FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden

Stärkung der Grundrechte-Architektur in der EU – Teil II

Der vorliegende Bericht befasst sich mit Fragen im Zusammenhang mit dem Schutz personenbezogener Daten (Artikel 8), der unter das Kapitel II „Freiheiten" der Charta der Grundrechte der Europäischen Union fällt.

Europe Direct soll Ihnen helfen, Antworten auf Ihre Fragen zur Europäischen Union zu finden

Gebührenfreie Telefonnummer (*):
00 800 6 7 8 9 10 11

(*) Einige Mobilfunkanbieter gewähren keinen Zugang zu 00 800-Nummern oder berechnen eine Gebühr.

Foto (Umschlag): Comstock Images

Weitere Informationen zur Europäischen Union sind online verfügbar (http://europa.eu).

Katalogisierungsdaten befinden sich am Ende der Veröffentlichung.

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2012

ISBN 978-92-9192-508-7
doi:10.2811/47194

Printed in Belgium

Gedruckt auf chlorfrei gebleichtem papier (PCF)

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden

Stärkung der Grundrechte-Architektur in der EU – Teil II

Inhalt

Vorwort

Die Grundrechte-Architektur in der Europäischen Union hat sich über die Jahre herausgebildet und entwickelt sich ständig weiter. Dieser Bericht ist Bestandteil einer Reihe von vier Berichten der Agentur der Europäischen Union für Grundrechte (FRA), die sich mit drei eng verbundenen Aspekten und Einrichtungen befassen, welche die Grundrechte-Architektur in der Europäischen Union mitgestalten: die Gleichbehandlungsstellen, die Datenschutzbehörden und die nationalen Menschenrechtsinstitutionen.

Für die FRA sind diese drei Gruppen von Beobachtungsstellen auf nationaler Ebene von großer Bedeutung. Im Zusammenhang mit den Grundrechten in den Mitgliedstaaten wurde die FRA zum Beispiel ausdrücklich mit der Zusammenarbeit mit Regierungsorganisationen und öffentlichen Stellen, einschließlich Datenschutzbehörden, beauftragt, um die Zusammenarbeit zwischen der nationalen und der EU-Ebene zu verbessern. Die zu gestaltende Grundrechte-Architektur in der Europäischen Union orientiert sich an der Notwendigkeit, Grundrechte insbesondere auf nationaler Ebene noch wirksamer zu schützen und zu fördern und entsprechende Mechanismen auch auf europäischer und auf internationaler Ebene zu schaffen.

Dieser Bericht analysiert die entscheidende Rolle der Datenschutzbehörden in Bezug auf das Grundrecht des Datenschutzes und bewertet die Effizienz, das Funktionieren und die Unabhängigkeit der Datenschutzbehörden. Der Bericht wird zur rechten Zeit vorgelegt, da der Datenschutz in der EU gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union inzwischen den Status eines eigenen Grundrechts erlangt hat, das zwar mit dem Recht auf Achtung des Privat- und Familienlebens im Zusammenhang steht, aber dennoch ein eigenständiges Grundrecht darstellt. Gleichzeitig wird der Datenschutz zunehmend zu einem Schlüsselbereich der EU-Politik, und in vielen Mitgliedstaaten war die EU maßgeblich an der Entwicklung entsprechender Rechtsvorschriften beteiligt.

Viviane Reding, das für Justiz, Grundrechte und Bürgerschaft zuständige Mitglied der Europäischen Kommission, hat kürzlich in einer schriftlichen Erklärung für das Europäische Parlament die besondere Bedeutung des Datenschutzes für die EU hervorgehoben. Sie sagte, sie sei „fest davon überzeugt, dass die Bürgerinnen und Bürger nie Vertrauen zu Europa gewinnen werden, wenn wir nicht garantieren können, dass personenbezogene Daten gegen Missbrauch geschützt sind, und dass sie über die Verarbeitung ihrer Daten selbst bestimmen." Diesem Gedanken folgend legt die FRA diesen Bericht vor.

Morten Kjaerum
Direktor

Zusammenfassung

Weltweite Vorreiterrolle der EU beim Schutz des Grundrechts des Datenschutzes

Die EU hat in der Vergangenheit entscheidend zur Entwicklung und Einführung einzelstaatlicher Datenschutzgesetze und zur Einführung dieser in verschiedene Rechtssysteme der EU, in denen es vorher keine entsprechenden Rechtsvorschriften gab, beigetragen. Ein wichtiges Instrument in diesem Zusammenhang war die Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (im Folgenden die „Datenschutzrichtlinie").

