schwierigkeiten bei der Definierung und Spezifizierung der Anforderungen aus dem Grundsatz “Privacy by Design” minimiert werden. Solche Standards können in Bezug auf verschiedene Verarbeitungszwecke und -technologien sowohl genereller als auch spezifischer Natur sein.

52. Die folgenden Beispiele zeigen, wie PdB zu einem besseren Datenschutz beitragen kann:

    - Biometrische Identifikatoren sollten nicht in externen Datenbanken gespeichert werden, sondern stattdessen auf Speichermedien, über die die betroffene Person selbst die Kontrolle hat (d. h. intelligente Chipkarten „Smart Cards“).
    - Die Videoüberwachung in öffentlichen Verkehrssystemen sollte so konzipiert sein, dass die Gesichter der aufgezeichneten Personen nicht erkennbar sind oder es sollten andere Maßnahmen ergriffen werden, um die Risiken für die Betroffenen zu verringern. Natürlich müssen unter besonderen Umständen Ausnahmen gemacht werden, z. B., wenn die betreffende Person einer Straftat verdächtigt wird.
    - Die Namen von Patienten und sonstige Personen-Identifikatoren, die in den Informationssystemen von Krankhäusern gespeichert werden, sollten von Daten über den Gesundheitszustand und über medizinische Behandlungen getrennt werden. Sie sollten nur insoweit kombiniert werden, wie es für medizinische oder andere angemessene Gründe in einem sicheren Umfeld erforderlich ist.
    - Gegebenenfalls sollte eine Funktion integriert werden, die es den Betroffenen erleichtert, ihr Recht auf Widerruf der Einwilligung auszuüben, mit der daraus resultierenden Löschung der Daten auf allen betreffenden Servern (einschließlich Proxies und Mirrors).

53. In der Praxis erfordert die Umsetzung des Grundsatzes “Privacy by Design” die Bewertung verschiedener konkreter Aspekte oder Ziele. Insbesondere bei der Entscheidung über die Entwicklung, den Erwerb oder den Betrieb eines Verarbeitungssystems sollten die folgenden allgemeinen Aspekte/Ziele berücksichtigt werden:

- Datensparsamkeit: Die Entwicklung und Auswahl der Datenverarbeitungssysteme muss mit dem Ziel übereinstimmen, überhaupt keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
- Kontrollierbarkeit: Ein IT-System sollte den Betroffenen wirkungsvolle Mechanismen für die Kontrolle ihrer personenbezogenen Daten zur Verfügung stellen. Die Möglichkeiten bezüglich Einwilligung und Widerspruch sollten durch technologische Mittel unterstützt werden.
- Transparenz: Sowohl die Entwickler als auch die Betreiber von IT-Systemen müssen sicherstellen, dass die Betroffenen ausreichend über die Wirkungsweise des Systems informiert sind. Elektronische Auskunft/Information sollten ermöglicht werden.
- Anwenderfreundliche Systeme: Funktionen und Einrichtungen mit Bezug zur Privatsphäre sollten anwenderfreundlich sein, d. h., sie sollten in ausreichendem Umfang Hilfefunktionen und einfache Schnittstellen für die Nutzung durch weniger erfahrene Anwender bereitstellen.
- Datenvertraulichkeit: IT-Systeme müssen so entwickelt und gesichert werden, dass nur autorisierte Stellen Zugang zu personenbezogenen Daten haben.
- Datenqualität: Die für die Datenverarbeitung Verantwortlichen müssen die Datenqualität mit Hilfe technischer Mittel unterstützen. Die entsprechenden Daten sollten zugänglich sein, wenn sie für Rechtszwecke benötigt werden.
- Verwendungsbeschränkung: IT-Systeme, die für verschiedene Zwecke genutzt werden können oder die in einer Mehrbenutzerumgebung (d. h. virtuelle verbundenen Systeme wie Data-Warehouses, Cloud Computing, digitale Identifikatoren) betrieben werden, müssen sicherstellen, dass Daten und Prozesse, die für verschiedene Aufgaben oder Zwecke genutzt werden, auf eine sichere Weise voneinander getrennt werden können.

Verordnungen über bestimmte technologische Kontexte

54. Der Grundsatz „Privacy by Design“ reicht möglicherweise nicht aus, um in allen Fällen sicherzustellen, dass die angemessenen technologischen Datenschutzmaßnahmen ordnungsgemäß in die IKT integriert sind. Es könnte Fälle geben, in denen ein aktiveres Vorgehen erforderlich wäre. Um die Umsetzung solcher Maßnahmen zu erleichtern, sollte ein neuer Rechtsrahmen eine Bestimmung enthalten, die die Umsetzung bestimmter Verordnungen für bestimmte technologische Kontexte ermöglicht, die die Eingliederung von Grundsätzen zum Schutz der Privatsphäre erfordern.

55. Das ist kein neues Konzept: Artikel 14 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation enthält eine ähnliche Bestimmung: „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 (10) 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.”

56. Obenstehendes würde in bestimmten Fällen den Erlass besonderer normativer Akte erleichtern und dabei das Konzept “Privacy by Design” verankern und gleichzeitig sicherstellen, dass angemessene Spezifikationen bereitgestellt werden. Dies könnte

z. B. bei der RFID-Technologie, bei sozialen Netzwerken, personalisierter Werbung usw. der Fall sein.

Abschließende Bemerkungen

57. Die wachsende Bedeutung des Datenschutzes beim Erstellen und Betreiben von IT-System stellt an IT-Spezialisten zusätzliche Anforderungen. Also muss der Datenschutz fest in die Lehrpläne von IT-Berufen verankert werden.

58. Die Grundsätze des technologischen Datenschutzes und die daraus resultierenden konkreten Kriterien sollten im Rahmen von Datenschutzaudits[14] als Grundlage für die Vergabe von Gütesiegeln (Zertifizierungssystemen) genutzt werden.

5. Stärkung der betroffenen Personen

59. Das Potential, das die Richtlinie 95/46/EG der Stellung der betroffenen Person einräumt, wurde nicht vollständig ausgeschöpft. Darüber hinaus haben sich sowohl das Verhalten der Bürger als auch die Rolle der Betroffenen in Bezug auf den Datenschutz gewandelt. Dies war unter anderem wegen soziologischer Veränderung der Fall und da bei der Erhebung von Daten neue Wege beschritten werden (z. B. für Zwecke der Profilerstellung). Die Betroffenen gehen manchmal recht sorglos mit ihrer Privatsphäre um. Manchmal sind sie dazu bereit, die Privatsphäre gegen vermeintliche Vorteile einzutauschen. Auf der anderen Seite haben sie immer noch hohe Erwartungen an diejenigen, mit denen sie Geschäfte tätigen. Außerdem spielen die Betroffenen selbst in steigendem Maße eine aktive Rolle bei der Verarbeitung personenbezogener Daten, insbesondere im Internet.

60. Änderungen im Verhalten und in der Rolle der Betroffenen und die Erfahrungen mit der Richtlinie 95/46/EG machen es erforderlich, dass die Position der Betroffenen in dem Datenschutzrechtsrahmen gestärkt wird.[15] Die weitere Stärkung der Betroffenen ist unerlässlich, so dass sie eine aktivere Rolle spielen können.