In der Charta der Grundrechte der Europäischen Union – die gemäß dem neuen Artikel 6 des Vertrags über die Europäischen Union „rechtlich gleichrangig" mit den Verträgen ist – wird der Schutz personenbezogener Daten gemäß Artikel 8 als eigenes Grundrecht genannte, dass sich vom Recht auf Achtung des Privat- und Familienlebens gemäß Artikel 7 unterscheidet. Dieses Merkmal unterscheidet die Grundrechte-Charta von allen anderen wichtigen Menschenrechtsdokumenten, in denen der Schutz personenbezogener Daten überwiegend als Erweiterung des Rechts auf Privatsphäre behandelt wird.

Mit der Einbeziehung des Datenschutzes als eigenständiges Grundrecht trägt die EU der Bedeutung des technischen Fortschritts Rechnung, und möchte sicherstellen, dass dieser Fortschritt auch im Zusammenhang mit den Grundrechten berücksichtigt wird. Angesichts der unbestreitbaren Tatsache, dass unser Leben zunehmend durch den ständigen Austausch von Informationen bestimmt wird und wir einem ständigen Datenstrom ausgesetzt sind, gewinnt der Datenschutz an Bedeutung und rückt immer stärker ins Zentrum des politischen und institutionellen Systems. Diese Entwicklung zeigt sich besonders im Vergleich der EU-Charta mit der Europäischen Menschenrechtskonvention (EMRK) des Europarats aus dem Jahr 1950. Gemäß Artikel 8 der EMRK gilt: *„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."* Die EMRK sieht jedoch kein ausdrückliches und eigenständiges Recht auf Datenschutz vor. Vielmehr ergibt sich das Recht auf Datenschutz aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Straßburg als Bestandteil des Schutzes der Privatsphäre. Dagegen erkennt Artikel 8 der Charta der Grundrechte der Europäischen Union die zentrale Bedeutung und die Wichtigkeit an, die das Recht auf Datenschutz in unserer durch technische Entwicklungen geprägten Gesellschaft erlangt hat.

Diese vergleichende Untersuchung analysiert die gegenwärtigen Herausforderungen und beschreibt vielversprechende Praktiken im Zusammenhang mit dem Datenschutzsystem der EU.

Herausforderungen für das Datenschutzsystem der EU

Die Agentur der Europäischen Union für Grundrechte (FRA) hat die folgenden Herausforderungen für das Datenschutzsystem der EU ermittelt:

Defizite bei den Datenschutzbehörden

Auf struktureller Ebene stellt die mangelnde Unabhängigkeit verschiedener Datenschutzbehörden ein erhebliches Problem dar. In verschiedenen Mitgliedstaaten bestehen Bedenken dahingehend, dass die Mitarbeiter[1] von Datenschutzbehörden ihre Aufgaben möglicherweise nicht effizient und in völliger Unabhängigkeit erfüllen können. Auf funktionaler Ebene sehen sich mehrere Datenschutzbehörden mit einem Mangel an personellen und angemessenen finanziellen Ressourcen konfrontiert. Auf operativer Ebene wiederum stellen die begrenzten Befugnisse mehrerer Kontrollstellen ein größeres Problem dar. So sind in manchen Mitgliedstaaten die Datenschutzbehörden im Hinblick auf Verarbeitungsvorgänge nicht in vollem Umfang mit Untersuchungs-, Einwirkungs-, Beratungs- und Befassungsbefugnissen ausgestattet.

Mangelnde Durchsetzung des Datenschutzsystems

In einigen Mitgliedstaaten sind die Strafverfolgung und Sanktionen bei Verstößen gegen das Datenschutzgesetz begrenzt oder nicht existent. In den nationalen Rechtssystemen verschiedener Mitgliedstaaten schließt das Zusammenwirken mehrerer Faktoren die Geltendmachung von Schadenersatzansprüchen aufgrund der Verletzung von Datenschutzrechten praktisch aus. Zu diesen Faktoren zählen etwa die Handhabung der Beweislast, Schwierigkeiten bei der Quantifizierung des Schadens sowie die kaum vorhandene Unterstützung seitens der Kontrollstellen, die zumeist mit proaktiven, „weichen" Tätigkeiten wie Registrierung und Sensibilisierung beschäftigt sind. Die Mitgliedstaaten konzentrieren sich eher auf „weiche" Methoden zur Gewährleistung der Einhaltung der Datenschutzbestimmungen, anstatt „harte" Instrumente durchzusetzen, mit deren Hilfe Urheber von Verletzungen des Rechts auf Datenschutz ermittelt, bestraft und zu Schadensersatzleistungen für Opfer verpflichtet werden können. Vielversprechende Praktiken der Zusammenarbeit von Datenschutzbehörden und anderen Behörden zur Stärkung der Ermittlungstätigkeit wurden in einigen Mitgliedstaaten ausgemacht.

1 Im Interesse einer besseren Lesbarkeit wird auf die durchgehende Nennung der männlichen und weiblichen Form verzichtet, obwohl selbstverständlich immer beide Geschlechter gemeint sind.

Rechtsbewusstsein

Während der Untersuchungen für diesen Bericht konnte die FRA in zwölf der 27 Mitgliedstaaten der EU feststellen, dass einzelstaatliche Umfragen durchgeführt worden waren. Diese Umfragen waren teilweise von den nationalen Datenschutzbehörden in Auftrag gegeben worden. Die gestellten Fragen, die Anzahl der Befragten, die Methodik und die Endergebnisse sind äußerst unterschiedlich und lassen sich nicht immer vergleichen. Die bloße Durchführung dieser einzelstaatlichen Umfragen ist jedoch schon als vielversprechende Praktik zu bewerten. Im Februar 2008 wurden zwei Eurobarometer-Umfragen veröffentlicht. Die wichtigsten Erkenntnisse dieser Umfragen lauteten, dass die meisten EU-Bürger Vorbehalte hinsichtlich des Datenschutzes hatten, und dass die nationalen Datenschutzbehörden den meisten EU-Bürgern relativ unbekannt sind.

Mangelnder Datenschutz in der dritten Säule der EU

Die wichtigste Beschränkung, der sich die EU derzeit bei der Gewährleistung eines wirksamen und umfassenden Datenschutzes gegenübersieht, resultiert aus der früheren, auf der Unterteilung in Säulen basierenden Verfassungsarchitektur der EU. In der früheren ersten Säule der EU ist der Datenschutz zwar hoch entwickelt, in der früheren dritten Säule kann das Datenschutzsystem jedoch nicht als zufrieden stellend betrachtet werden. Bislang umfasste die frühere dritte Säule der EU Bereiche wie die polizeiliche Zusammenarbeit, die Terrorismusbekämpfung und strafrechtliche Fragen, in denen die Notwendigkeit des Datenschutzes besonders wichtig ist. Mit dem Vertrag von Lissabon kann diese Lücke leichter geschlossen werden. In Erklärung Nr. 21 zum Vertrag von Lissabon heißt es, dass es sich aufgrund des spezifischen Charakters der Bereiche justizielle Zusammenarbeit in Strafsachen und polizeiliche Zusammenarbeit als erforderlich erweisen könnte, in diesen Bereichen spezifische Vorschriften zum Schutz personenbezogener Daten und zum freien Datenverkehr zu erlassen.

Ausnahmen vom Datenschutz für Sicherheit und Landesverteidigung

Artikel 13 Absatz 1 der Datenschutzrichtlinie sieht umfassende Ausnahmen und Beschränkungen im Zusammenhang mit der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates (wenn die Verarbeitung die staatliche Sicherheit berührt, einschließlich seines wirtschaftlichen Wohls) sowie staatlicher Maßnahmen im Bereich des Strafrechts vor. Hinsichtlich der Reichweite dieser Ausnahmen und Beschränkungen fehlt es an Klarheit. In verschiedenen Mitgliedstaaten sind diese Bereiche insgesamt vom Schutzumfang des Datenschutzrechts ausgenommen. Dass somit ein erheblicher Bereich nicht dem Datenschutz unterliegt, hat möglicherweise schwerwiegende Folgen für den Schutz der Grundrechte. Erklärung Nr. 20 zum Vertrag von Lissabon besagt, dass immer dann, wenn Bestimmungen über den Schutz personenbezogener Daten zu erlassen sind, die direkte Auswirkungen auf die nationale Sicherheit haben könnten, die besonderen Umstände im jeweiligen Fall „gebührend" zu berücksichtigen sind.

Neue Technologien als Herausforderung

Anhaltende und neue technologische Entwicklungen gehen mit neuen Herausforderungen einher, die dringend angegangen werden müssen. Die Videoüberwachung im öffentlichen Raum und im Arbeitsumfeld ist vielfach üblich; die entsprechende Anpassung des Rechtsrahmens hinkt jedoch nach. Als Beispiel zeigt der Bericht auf, dass CCTV-Kameras in manchen Mitgliedstaaten in der Praxis häufig nicht registriert bzw. überwacht werden.