Verbesserung der Rechtschutzmechanismen

61. Eine Stärkung des Betroffenen erfordert, dass er mehr Möglichkeiten hat, seine Rechte auszuüben und geltend zu machen. Da Gerichtsverfahren manchmal sehr schwierig sein können und ein finanzielles Risiko in sich bergen, sollte in die Richtlinie 95/46/EG die Möglichkeit einer Sammelklage aufgenommen werden.[16]

62. Darüber hinaus sollten die für die Datenverarbeitung Zuständigen für Beschwerdeverfahren sorgen, die leichter zugänglich, effektiver und bezahlbar sind (siehe auch Kapitel 6). Wenn diese Verfahren den Streit zwischen dem Betroffenen und dem für die Datenverarbeitung Verantwortlichen nicht lösen, sollte der Betroffene die Möglichkeit haben, auf alternative Verfahren der Streitbeilegung

---

[14] Das ist z. B. bei dem Projekt EuroPriSe der Fall.

[15] Dies ist insbesondere dann der Fall, wenn Kinder betroffen sind. Wenn Entscheidungen über die personenbezogenen Daten von Kindern getroffen werden, ist das Wohl des Kindes vorrangig zu berücksichtigen, wie in der UN-Kinderrechtskonvention (http://www2.ohchr.org/english/law/crc.htm) und in weiteren speziellen internationalen Vertragswerken und im innerstaatlichen Recht niedergelegt ist.

[16] Im Umweltrecht beispielsweise besteht die Möglichkeit einer Sammelklage.

zurückzugreifen. Diese werden hauptsächlich in der Industrie angeboten.[17] Diese Möglichkeiten sollten in einen neuen Rechtsrahmen integriert werden.

Transparenz

63. Transparenz ist eine weitere Grundvoraussetzung. Sie gibt dem Betroffenen *„ex ante"* ein Mitspracherecht, also vor der Verarbeitung. Das Erstellen von Profilen, Data Mining und technologische Entwicklungen, welche die Austauschbarkeit personenbezogener Daten vereinfachen, machen es für die Betroffenen noch wichtiger, dass sie wissen, durch wen, auf welcher Grundlage, von wo aus, für welche Zwecke und mit welchen technischen Mitteln die Daten verarbeitet werden. Es ist wichtig, dass diese Informationen verständlich sind. Die Pflicht, den Betroffenen zu informieren (Artikel 10 und 11 der Richtlinie 95/46/EG) wird jedoch nicht immer ordnungsgemäß umgesetzt. Ein neuer Rechtsrahmen sollte alternative Lösungen zur Förderung der Transparenz bieten. So sollten z. B. in Bezug auf die personalisierte Werbung neue Wege zum Informieren des Betroffenen entwickelt werden.

64. Darüber hinaus erfordert Transparenz, dass betroffene Personen benachrichtigt werden, wenn eine Datenschutzverletzung eintritt, die vermutlich negative Auswirkungen auf ihre personenbezogenen Daten und ihre Privatsphäre haben. Das würde dem Betroffenen die Möglichkeit geben, einen Versuch zur Kontrolle des erlittenen Schadens zu unternehmen (in bestimmten Fällen sollten auch die Behörden informiert werden, siehe auch Kapitel 6). In den neuen Rechtsrahmen sollte eine allgemeine Meldung von Datenschutzverletzungen eingefügt werden (siehe auch Kapitel 6).[18]

Einwilligung

65. Gemäß Richtlinie 95/46/EG ist die Einwilligung eine rechtmäßige Grundlage für die Datenverarbeitung (Artikel 7 und 8 der Richtlinie 95/46/EG). Die Einwilligung ist und bleibt eine wichtige Grundlage für die Verarbeitung, die unter bestimmten Umständen die Stellung des Betroffenen stärken könnte. Die Einwilligung muss jedoch ohne Zwang, in Kenntnis der Sachlage und für den konkreten Fall gegeben werden (Artikel 2 Buchstabe h Richtlinie 95/46/EG).

66. Es gibt viele Fälle, in denen die Einwilligung nicht ohne Zwang gegeben werden kann, insbesondere wenn ein deutliches Ungleichgewicht zwischen der betroffenen Person und dem für die Datenverarbeitung Verantwortlichen besteht (z. B. bei einem Beschäftigungsverhältnis oder wenn die personenbezogenen Daten öffentlichen Behörden erteilt werden müssen).

---

[17] Dadurch darf dem Einzelnen natürlich nicht das Recht auf das Einlegen geeigneter Rechtsmittel vor einem Gericht oder einer Datenschutzbehörde genommen werden.

[18] In der "Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre in der elektronischen Kommunikationen (Datenschutzrichtlinie für die elektronische Kommunikation)" hat die WP29 eine empfohlene Vorgehensweise im Zusammenhang mit der Meldung von bestimmten Datenschutzverletzungen, die in der Datenschutzrichtlinie für die elektronische Kommunikation behandelt werden, festgestellt. Dieselben Empfehlungen gelten auch für die Einführung allgemeiner Meldungen von Datenschutzverletzungen.

67. Darüber hinaus wird bei der Forderung, dass die Einwilligung ohne Zwang zu erfolgen hat, von der Annahme ausgegangen, dass die betroffene Person in vollem Umfang verstehen muss, was bei ihrer Einwilligung in die Bearbeitung ihrer Daten passiert. In vielen Fällen jedoch übersteigt die Komplexität von Datenerhebungsverfahren, Wirtschaftsmodellen, Käufer- Verkäuferbeziehungen und technologischen Anwendungen die Fähigkeit oder Bereitschaft des Einzelnen, aktiv über die Verwendung und gemeinsame Nutzung der Informationen zu entscheiden.[19]

68. In beiden Hypothesen ist die Einwilligung eine unangemessene Grundlage für die Verarbeitung. Sie wird aber dennoch häufig fälschlicherweise als die anzuwendende Grundlage angegeben. Die technologischen Entwicklungen fordern auch eine genaue Erwägung der Einwilligung. In der Praxis wird Artikel 7 der Richtlinie 95/46/EG nicht immer richtig angewendet. Dies ist insbesondere im Umfeld des Internet der Fall, wo eine stillschweigende Einwilligung nicht immer zu einer eindeutigen Einwilligung führt (wie dies in Artikel 7 Buchstabe a der Richtlinie gefordert wird). Wenn die Position der betroffenen Personen jedoch *„ex ante"*, also vor der Verarbeitung ihrer personenbezogenen Daten durch Dritte, gestärkt wird, muss die Einwilligung ausdrücklich (und deshalb ein Opt-in) für alle Verarbeitungen erfolgen, die auf der Einwilligung basieren.[20]

69. Der neue Rechtsrahmen sollte die Voraussetzung der Einwilligung näher darlegen und dabei die oben gemachten Anmerkungen berücksichtigen.

Harmonisierung

70. Derzeit wird eine Stärkung der Position der betroffenen Parteien durch die mangelnde Harmonisierung der innerstaatlichen Gesetze untergraben, mit denen die Richtlinie 95/46/EG umgesetzt wird. Verschiedene Elemente der Richtlinie, die essentiell für die Stellung der betroffenen Personen sind, wie die Bestimmung zur Haftung und die Möglichkeit, immaterielle Schäden einzuklagen[21], wurden nicht von allen Mitgliedstaaten umgesetzt. Abgesehen von diesen Unterschieden bei der Umsetzung der Richtlinie 95/46/EG, wird die Richtlinie in den Mitgliedstaaten nicht immer einheitlich ausgelegt. Bei einer wachsenden Globalisierung schwächen diese Unterschiede die Position der betroffenen Personen immer weiter. Eine Verbesserung der Harmonisierung ist deshalb von größter Bedeutung (siehe auch Kapitel 7). Sofern erforderlich sollte dies durch den Erlass von Rechtsvorschriften geschehen.

Die Rolle der betroffenen Personen im Internet

71. Natürliche Personen laden ihre eigenen personenbezogenen Daten in steigendem Maße im Internet hoch (soziale Netzwerke, Cloud Computing-Dienste usw.). Die Richtlinie 95/47/EG findet jedoch keine Anwendung auf Personen, die die Daten aus „ausschließlich persönlichen" Gründen oder „bei der Ausübung einer familiären

---

[19] Siehe „Data Protection Accountability: The essential Elements – A Document for Discussion", Centre for Information Policy Leadership, als die Sekretariatsgeschäfte des Galway-Projekts wahrnehmende Stelle, Oktober 2009, S. 4.

[20] Bezüglich der Einwilligung und Opt-in / Opt-out siehe auch Kapitel 2, in dem festgestellt wird, dass eine Verwechslung zwischen Opt-in und Opt-out vermieden werden sollte sowie die Verwendung der Einwilligung in Situationen, in denen sie nicht die angemessene Rechtsgrundlage darstellt.

[21] In den meisten Fällen, in denen die betroffenen Personen Schaden erlitten haben, handelt es sich um einen immateriellen Schaden, wie das Gefühl, sich nicht länger im öffentlichen und privaten Sektor bewegen zu können, ohne dabei beobachtet zu werden. Dieses Problem wird in der aktuellen „Überwachungsgesellschaft" größer.

Tätigkeit“[22] hochladen. Vertretbarerweise findet sie auch auf die Organisationen keine Anwendung, die den Dienst anbieten, d. h., die von einem Einzelnen hochgeladenen Informationen hosten und verfügbar machen (sofern der Dienst keine Daten für seine eigenen Zwecke verarbeitet), da der Service Provider nicht als für die Datenverarbeitung Verantwortlicher angesehen werden kann.[23] Das Ergebnis ist eine Situation, in der Garantien fehlen. Dies müsste möglicherweise geklärt werden, insbesondere angesichts der steigenden Zahl solcher Situationen. In diesem Zusammenhang sollte jeder, der einer Privatperson Leistungen anbietet, zur Bereitstellung bestimmter Schutzgarantien sowie, sofern angemessen, zur Bereitstellung von Garantien bezüglich der Vertraulichkeit der durch die Nutzer hochgeladenen Informationen verpflichtet sein, unabhängig davon, ob der Kunde ein für die Datenverarbeitung Verantwortlicher ist oder nicht. Zusätzlich sollte darüber nachgedacht werden, ob die Betroffenen mehr Möglichkeiten zur Ausübung ihrer Rechte im Internet erhalten sollten. Dazu gehört auch der Schutz der Rechte Dritter, deren personenbezogenen Daten verarbeitet werden könnten (z. B. soziale Netzwerke). Da es noch mehr ungelöste Fragen in diesem Zusammenhang geben könnte,[24] sollte angesichts eines neuen Rechtsrahmens die Rolle der betroffenen Person im Internet weiter geklärt werden.

6. Stärken der Verantwortung des für die Datenverarbeitung Verantwortlichen

72. Gemäß Richtlinie 95/46/EG obliegt es in erster Linie dem für die Datenverarbeitung Verantwortlichen, für die Einhaltung der Grundsätze und Verpflichtungen zu sorgen, die der Sicherstellung des Schutzes der personenbezogenen Daten von Einzelnen dienen. Die Richtlinie setzt implizit und in vielen Fällen auch explizit voraus, dass der für die Datenverarbeitung Verantwortlicher die Datenschutzgrundsätze einhält und bestimmte andere Verpflichtungen erfüllt.[25] Beispiele für die letztgenannten Verpflichtungen sind die Meldung an und die Vorabprüfung der Verarbeitung durch nationale Stellen.[26] Damit die Einhaltung der Datenschutzrechte des Einzelnen sichergestellt wird, müssen dem für die Datenverarbeitung Zuständigen bestimmte Pflichten wie die Informationspflicht auferlegt werden.[27]

---

[22] Für ein besseres Verständnis, ob eine Tätigkeit unter die “Ausnahmeklausel für Privathaushalte” fällt oder nicht, siehe Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163).

[23] Dieses Problem tritt nicht auf, wenn Organisationen – sowohl im öffentlichen als auch im privaten Sektor – Cloud Computing Anwendungen verwenden, denn die Richtlinie findet auf sie und ihre Verarbeitungsoperationen Anwendung, die „im Rahmen der Tätigkeit einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche” in der EU besitzt (siehe Artikel 4 Absatz 1 Buchstabe a). Kapitel 5 findet folglich Anwendung, unabhängig davon, ob der Service Provider seinen Sitz in der EU hat oder nicht.

[24] Z. B. in Bezug auf die Einwilligung von Kindern und/oder ihren Eltern, Auskunftsforderungen durch Strafverfolgungsbehörden, Informationsrechte in Bezug auf Internetaccounts durch Erben und Anwendungen von Drittanbietern.

[25] Artikel 6 Absatz 2 legt ausdrücklich Folgendes fest: “Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.” Dieser bezieht sich auf die wichtigsten Grundsätze zur Datenqualität.

[26] Siehe Artikel 18-21 der Richtlinie 95/46/EG.

[27] Andere Beispiele für die Rechte der Betroffenen sind unter anderem das Auskunftsrecht, das Recht auf Berichtigung, Löschung oder Sperrung sowie das Recht, Widerspruch gegen die Verarbeitung personenbezogener Daten einzulegen (Artikel 10-12 und 14). Diese Rechte ziehen die Verpflichtung für den für die Datenverarbeitung Verantwortlichen nach sich, für ihre Einhaltung zu sorgen.

73. Diese Verpflichtungen bestehen direkt oder indirekt auch für den Auftragsverarbeiter, wenn der für die Datenverarbeitung Verantwortliche einen Teil oder alle Datenverarbeitungsvorgänge auf diesen übertragen hat. Die WP29 verfasst derzeit eine interpretative Stellungnahme, um eine Orientierungshilfe zum Konzept des für die Datenverarbeitung Verantwortlichen und des Auftragsverarbeiters zu geben. Die WP29 möchte die Kommission bald zu diesem Thema beraten. Der Ratschlag könnte weitere Empfehlungen für einen zukünftigen Rechtsrahmen enthalten.

Einbetten des Datenschutzes in Organisationen

74. Die einschlägigen Bestimmungen der Richtlinie 95/46/EG bilden zweifellos eine solide Grundlage für den Schutz personenbezogener Daten und sollten beibehalten werden. Die Einhaltung der bestehenden Rechtsvorschriften ist jedoch häufig nicht richtig in die interne Praxis von Organisationen eingebettet. Die Privatsphäre ist häufig nicht in den Informationsverarbeitungstechnologien und -systemen verankert. Darüber hinaus ist das Management - und darunter fallen auch die Manager auf höchster Ebene - im allgemeinen nicht in ausreichendem Maße mit den Datenverarbeitungspraktiken ihrer eigenen Organisation vertraut und kann folglich auch keine aktive Verantwortung übernehmen. Die Datenschutzskandale der letzten Jahre in den Mitgliedstaaten lassen diese Besorgnis noch wachsen.