Vielversprechende Praktiken

Die meisten von der Agentur der Europäischen Union für Grundrechte ermittelten vielversprechenden Praktiken, die zu einem wirksamen Datenschutz beitragen, sind Sensibilisierungsmaßnahmen, die in manchen Mitgliedstaaten von nationalen Datenschutzbehörden durchgeführt werden, wie etwa die Veranstaltung spezieller Kurse, Seminare und Vorträge, die Bereitstellung von Bildungsprogrammen, die Herausgabe von Leitfäden und Empfehlungen, die Organisation von Informations- und Beratungskampagnen usw. Andere vielversprechende Praktiken betreffen die institutionelle Stellung der Kontrollstellen, d. h. den Grad ihrer Unabhängigkeit, die Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, die aktive Mitwirkung an der Ausarbeitung und Vorlage von Verhaltenskodizes sowie die Zusammenarbeit mit einzelstaatlichen Einrichtungen, Nichtregierungsorganisationen (NRO) und Datenschutzbehörden anderer Mitgliedstaaten.

Gutachten

Auf der Grundlage der in diesem Bericht erläuterten Ergebnisse und vergleichenden Analysen hat die Agentur der Europäischen Union für Grundrechte folgende Gutachten formuliert:

Erweiterung des Datenschutzsystems der EU

Mit dem Vertrag von Lissabon wurde die Säulenstruktur der EU abgeschafft; dadurch kann die EU ihr Datenschutzsystem, das gegenwärtig nur im Zusammenhang mit der früheren ersten Säule besteht, nun auf alle (früheren) Säulen der EU ausdehnen. Einschränkungen des Datenschutzes aus Gründen der Sicherheit, zu Verteidigungszwecken oder zu sonstigen rechtmäßigen Zwecken sind gemäß Artikel 52 der Grundrechte-Charta der EU weiterhin möglich; diese Einschränkungen müssen jedoch gesetzlich geregelt sein und den Kerngedanken des Rechts auf den Schutz personenbezogener Daten sowie den Erfordernissen der Notwendigkeit und der Verhältnismäßigkeit gerecht werden. Dass bestimmte Bereiche vollständig aus dem Recht auf Datenschutz ausgenommen werden, ist im Hinblick auf die Wahrung von Grundrechten problematisch und zu vermeiden.

Gewährleistung einer wirksamen Durchsetzung

In diesem Bericht werden die mangelnde Personalausstattung und unzureichende Finanzmittel als problematisch bewertet. Auf operativer Ebene stellen die begrenzten Befugnisse mehrerer Datenschutzbehörden ein großes Problem dar. In manchen Mitgliedstaaten sind die Datenschutzbehörden nicht in vollem Umfang mit Untersuchungs-, Einwirkungs-, Beratungs- und Befassungsbefugnissen ausgestattet. Die Datenschutzbehörden müssen über die erforderlichen Ressourcen und Befugnisse verfügen und die nötige Unabhängigkeit besitzen, um zur wirksamen Durchsetzung des Datenschutzsystems beitragen zu können.

Garantien für eine wirksame Durchsetzung des Datenschutzes sowie für effiziente Untersuchungen und die zuverlässige Erkennung von Zuwiderhandlungen sind entscheidend, um eine abschreckende Wirkung zu erzielen und Verstöße gegen den Datenschutz zu unterbinden. Eine deutlich nachdrücklichere Durchsetzung würde auch dazu beitragen, die Bevölkerung davon zu überzeugen, dass datenschutzrechtliche Bedenken ernst genommen werden. Die ausschließliche Konzentration auf „weiche" Maßnahmen und die Vermeidung „harter" Maßnahmen untergräbt die Glaubwürdigkeit des gesamten Systems. In diesem Sinne würde eine wirksame Durchsetzung auch zur stärkeren Aufklärung der Bevölkerung über die bestehenden Datenschutzrechte beitragen. Die Datenschutzbehörden sollten eine wichtige Rolle bei der Durchsetzung des Datenschutzsystems spielen; dazu sollte ihnen entweder die Befugnis zur unmittelbaren Verhängung von Sanktionen oder die Befugnis zur Einleitung von Verfahren übertragen werden, in denen Sanktionen von Amts wegen verhängt werden können. Dies würde die Autorität und die Glaubwürdigkeit der Behörden stärken.

Nationale Datenschutzbehörden als unabhängige Hüterinnen

Auf struktureller Ebene stellt die mangelnde Unabhängigkeit verschiedener Datenschutzbehörden ein erhebliches Problem dar. In verschiedenen Ländern geben jedoch normative oder praktische Hindernisse Anlass zu Bedenken hinsichtlich der tatsächlichen Unabhängigkeit nationaler Datenschutzbehörden von der staatlichen Politik. Die erforderliche Unabhängigkeit wird in erster Linie durch das Verfahren zur Benennung und Abberufung von Mitarbeitern der Datenschutzbehörden gewährleistet. Die Kontrolle über Finanzmittel ist ein zweiter maßgeblicher Punkt bei der Sicherstellung der Unabhängigkeit von Überwachungsbehörden.

In verschiedenen Mitgliedstaaten werden Datenschutzbeauftragte unter Ausschluss der parlamentarischen Opposition direkt von der Regierung benannt. Dies gab in mehreren Fällen Anlass für ernsthafte Bedenken hinsichtlich der tatsächlichen Unabhängigkeit der betreffenden Datenschutzbehörden. Ähnliche Probleme können sich in Ländern ergeben, in denen die Überwachungsbehörde dem Justizministerium zugeordnet ist. Andere Staaten sehen schließlich ein kombiniertes Verfahren zur Benennung der Mitarbeiter der nationalen Datenschutzbehörden vor, an dem die Exekutive, die Legislative und die Judikative bzw. sonstige organisierte Gruppen der Gesellschaft gleichzeitig beteiligt sind. Verschiedentlich muss sichergestellt werden, dass die Regierung nicht de facto direkt oder indirekt die Mehrheit der benannten Mitarbeiter kontrolliert und damit letztlich den Zweck eines pluralistischen Benennungsverfahrens unterläuft.

Die Datenschutzrichtlinie 95/46/EG sieht vor, dass die Datenschutzbehörden „die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit" wahrnehmen (Artikel 28 Absatz 1 der Datenschutzrichtlinie). Diese „Unabhängigkeit" wird allerdings nicht näher spezifiziert. Die in der Richtlinie vorgesehenen Garantien der Unabhängigkeit sollten im Einzelnen spezifiziert werden, um eine wirksame Unabhängigkeit der Datenschutzbehörden auch in der Praxis gewährleisten zu können. Daher sollte in einer künftigen Änderung der Richtlinie auf die so genannten „Pariser Grundsätze" und auf sonstige verfügbare Normen Bezug genommen werden, um den Begriff der Unabhängigkeit umfassender zu definieren.

Nationale Datenschutzbehörden als Bestandteil der sich herausbildenden Grundrechte-Architektur der EU

Im Rahmen dieser im Aufbau befindlichen Grundrechte-Architektur der EU sollten die Datenschutzbehörden eine engere Zusammenarbeit und stärkere Synergien mit anderen Hütern von Grundrechten (z. B. nationalen Menschenrechtseinrichtungen oder Gleichbehandlungsstellen) fördern. Ein Beitrag der EU zu einer besseren Abstimmung und zur besseren Nutzung von Synergien könnte darin bestehen, in Artikel 28 der Datenschutzrichtlinie 95/46/EG einen Zusatz aufzunehmen, der den Mitgliedstaaten die Möglichkeit einräumen würde, durch entsprechende Rechtsvorschriften

vorzusehen, dass die jeweiligen nationalen Datenschutzbehörden tatsächlich zu einer Spezialabteilung der nationalen Menschenrechtseinrichtungen würden. (Ein interessantes Beispiel mit ähnlicher Wirkung in diesem Zusammenhang ist Artikel 13 der Richtlinie 2000/43/EG des Rates.)

Nationale Datenschutzbehörden als wirksame Zentralstellen

Die Datenschutzbehörden tragen maßgeblich zu einem wirksamen Datenschutz bei. Sie dienen als niederschwellige Zugangsstellen für einen wirksamen Datenschutz für Bürger und andere Personen. Sie sollten nicht nur die Bereiche abdecken, die früher unter die erste Säule der EU fielen (wie gegenwärtig in einigen Mitgliedstaaten der Fall), sondern auch als zentrale Anlaufstellen für alle Datenschutzbelange von Bürgern und anderen Personen ausgelegt sein; dabei sollten auch Bereiche abgedeckt sein, die früher im Rahmen der dritten Säule der EU erfasst wurden. Eine übermäßig große Anzahl an Datenschutzorganen und -stellen wäre für eine Sensibilisierung der Bürger für die Existenz solcher Stellen nicht förderlich. Zudem führt eine Vielzahl von Organen zu Unübersichtlichkeit und unnötiger Komplexität.