75. Solange der Datenschutz nicht Teil der gemeinsamen Werte und Praktiken einer Organisation wird, und solange die Verantwortung für den Datenschutz nicht ausdrücklich zugewiesen wird, ist die tatsächliche Einhaltung der Vorschriften gefährdet und es wird weiterhin zu Pannen kommen. Das wiederum wird das öffentliche Vertrauen in Unternehmen und öffentliche Verwaltungen gleichermaßen untergraben. Darüber hinaus würde eine Verankerung des Datenschutzes in die Organisationskultur den nationalen Datenschutzbehörden die Ausübung ihrer Kontroll- und Rechtsdurchsetzungsaufgaben erleichtern, da dies - wie in Kapitel 7 weiter ausgeführt - die Wirksamkeit des Datenschutzes erhöhen würde.

76. Die Grundsätze und Vorschriften der Richtlinie 95/46/EG sollten das kulturelle Gefüge von Organisationen auf allen Ebenen durchdringen, statt nur als eine Reihe von gesetzlichen Anforderungen gesehen zu werden, die von der Rechtsabteilung abgehakt werden. Die Anforderungen der Richtlinie sollten zur tagtäglichen Anwendung konkreter Datenschutzvorkehrungen führen. In die Planung von Informationstechnologien und -systemen sollte die Kontrolle der Privatsphäre integriert werden (siehe auch Kapitel 4). Darüber hinaus sollte innerhalb der Organisationen sowohl im öffentlichen als auch im privaten Sektor die interne Verantwortung für den Datenschutz in geeigneter Weise anerkannt, gestärkt und ausdrücklich zugewiesen werden.

77. Die Wirksamkeit der Bestimmungen der Richtlinie 95/46/EG hängt von den Anstrengungen der für die Datenverarbeitung Verantwortlichen ab, diese Ziele zu erreichen. Das macht die folgenden proaktiven Maßnahmen erforderlich:

    - *Einführung interner Strategien und Verfahren durch die für die Datenverarbeitung Verantwortlichen,* um die Forderungen der Richtlinie nach der Durchführung spezieller Verarbeitungsvorgänge durch den für die Verarbeitung Verantwortlichen umzusetzen. Diese internen Strategien und

Verfahren sollten auf höchster Organisationsebene genehmigt werden und folglich für alle Mitarbeiter bindend sein.

- *Einführung von Mechanismen zur Ausführung der internen Strategien und Verfahren einschließlich Beschwerdeverfahren (siehe auch Kapitel 5),* damit diese Strategien in der Praxis wirkungsvoll sind. Dazu kann auch die Sensibilisierung für den Datenschutz gehören sowie die Ausbildung des Personals und Schulungen.
- *Abfassen von Berichten über die Einhaltung der Vorschriften, das Durchführen von Audits, der Erhalt von Bescheinigungen einer neutralen Partei und/oder von Gütesiegeln,* als Kontrolle und Bewertung, ob die angenommenen internen Maßnahmen, mit denen die Einhaltung der Vorschriften sichergestellt werden soll, die personenbezogenen Daten wirkungsvoll verwalten, schützen und sichern (siehe auch Kapitel 4).
- Durchführen von *Datenschutz-Verträglichkeitsprüfungen*, insbesondere für bestimmte Datenverarbeitungsvorgänge, von denen angenommen wird, dass sie z. B. aufgrund ihrer Natur, ihres Umfangs oder ihres Zwecks besondere Risiken für die Rechte und Freiheiten der Betroffenen darstellen.
- *Übertragung der Verantwortung für den Datenschutz* an hierfür ernannte Personen, die die direkte Verantwortung dafür tragen, dass ihre Organisation die Datenschutzgesetze einhält.
- *Bescheinigungen der Führungskräfte des Unternehmens über das Einhalten der Bestimmungen*, in denen bestätigt wird, dass angemessene Maßnahmen für den Schutz der personenbezogenen Daten ergriffen wurden.
- *Transparenz dieser eingeführten Maßnahmen* gegenüber den Betroffenen und der Öffentlichkeit im Allgemeinen. Transparenz-Anforderungen tragen zur Rechenschaftslegung der für die Datenverarbeitung Verantwortlichen bei (z. B. Veröffentlichung der Datenschutzerklärung im Internet, Transparenz in Bezug auf interne Beschwerdeverfahren und die Veröffentlichung in Jahresberichten).

78. Artikel 17 Absatz 1 der Richtlinie 95/46/EG verlangt von den für die Datenverarbeitung Verantwortlichen bereits in gewissem Umfang sowohl technische als auch organisatorische Maßnahmen (der für die Datenverarbeitung Verantwortliche muss *„die geeigneten technischen und organisatorischen Maßnahmen durchführen, die für den Schutz gegen […] jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind“*). Diese Maßnahmen können einige der oben genannten Maßnahmen umfassen. In der Praxis hat Artikel 17 Absatz 1 jedoch nicht erfolgreich dazu beigetragen, den Datenschutz in Organisationen ausreichend effizient zu gestalten. Dies liegt auch an dem unterschiedlichen Vorgehen bei den nationalen Umsetzungsmaßnahmen.

Grundsatz der Rechenschaftspflicht[28]

79. Zur Bekämpfung dieses Problems wäre es angebracht, in den umfassenden Rechtsrahmen den Grundsatz der Rechenschaftspflicht aufzunehmen. Dieser Grundsatz würde die für die Datenverarbeitung Verantwortlichen dazu verpflichten, die notwendigen Maßnahmen zu ergreifen, um *sicherzustellen,* dass die wesentlichen Grundsätze und Verpflichtungen der geltenden Richtlinie bei der Verarbeitung personenbezogener Daten *eingehalten werden.* Eine solche Bestimmung würde die Forderung unterstreichen, dass Strategien und Mechanismen eingeführt werden müssen, mit denen die wesentlichen Grundsätze und Verpflichtungen der geltenden

[28] Zur Rechenschaftspflicht siehe auch Punkt 39.

Richtlinie wirkungsvoll werden. Sie würde den Bedarf an wirkungsvollen Schritten unterstreichen, die zu einer wirkungsvollen internen Durchführung der wesentlichen Verpflichtungen und Grundsätze führen, die in der aktuellen Richtlinie verankert sind. Darüber hinaus würde der Grundsatz der Rechenschaftspflicht von den für die Datenverarbeitung Verantwortlichen verlangen, dass sie Rechenschaftspflicht für die notwendigen internen Mechanismen sorgen, damit sie gegenüber externen interessierten Parteien, einschließlich der nationalen Datenschutzbehörden, die *Einhaltung beweisen* können. Die daraus resultierende Forderung nach Beweisen für die für Einhaltungszwecke durchgeführten angemessenen Maßnahmen wird die Durchsetzung von anzuwendenden Vorschriften sehr vereinfachen.

80. Die Maßnahmen, die von den für die Datenverarbeitung Verantwortlichen erwartet werden, sollten jedenfalls anpassbar sein und unter anderem die Art des Unternehmens berücksichtigen, seine Größe, ob es eine GmbH ist und die Art, Natur und Menge der zu verarbeitenden personenbezogenen Daten.

Mehr Optionen: proaktiv oder reaktiv

81. Einige der oben beschriebenen Maßnahmen könnten als übliche bewährte Praktiken angesehen werden, mit denen der Grundsatz der Rechenschaftspflicht beim Umsetzen in die Praxis erfüllt wird. Es könnte per Gesetz eine integrierte Belohnungsstruktur vorgesehen werden, um die Organisationen zur Umsetzung anzuregen.