Rechtsbewusstsein

Im Februar 2008 wurden zwei Eurobarometer-Umfragen veröffentlicht. Die wichtigsten Ergebnisse dieser Umfragen waren, dass die meisten EU-Bürger Vorbehalte hinsichtlich des Datenschutzes hatten, und dass die nationalen Datenschutzbehörden den meisten EU-Bürgern relativ unbekannt waren.

Die Datenschutzbehörden sollten besondere Aufmerksamkeit auf die Entwicklung ihres öffentlichen Profils als unabhängige Hüter des Grundrechts auf Datenschutz verwenden und sich um größere Präsenz und eine stärkere Sensibilisierung für ihre Aufgabe bemühen.

1 Einleitung

In Artikel 8 der Grundrechte-Charta der EU ist das Grundrecht auf den Schutz personenbezogener Daten verankert. Der Datenschutz ist auch eines der entscheidenden Gebiete im Bereich der Grundrechte, in denen die EU die Zuständigkeit zur Erlassung von Rechtsvorschriften besitzt.

Die FRA hat diesen Bericht mit Unterstützung von Fralex, einer Gruppe von Rechtsexperten der Agentur, erstellt. Nationale Teams von Fralex haben auf der Grundlage allgemeiner Leitlinien der FRA 27 nationale Studien und eine Studie auf EU- bzw. internationaler Ebene erstellt. Dieser Bericht wurde auf der Grundlage dieser Studien verfasst. Die nationalen Studien stammen vom Februar 2009. Die so genannte „Artikel-29-Datenschutzgruppe" wurde zum Entwurf des vergleichenden Berichts konsultiert und hat Gutachten übermittelt.

Dieser Bericht steht in engem Zusammenhang mit den folgenden Projekten und Veröffentlichungen der FRA:

- FRA-Gutachten zu PNR-Daten (*Passenger Name Record*, PNR), Oktober 2008[2]
- Beitrag der FRA zu einer Konsultation der Europäischen Kommission zu Körperscannern, Januar 2009[3]
- *National Human Rights Institutions in the EU Member States – Strengthening the fundamental rights architecture in the EU I* (Nationale Menschenrechtsinstitutionen in den Mitgliedstaaten der EU – Stärkung der Grundrechte-Architektur in der EU I), 2010[4]
- Bericht der Reihe *„Daten kurz gefasst": Rechtsbewusstsein und Gleichbehandlungsstellen – Stärkung der Grundrechte-Architektur in der EU III* 2010[5]

In diesem Bericht werden die internationalen Rechtsstandards zum Datenschutz erläutert. Anschließend werden der Datenschutz im EU-Recht und die Änderungen durch den Vertrag von Lissabon analysiert. Danach folgt eine vergleichende Übersicht über Datenschutzeinrichtungen und -verfahren in den Mitgliedstaaten. Der Bericht schließt mit einer Beschreibung ermittelter Defizite und vielversprechender Praktiken.

2 Siehe: http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf (Alle aufgeführten links wurden frühestens am 24.9.2008 aufgerufen).
3 Nicht veröffentlichter Beitrag der Agentur der Europäischen Union für Grundrechte zu einer Konsultation der Europäischen Kommission.
4 Siehe: http://fra.europa.eu/.
5 Siehe: http://fra.europa.eu/eu-midis.

2 Grundrechtestandards in Bezug auf den Datenschutz

Der Schutz personenbezogener Daten wird in verschiedenen europäischen und internationalen Verträgen als Grundrecht anerkannt und in der Rechtsprechung internationaler und regionaler Gerichte ausgelegt.

2.1. Datenschutz im Rahmen der Vereinten Nationen

Das Grundrecht auf den Schutz personenbezogener Daten wird auch auf globaler Ebene in verschiedenen unter der Federführung der Vereinten Nationen erlassenen Menschenrechtsinstrumenten anerkannt, überwiegend als Erweiterung des Rechts auf Privatsphäre.[6]

Insbesondere im Internationalen Pakt über bürgerliche und politische Rechte (IPBPR), der von vier Fünftel der Staaten der Welt ratifiziert wurde, ist in Artikel 17 das Recht auf Schutz von Privatsphäre, Familie, Wohnung und Schriftverkehr wie folgt verankert: „1. Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. 2. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen." Der Allgemeine Kommentar Nr. 16 zu Artikel 17 IPBPR behandelt ausdrücklich das Recht auf den Schutz personenbezogener Daten.[7] Er sieht insbesondere Folgendes vor: „Die Sammlung und Aufbewahrung personenbezogener Informationen in Computern, Datenbanken und anderen Geräten, sei es durch staatliche Behörden, Privatpersonen oder nichtstaatliche Körperschaften, muss gesetzlich geregelt werden. Von den Staaten müssen wirksame Maßnahmen getroffen werden, um sicherzustellen, dass Informationen über das Privatleben einer Person nicht in die Hände von Personen gelangen, die nicht gesetzlich befugt sind, solche Informationen zu erhalten, zu verarbeiten und zu nutzen, und um zu gewährleisten, dass solche Informationen niemals für Zwecke verwendet werden, die mit dem Pakt unvereinbar sind. Um einen möglichst wirksamen Schutz des Privatlebens zu erreichen, sollte jede natürliche Person das Recht haben, in verständlicher Form Auskunft darüber zu erhalten, ob und, falls ja, welche personenbezogenen Daten in automatisierten Dateien zu welchen Zwecken gespeichert sind. Jede natürliche Person sollte auch feststellen können, welche Behörden, Privatpersonen oder privaten Körperschaften ihre Dateien kontrollieren oder kontrollieren können. Enthalten derartige Dateien fehlerhafte personenbezogene Daten, oder wurden diese Daten unter Verstoß gegen die gesetzlichen Bestimmungen erhoben oder verarbeitet, sollte jede natürliche Person das Recht haben, eine Berichtigung oder Löschung der Daten zu verlangen." Darüber hinaus wird in der Rechtsprechung des Menschenrechtsausschusses ausgeführt, dass der Begriff des Privatlebens im Allgemeinen Kommentar Nr. 16 nicht eng ausgelegt werden sollte.[8]

Ein weiteres Instrument von besonderer Bedeutung sind die von der Generalversammlung der Vereinten Nationen am 14. Dezember 1990 angenommenen Leitlinien für die Regelung der personenbezogenen Datenbanken.[9] Die Leitlinien enthalten bestimmte Grundsätze in Bezug auf die Mindestgarantien, die mit einzelstaatlichen Rechtsvorschriften zum Schutz personenbezogener Daten begründet werden sollten. Sie sehen den Grundsatz der Rechtmäßigkeit und Fairness der Erhebung und Verarbeitung personenbezogener Daten, die sachliche Richtigkeit, die Zweckbindung, den Zugang betroffener Personen, die Nichtdiskriminierung und die Sicherheit der Datenbanken vor. Abweichungen von diesen Grundsätzen sind diesen Leitlinien zufolge nur dann zulässig, wenn sie zum Schutz der nationalen Sicherheit, der öffentlichen Ordnung, der öffentlichen Gesundheit oder der Moral sowie, unter anderem, zum Schutz der Rechte und Freiheiten anderer, insbesondere verfolgter Personen (humanitäre Klausel), notwendig sind, vorausgesetzt, dass derartige Abweichungen in einem Gesetz oder einer in Übereinstimmung mit dem internen Rechtssystem veröffentlichten gleichwertigen Vorschrift festgelegt sind, in dem/der ausdrücklich die Grenzen dieser Abweichungen dargelegt und angemessene Sicherheitsvorkehrungen festgeschrieben werden. Ausnahmen vom Grundsatz der Nichtdiskriminierung unterliegen gemäß diesen Leitlinien noch stärkeren Beschränkungen; sie sind nur innerhalb der Grenzen zulässig, die durch die Internationale Charta der Menschenrechte und die anderen einschlägigen Instrumente im Bereich des Schutzes der Menschenrechte und der Verhütung von Diskriminierung festgelegt wurden. Den Leitlinien zufolge sollten die dort verankerten Grundsätze zunächst für alle öffentlichen und privaten automatisch verarbeiteten Dateien gelten und gegebenenfalls mit erforderlichen Ergänzungen in entsprechend angepasster Form auch auf manuell verarbeitete Dateien Anwendung finden. Durch eine ebenfalls fakultative Sonderregelung könnten die Grundsätze im Ganzen oder in Teilen auf Dateien über juristische Personen ausgedehnt werden, insbesondere wenn diese Dateien bestimmte Informationen über natürliche Personen enthalten.