82. Eine alternative Lösung hätte eher den Charakter einer Vorschrift. Artikel 17 Absatz 1 könnte z. B. so ausgearbeitet werden, dass zusätzliche proaktive Maßnahmen wie die vorgenannten niedergelegt werden, die durch die für die Datenverarbeitung Verantwortlichen umgesetzt werden müssen. Diese Maßnahmen könnten auf bestimme Resultate abzielen und sollten technologisch neutral sein.

83. Andere Maßnahmen hätten einen mehr reaktiven Charakter. Sie würden im Fall einer unrechtmäßigen Verarbeitung personenbezogener Daten angewendet werden und könnten unter anderem Folgendes beinhalten:

- *Einführen einer zwingend vorgeschriebenen Pflicht zur Meldung von Sicherheitsverletzungen* (siehe auch Kapitel 2 und 5).
- *Stärken der Durchsetzungsbefugnisse der Datenschutzbehörden*, einschließlich der Befugnis, konkrete Forderungen zur Sicherstellung eines effektiven Schutzes zu stellen (siehe auch Kapitel 7 Buchstabe a).

Vereinfachung der Meldungen

84. Die Meldungen von Datenverarbeitungsvorgängen an die nationalen Datenschutzbehörden könnten vereinfacht oder ihre Zahl verringert werden. In diesem Zusammenhang sollte die Verbindung zwischen der Einhaltung der oben genannten Anforderungen und der Möglichkeit einer weiteren Abstufung der behördlichen Anforderungen, insbesondere zur Meldung von Datenverarbeitungsvorgängen an die nationalen Datenschutzbehörden, untersucht werden.

85. Meldungen tragen zur Sensibilisierung in Bezug auf die Datenverarbeitungsvorgänge und die Datenschutzgepflogenheiten in einer

Organisation bei.[29] Sie geben den Datenschutzbehörden auch einen Überblick über die Datenverarbeitungsvorgänge. Eine bessere Datenverwaltung und Rechenschaftspflichten könnten jedoch denselben Zweck erfüllen. Diese Mechanismen könnten dabei helfen, die notwendigen Maßnahmen durchzuführen, um die wesentlichen Grundsätze und Verpflichtungen zu beachten, die in der geltenden Richtlinie verankert sind und die Beweise für eine solche Einhaltung zu liefern.

86. Es sollte untersucht werden, ob und in welchem Umfang die Meldungen auf solche Fälle eingeschränkt werden könnten, in denen ein ernsthaftes Risiko für den Datenschutz besteht. Das würde den Datenschutzbehörden die Möglichkeit geben, mehr Auswahl zu treffen und ihre Anstrengungen auf solche Fälle zu konzentrieren. Selbst in solchen Fällen könnten den Meldungen rationalisiert werden, z. B., indem die Ergebnisse von Datenschutz-Verträglichkeitsprüfungen oder die Ergebnisse von Audits durch eine neutrale Partei bereitgestellt würden. Dies könnte mit einem Meldesystem verbunden werden, bei dem alle für die Datenverarbeitung Verantwortlichen in ein von den Datenschutzbehörden geführtes Verzeichnis eingetragen würden. Somit würde im Bedarfsfall die einfache Ermittlung der organisatorischen Instanzen für eine effiziente und wirkungsvolle Durchsetzung gewährleistet werden.

7. Eine stärkere und eindeutigere Rolle für die Datenschutzbehörden und ihre Zusammenarbeit in der EU

7a. Datenschutzbehörden

87. Derzeit gibt es große Unterschiede in Bezug auf die Positionen der Datenschutzbehörden in den 27 Mitgliedstaaten. Der Grund hierfür liegt in den Unterschieden in der geschichtlichen Entwicklung, der Rechtsprechung, Kultur und den internen Organisationen der Mitgliedstaaten, aber auch daran, dass es Artikel 28 der Richtlinie 95/46/EG in mehrerlei Hinsicht an Präzision mangelt. Außerdem wurde die Richtlinie in einigen Gebieten bis zu einem gewissen Grad schlecht umgesetzt. Das hat zu großen Unterschieden zwischen den Mitgliedstaaten geführt, unter anderem bezüglich der Position, den Ressourcen und den Befugnissen der Datenschutzbehörden.

88. Die neuen Herausforderungen an den Datenschutz (Globalisierung und die technologischen Änderungen, Kapitel 3 und 4) machen eine strikte, einheitlichere und effektivere Überwachung erforderlich. Der neue Rechtsrahmen sollte folglich hochrangig und richtunggebend einheitliche Standards in Bezug auf Unabhängigkeit und effektive Befugnisse garantieren sowie den Datenschutzbehörden eine beratende Rolle im Gesetzgebungsverfahren geben und die Möglichkeit, die Geschäftsordnung selbst festzulegen, insbesondere durch das Setzen von Prioritäten bei der Behandlung von Beschwerden.

[29] Diese Ansichten werden durch den Bericht der Artikel-29-Gruppe WP106 über die Meldepflicht an die nationalen Kontrollstellen, zur bestmöglichen Nutzung der Ausnahmen und Vereinfachungen und zur Rolle von Datenschutzbeauftragten in der Europäischen Union bestätigt, der am 18. Januar 2005 angenommen wurde.

89. Datenschutzbehörden müssen gänzlich unabhängig sein. Der geltende Artikel 28 Absatz 1 der Richtlinie 95/46/EG ist in dieser Hinsicht unklar, wie der Fall C-584/07 (Kommission gegen Deutschland) zeigt, der derzeit vor dem Europäischen Gerichtshof verhandelt wird. In dem neuen Rechtsrahmen sollten die Datenschutzbehörden:

- über eine vollumfängliche institutionelle Unabhängigkeit verfügen und keiner anderen Regierungsbehörde unterstehen;
- über eine funktionale Unabhängigkeit verfügen und nicht Anweisungen oder Kontrollen in Bezug auf die Art und den Umfang ihrer Tätigkeiten unterliegen;
- über finanzielle Unabhängigkeit verfügen. Sie sollten über eine Infrastruktur verfügen, die den reibungslosen Ablauf ihrer Tätigkeiten ermöglicht und insbesondere über eine angemessene Finanzierung. Den Datenschutzbehörden sollten in ausreichendem Umfang Ressourcen zugewiesen werden.

90. Die Aufgaben der Datenschutzbehörden zur Rechtsdurchsetzung werden immer wichtiger. Sie sollten stark, mutig und strategisch bei ihrem Eingreifen und bei der Rechtsdurchsetzung sein. Der aktuelle Wortlaut von Artikel 28 der Richtlinie 95/46/EG hat zu großen Unterschieden in den Befugnissen zur Rechtsdurchsetzung geführt. Der neue Rechtsrahmen sollte ein einheitlicheres Vorgehen der Mitgliedstaaten bei der Ausstattung der Datenschutzbehörden mit den erforderlichen Befugnissen fordern und er sollte diesbezüglich spezifischere Angaben machen als die Richtlinie 95/46/EG. Die erforderlichen Befugnisse sollten unter anderem das Recht auf Verhängung von Geldbußen gegen die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter umfassen.

91. Die beratende Funktion der Datenschutzbehörden im Gesetzgebungsprozess ist unabdingbar. Denn für eine Verbesserung der (Datenschutz)-Gesetzgebung ist häufig das Wissen der Datenschutzbehörden aus Ermittlungen und Rechtssetzungsaktion erforderlich. Die beratende Rolle sollte alle Maßnahmen und Verordnungen zum Schutz der Rechte und Freiheiten des Einzelnen in Bezug auf die Verarbeitung personenbezogener Daten umfassen und nicht nur „Rechtsverordnungen und Verwaltungsvorschriften“.[30] Die Datenschutzbehörden sollten um Rat gefragt werden, bevor die Gesetzgebungsvorlage angenommen wird. Darüber hinaus sollte der neue Rechtsrahmen sicherstellen, dass die Datenschutzbehörden gegenüber ihren nationalen Parlamenten und/oder gegenüber anderen zuständigen innerstaatlichen Einrichtungen eine beratende Rolle haben, wenn die letztgenannten mit dem Gesetzgebungsprozess für neue EU-Rechtsvorschriften befasst sind.

92. Datenschutzbehörden müssen ihre eigene Geschäftsordnung machen können, wenn sie die Prioritäten unter anderem in Bezug auf die Abwicklung von Beschwerden regeln. Dazu gehört auch die Art und Weise, in der auf Beschwerden reagiert wird.[31] Die Datenschutzbehörden sollten auf jeden Fall in Betracht ziehen können, ob die Bearbeitung einer Beschwerde in ausreichendem Maße zum Schutz der personenbezogenen Daten beiträgt.[32] Der neue Rechtsrahmen sollte den Datenschutzbehörden die Möglichkeit geben „selektiv zu sein, um effektiv zu sein“.

---

30 Artikel 28 Absatz 2 der Richtlinie 95/46/EG.

31 Die Möglichkeit selektiv zu sein, kann auf verschiedene Weise in die Praxis umgesetzt werden, z. B. durch die Einführung von „Schnellverfahren“ für geringfügigere Beschwerden.

32 Bei der Frage, ob eine Beschwerde bearbeitet werden sollte, können z. B. die folgenden Kriterien angewendet werden: Betrifft die Situation viele Personen, betrifft die Beschwerde eine Verletzung

93. Auf der anderen Seite müssen die Datenschutzbehörden für die Art und Weise rechenschaftspflichtig sein, in welcher sie ihre stärkere Überwachungsrolle ausüben. Sie sollten diesbezüglich transparent sein und öffentlich über ihre Vorgehensweise und ihre Prioritäten berichten. Der aktuelle Wortlaut von Artikel 28 Absatz 5 der Richtlinie 95/46/EG muss diesbezüglich in dem neuen Rechtsrahmen präzisiert werden.

7b. Zusammenarbeit der Datenschutzbehörden

Der geltende Rechtsrahmen

94. Artikel 29 der Richtlinie 95/46/EG hat die Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (WP29) als institutionelle Einrichtung für die Zusammenarbeit zwischen den nationalen Datenschutzbehörden eingesetzt. Die WP29 ist unabhängig und hat eine beratende Funktion. Ihre Aufgaben sind in Artikel 30 Absatz 1 der Richtlinie festgelegt. Sie soll zu einer einheitlichen Anwendung der Richtlinie beitragen, indem sie Fragen im Zusammenhang mit den einzelstaatlichen Vorschriften prüft, Stellung nimmt zum Schutzniveau in der Gemeinschaft und in Drittländern und (auch auf eigene Initiative hin) bei Vorschlägen zu Gemeinschaftsrecht mit Auswirkungen auf den Datenschutz oder bei anderen Angelegenheiten des Schutzes von Personen mit Bezug auf die Verarbeitung personenbezogener Daten in der Gemeinschaft berät. Die Kommission ist Mitglied der WP29 und nimmt die Sekretariatsgeschäfte der Gruppe wahr.

95. Die WP29 erfüllt ihre Aufgabe im Anwendungsbereich der Richtlinie, wie in Artikel 3 Absatz 2 dargelegt. Im Bereich der polizeilichen und justiziellen Zusammenarbeit haben die europäischen Datenschutzbehörden im Jahr 2007 die Arbeitsgruppe Polizei und Justiz (WPPJ) gegründet, welche eine ähnliche Rolle wie die WP29 erfüllt, jedoch ohne Rechtsgrundlage und ohne dass die Sekretariatsgeschäfte durch eine Gemeinschaftsinstitution übernommen werden. Der Rahmenbeschluss 2008/977/JI, der in diesem Bereich Datenschutzgrundsätze einführt, sieht keine institutionalisierte Zusammenarbeit mit den Datenschutzbehörden vor.

Die Arbeitsweise der WP29

96. Die WP29 besteht seit nunmehr über 10 Jahren und hat signifikant zum Erreichen der Ziele gemäß Artikel 30 der Richtlinie 95/46/EG beigetragen. Das Ergebnis vieler Aktivitäten dieser Arbeitsgruppe kann auf der Webseite nachgelesen werden.[33]

97. Die WP29 hat konstant an einer Verbesserung ihre Wirksamkeit gearbeitet und sollte weiterhin das Augenmerk auf ihre eigene Arbeitsweise richten.
Hierbei sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Wie kann die WP29 wirksam zu einer einheitlichen Umsetzung der EU-Rechtsvorschriften in innerstaatliche Gesetze und zu einer einheitlichen Anwendung derselben beitragen?

---

eines wichtigen Datenschutzgesetzes oder ist es nur ein Zufall, wird die Bearbeitung vermutlich erfolgreich sein und wird sie nicht unverhältnismäßig hohe Anstrengungen erfordern?

[33] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue

- Wie kann sie ihre Wirksamkeit gegenüber den EU-Institutionen und insbesondere gegenüber der Kommission verbessern und dabei gleichzeitig die hybride Rolle der Kommission berücksichtigen, die Mitglied der WP29 ist, deren Sekretariatsgeschäfte führt und gleichzeitig auch der Empfänger vieler der Stellungnahmen der WP29 ist.

Folgen für die Zukunft

98. Als oberste Priorität sollte sichergestellt werden, dass alle Fragen bezüglich der personenbezogenen Daten, insbesondere im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in die Aktivitäten der aktuellen WP29 einbezogen werden. Ein umfassender Rechtsrahmen sollte einen Gesamtberater und eine effektive Zusammenarbeit zwischen den Kontrollbehörden beinhalten. In der Übergangszeit bis zur Umsetzung der Gesetzesänderungen, müssen angemessene Formen für eine Zusammenarbeit zwischen der WP29 und der WPPJ gefunden werden.

99. Andere Verbesserungen setzen keine Gesetzesänderungen voraus.

- Die einheitliche Anwendung des innerstaatlichen Rechts, mit dem die Richtlinie 95/46/EG umgesetzt wird, kann mit dem geltenden Rechtsrahmen erreicht werden, indem die Arbeitsmethoden der Arbeitsgruppe weiter verbessert werden und soweit erforderlich, die Mitglieder der WP29 zur Umsetzung der Ansichten der Gruppe in nationale Praxis aufgefordert werden.
- Gemäß Artikel 29 der Richtlinie 95/46/EG übernimmt die Kommission die Sekretariatsgeschäfte der WP29. Das Sekretariat sollte eng mit dem Vorsitz der WP29 und dem Stab zusammenarbeiten. Die Aufgaben des Sekretariats und des Vorsitzes ergänzen sich, und sie sollten eng zusammenarbeiten, um der WP29 so die Möglichkeit zu geben, ihre Aufgaben auf die wirkungsvollste Weise zu erfüllen. Während das Sekretariat die logistischen Aspekte der Arbeit der WP29 regelt und die Arbeitsgruppe bei der Vorbereitung ihrer Stellungnahmen und Dokumente unterstützt, konzentrieren sich der Vorsitz (und der stellvertretende Vorsitz) hauptsächlich auf den Entscheidungsfindungsprozess und auf die Strategie der WP29.
- Die Beziehungen zwischen der WP29 und der Kommission, die die Sekretariatsgeschäfte für die WP29 wahrnimmt, können durch das Niederlegen der wichtigsten Rollen der beiden Akteure in einem Memorandum of Understanding weiter verbessert werden. Dieses Memorandum sollte auch die der WP29 zur Verfügung stehenden Geldmittel ansprechen, so dass diese bei der Ausübung ihrer Aufgaben auf ihre vollen Ressourcen zurückgreifen kann. Schließlich sollte auch die Arbeitsweise des Sekretariats angesprochen werden, so dass sowohl die WP29 als auch das Sekretariat über ausreichende Mittel verfügen, um die Stellungnahmen und Arbeitsdokumente der WP29 vorzubereiten. Die WP29 wird im Jahr 2010 Beratungen mit der Kommission zu Obenstehendem aufnehmen.

8. Datenschutzherausforderungen im Bereich der Strafverfolgung

100. Der Datenschutz im Bereich Polizei und Justiz ist ein spezielles Thema, dem besondere Aufmerksamkeit gewidmet werden muss. Dabei muss der komplexen Beziehung zwischen den Aktivitäten des Staates zur Wahrung der Sicherheit und

dem Schutz der personenbezogenen Daten des Einzelnen Rechnung getragen werden. Die Besonderheit dieses Themas ist nicht nur das Ergebnis der vormaligen Säulenstruktur der ehemaligen EU-Verträge, sondern sie ist in größerem Umfang anerkannt (siehe z. B. die Ausnahmen in Artikel 13 der Richtlinie 95/47/EG und die Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon).

Der sich ändernde Kontext innerhalb der EU

101. Mit dem Inkrafttreten des Vertrags von Lissabon werden im Bereich des Datenschutzes neue Perspektiven für die Gesetzgebung geschaffen. Die Säulenstruktur wird abgeschafft, und mit Artikel 16 AEUV wird für den Datenschutz in fast allen Bereichen des EU-Rechts eine einheitliche Rechtsgrundlage geschaffen (siehe Kapitel 2). Das heißt nicht unbedingt, dass die Datenschutzgrundsätze für Polizei und Justiz mit denselben Vorschriften umgesetzt werden sollte, wie in anderen Teilen der Gesellschaft. Die Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon besagt, dass es "sich als erforderlich erweisen könnte", im Bereich der Strafverfolgung spezifische Vorschriften zu erlassen.

102. Der Datenschutz und der Datenaustausch werden wichtige Kernpunkte des Stockholmer Programms sein. Die Beschlussfassung wird auf dem Konzept der richtigen Balance zwischen den Erfordernissen der Strafverfolgung und den Anforderungen des Datenschutzes beruhen. Neue Maßnahmen sollten erst nach einer angemessenen Bewertung des geltenden Rechtsrahmens ergriffen werden.

103. Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss von den Mitgliedstaaten bis zum 27. November 2010 umgesetzt werden. Dieser Rahmenbeschluss kann als erster Schritt in Richtung eines allgemeinen Rechtsrahmens in der ehemaligen dritten Säule angesehen werden. Er ist jedoch alles andere als vollständig. Er ist lediglich in grenzüberschreitenden Situationen anwendbar. Ihm scheinen die essentiellen Elemente und Mittel zu fehlen, um effektiv mit den sich ändernden Arbeitsmethoden im Bereich der Strafverfolgung umzugehen.

Die sich ändernde Gewichtung bei der Strafverfolgung

104. In den letzten Jahren zeigte sich eine Verschiebung bei der Gewichtung der Arbeitsmethoden der Polizei und der Strafverfolgungsbehörden in Bezug auf die Verwendung (personenbezogener) Informationen. Zu dieser Verschiebung kam es, da die Nutzung von Informationen immer wichtiger wurde, um den neuen Bedrohungen aus dem Terrorismus und der organisierten Kriminalität entgegenzutreten. Sie ist das Ergebnis der technologischen Entwicklungen der letzten Jahre.

105. Die Schwerpunktverschiebung hat mehrere Dimensionen:

- Die Nutzung der Informationen konzentriert sich auf frühere Phasen der Kette: Zusätzlich zu der traditionellen Verwendung der Informationen für die Ermittlungen und das Aufdecken einer bestimmten Straftat werden Informationen erhoben und ausgetauscht, um mögliche Straftaten zu verhindern („vorbeugende Überwachung").
- Die Nutzung der Informationen konzentriert sich auf eine größere Personengruppe. Die Informationen werden nicht nur von Personen erhoben

und ausgetauscht, die in indirekter Verbindung zu einer Straftat stehen wie Verdächtige oder Zeugen, sondern auch von größeren Populationsgruppen, die nicht Gegenstand von Ermittlungen sind (z. B. Reisende, Personen, die Zahlungsdienste in Anspruch nehmen usw.).

- Die genutzten Informationen basieren immer stärker auf Technologie. Technologie verbindet selbst verschiedene Faktoren, um so das zukünftige Verhalten von Personen mit Hilfe von automatisierten Mitteln (Data Mining, Erstellen von Profilen) vorherzusagen.
- Die genutzten Informationen sind unterschiedlicher Natur. Hierbei wird nicht nur auf objektiv ermittelte Informationen (Fakten und Zahlen) gebaut, sondern auch auf Informationen, die auf Bewertungen und Analysen aus dem Gefüge einer Ermittlung stammen (weiche Daten). Außerdem kann die Unterscheidung zwischen den beiden Informationsarten je nach Mitgliedstaat variieren.
- Die steigende Nutzung personenbezogener Informationen aus dem Privatsektor für vorbeugende Maßnahmen, wie z. B. Bank- oder Finanzdaten und Fluggastdaten, die durch Luftfahrtgesellschaften und CRS erhoben werden.
- Informationen, die für einen bestimmten, rechtmäßigen Grund erhoben werden, werden in zunehmendem Maße für andere teilweise unvereinbare Zwecke verwendet. Die Zwecke gleichen sich immer weiter an. Interoperabilität zwischen den Systemen ist eine wichtige Entwicklung, die jedoch kein rein technisches Thema ist, insbesondere im Hinblick auf die Gefahren der Verbindung von Datenbanken, die unterschiedlichen Zwecken dienen.
- An der Nutzung der Informationen sind mehr Behörden beteiligt, nicht nur die Polizei und die Justizbehörden *stricto sensu*, sondern auch andere öffentliche Behörden wie Grenzkontrollbehörden, Finanzbehörden und nationale Sicherheitsdienste.

106. Dieser Wandel in der Gewichtung bei der Strafverfolgung hat zu einem dramatischen Anstieg bei der Speicherung und dem Austausch personenbezogener Daten in Bezug auf Aktivitäten der Polizei und des Justizsektors geführt. Die technologische Möglichkeit, Informationen einfach zu kombinieren, hat möglicherweise tiefgreifende Auswirkungen auf die Privatsphäre und den Datenschutz aller Bürger sowie auf ihre Möglichkeit, ihre Grundrechte wirklich wahrzunehmen und auszuüben, insbesondere das Recht, sich frei zu bewegen sowie die Rede- und Meinungsfreiheit.

Herausforderungen für den Datenschutz

107. Angesichts dieses Hintergrunds sind die Herausforderungen an den Datenschutz immens. Ein zukünftiger Rechtsrahmen sollte auf jeden Fall die folgenden Punkte angehen:

- Die Tendenzen könnten zu einer mehr oder weniger ständigen Überwachung aller Bürger führen. Das wird häufig als Überwachungsgesellschaft bezeichnet. Ein Beispiel wäre die kombinierte Nutzung von intelligenten Cctv-Kameras und von anderen Instrumenten wie der automatischen Nummernschilderkennung, mit der alle Autos registriert werden, die in ein bestimmtes Gebiet einfahren oder es verlassen.

- Datenbanken können für Data Mining genutzt werden, und auf der Grundlage des Erstellens von Profilen Einzelner können Risikobewertungen einzelner Personen durchgeführt werden. Dies könnte Personen mit einem bestimmten Hintergrund stigmatisieren.
- Bei Analysen, die auf der Grundlage genereller Kriterien erstellt werden, besteht das Risiko großer Ungenauigkeiten, was zu einer großen Anzahl an falschen Negativ- oder falschen Positivergebnissen führt.
- Die Verarbeitung personenbezogener Daten von Personen, die nicht verdächtig sind, wird immer wichtiger. Bestimmte Bedingungen und Garantien werden benötigt, damit ihre Legitimität und die Proportionalität bewertet werden und um Vorurteile gegenüber Personen zu vermeiden, die nicht (aktiv) an einer Straftat beteiligt sind.
- Es ist eine erhöhte Verwendung biometrischer Daten, einschließlich der DNA zu verzeichnen. Dies stellt ein gewisses Risiko dar.

Forderungen an die Rechtsetzung und die Politikgestaltung

108. Die wachsende Zahl sektorspezifischer Initiativen, die angenommen oder geplant wurden, könnte leicht zum Überlappen oder sogar zur Verzerrung von Maßnahmen führen. Deshalb könnte es wertvoll sein, den Informationsaustausch auf eine einheitliche Strategie zu stützen, vorausgesetzt, dass der Datenschutz vollumfänglich berücksichtigt wird und ein wesentlicher Bestandteil der Strategie ist.[34]

109. Es ist von größter Wichtigkeit, die bestehenden Rechtsinstrumente und ihre Anwendung zu bewerten. Dabei sollten die Kosten für die Privatsphäre berücksichtigt werden. Die Bewertung der bestehenden Maßnahmen sollte vor der Ergreifung neuer Maßnahmen erfolgen. Darüber hinaus sollte eine regelmäßige Überprüfung der bestehenden Maßnahmen stattfinden.

110. Transparenz ist ein grundlegendes Element. Den Betroffenen sollten verständliche Informationen über die Verwendung der erhobenen Daten und über die Logik der Verarbeitung zur Verfügung stehen. Diese Informationserteilung sollte lediglich in individuellen Fällen eingeschränkt werden, um laufende Ermittlungen nicht zu gefährden und sollte zeitlich eingeschränkt sein. Die Informations- und Berichtigungsrechte der betroffenen Personen sollten in einem grenzüberschreitenden Kontext angegangen werden, damit die Betroffenen nicht die Kontrolle verlieren.

111. Besondere Aufmerksamkeit muss der Transparenz und der demokratischen Kontrolle bei der Gesetzgebung gewidmet werden. Datenschutz-Verträglichkeitsprüfungen, angemessene Formen der Beratung mit Datenschutzbehörden und eine effektive parlamentarische Debatte sowohl auf nationaler als auch auf gemeinschaftlicher Ebene sollten eine wichtige Rolle spielen.

112. Die Architektur jedes Systems für die Speicherung und den Austausch personenbezogener Daten sollte gut ausgearbeitet sein. Es folgen einige allgemeine Überlegungen:
    - Die Architektur sollte durch „Privacy by Design“ und Technologien zum Schutz der Privatsphäre (Zertifizierungsprogramm) bestimmt werden. In einem

[34] Eine europäische Informationsmanagement-Strategie, wie sie derzeit vom Rat erarbeitet wird, könnte sich in diesem Kontext als nützliches Instrument herausstellen, sofern sie richtig erstellt wird.

Raum der Freiheit, der Sicherheit und des Rechts, in dem die Behörden die wichtigsten Akteure sind und in dem sich jede Initiative, die auf eine wachsende Überwachung des Einzelnen und ein steigendes Einholen und Verarbeiten von personenbezogenen Daten abzielt, direkt auf das Grundrecht auf Privatsphäre und Datenschutz auswirken könnte, könnten solche Anforderungen zur zwingenden Vorschrift werden.

- Zweckbindung und Datensparsamkeit sollten als Leitgrundsätze bestehen bleiben.
- Der Zugang zu großen Datenbanken muss so konfiguriert werden, dass generell Online kein direkter Zugriff auf gespeicherte Daten gestattet ist. Ein Treffer/kein Treffer-System oder ein Index-System gilt allgemein als vorzuziehen.
- Die Entscheidung zwischen Modellen mit einem Zentralspeicher, also Systemen mit einer zentralen Datenbank auf EU-Ebene und mit einer dezentralisierten Speicherung sollte aufgrund transparenter Kriterien getroffen werden. Das Ergebnis dieser Entscheidung sollte jedenfalls die Rolle und die Verantwortung des/der für die Datenverarbeitung Verantwortlichen klar und solide definieren und eine angemessene Überwachung durch die zuständigen Datenschutzbehörden sicherstellen.
- Biometrische Daten sollten nur dann genutzt werden, wenn die Verwendung anderen, weniger intrusiven Materials nicht dieselben Ergebnisse liefert.

113. Die externe Dimension. Es sollte vermeiden werden, dass das strikte System für den Austausch personenbezogener Daten innerhalb der EU umgangen wird. Die Beziehungen zu Drittländern sollten auf einen klaren Rechtsrahmen gestützt werden, der für alle Parteien und im Hinblick auf das Konzept der Angemessenheit bindend ist. Das System der Angemessenheit sollte nach einer Beurteilung durch die nationalen Datenschutzbehörden bewertet werden und sofern erforderlich, durch gemeinsame Mechanismen, die eine einheitliche Umsetzung und Wirksamkeit sicherstellen.

114. Groß angelegten Informationssystemen in der EU muss besondere Aufmerksamkeit gewidmet werden, dazu gehören, sofern erforderlich, maßgeschneiderte Garantien für den Datenschutz.

115. Eine unabhängige Kontrolle, die justizielle Aufsicht und die Rechtsmittel sollten ordnungsgemäß durchgeführt werden. Dazu gehören in jedem Fall angemessene Ressourcen und Kompetenzen für eine unabhängige Kontrolle.

116. Die Datenschutzbehörden, die die Rechtmäßigkeit der Datenverarbeitung sicherstellen müssen, sollten in allen Bereichen gestärkt und in den Rechtsrahmen integriert werden, auch indem stabile Mechanismen ins Auge gefasst werden, ähnlich denen, die derzeit auf Angelegenheiten der ersten Säule angewendet werden, um ein harmonisiertes Vorgehen in der gesamten EU und darüber hinaus zu fördern.

Für die Artikel-29-Arbeitsgruppe

Der Vorsitzende
Alex Türk

Für die Arbeitsgruppe Polizei und Justiz

Der Vorsitzende
Francesco PIZZETTI