Das Grundrecht auf Schutz personenbezogener Daten wird auch auf regionaler Ebene in verschiedenen Menschenrechtsinstrumenten außerhalb Europas anerkannt, überwiegend als Erweiterung des Rechts auf Privatsphäre.[10]

2.2. Datenschutz im Rahmen des Europarats

Auf regionaler Ebene beruht der Standard für den Schutz personenbezogener Daten auf mehreren Übereinkommen, die unter der Ägide des Europarats angenommen wurden. Die meisten dieser Instrumente

6 Artikel 12 der Allgemeinen Erklärung der Menschenrechte schützt das Recht auf Privatleben.

7 Siehe Human Rights Committee, *General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies*, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), Randnummer 10.

8 Siehe beispielsweise Rechtssache *Coeriel & Aurik/Niederlande* (1994), Beschw.-Nr. 453 / 1991.

9 „Guidelines for the Regulation of Computerized Personal Data Files", angenommen von der Generalversammlung durch Resolution 45/95 vom 14. Dezember 1990.

10 Das Recht auf Privatleben findet sich in Artikel 12 der Allgemeinen Erklärung der Menschenrechte, in Artikel V der Amerikanischen Deklaration der Rechte und Pflichten des Menschen aus dem Jahr 1948 und in Artikel 11 der Amerikanischen Menschenrechtskonvention aus dem Jahr 1969. Die Afrikanische Charta der Menschenrechte und der Rechte der Völker aus dem Jahr 1981 enthält keine ausdrückliche Anerkennung des Rechtes auf Privatsphäre.

wurden von allen EU-Mitgliedstaaten ratifiziert und teilweise in den einzelstaatlichen Rechtssystemen als Verfassungsnormen eingeführt.

Der bedeutendste einschlägige Rechtsakt des Europarats – die von allen Mitgliedstaaten der EU ratifizierte Europäische Menschenrechtskonvention (EMRK) – enthält keinen expliziten Verweis auf den Schutz personenbezogener Daten. Die umfangreiche Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) belegt jedoch, dass Artikel 8 EMRK, der ausdrücklich das Recht auf Achtung des Privat- und Familienlebens anerkennt, das Recht auf Datenschutz umfasst; dort heißt es: „1. Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. 2. Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist".

Im Zusammenhang mit dem Europarat wird das Grundrecht auf den Schutz personenbezogener Daten ausdrücklich auch im Übereinkommen aus dem Jahr 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (auch als „Übereinkommen 108" bezeichnet)[11] anerkannt; dieses Übereinkommen wurde von allen Mitgliedstaaten der EU ratifiziert. Das Übereinkommen verpflichtet die Vertragsstaaten, in ihrem jeweiligen Hoheitsgebiet ungeachtet der Staatsangehörigkeit oder des Wohnorts für jeden sicherzustellen, dass die persönlichen Rechte und Grundfreiheiten, insbesondere das Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden („Datenschutz"). Das Übereinkommen ist auf automatisierte Dateien und die automatische Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich anwendbar. Es enthält eine Reihe von Grundsätzen zur Verarbeitung von Daten und zur Qualität der Daten (insbesondere die Forderung, dass die Daten dem jeweiligen Zweck angemessen und erheblich sein müssen und nicht über das erforderliche Maß hinausgehen dürfen (Grundsatz der Verhältnismäßigkeit), zur sachlichen Richtigkeit von Daten, zur Vertraulichkeit sensibler Daten, zur Unterrichtung der betroffenen Person und zum Recht der betroffenen Person auf Zugang zu den gespeicherten Daten und Berichtigung der Daten. Allerdings stützt sich das Übereinkommen generell auf relativ vage und allgemeine Formulierungen und ist nicht notwendigerweise unmittelbar anwendbar, sondern schreibt die Annahme von Durchführungsmaßnahmen durch die Vertragsstaaten vor. Daher können sich natürliche Personen vor Gericht nicht unmittelbar auf dieses Übereinkommen berufen. Zudem enthält das Übereinkommen weit reichende Ausnahmeregelungen; unter anderem können die Vertragsparteien von den Datenschutzbestimmungen abweichen, wenn eine solche Abweichung durch das innerstaatliche Recht der jeweiligen Vertragspartei gedeckt und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist.

Durch das Übereinkommen 108 wird ferner ein Beratender Ausschuss (T-PD) eingesetzt, der für die Auslegung der Bestimmungen sowie für die Verbesserung der Umsetzung des Übereinkommens zuständig ist; an diesem Beratenden Ausschuss sind Vertreter der Vertragsparteien des Übereinkommens sowie Beobachter aus anderen Staaten (Mitgliedstaaten oder Nichtmitgliedstaaten) und internationalen Organisationen beteiligt. Dieser Ausschuss nahm ein noch nicht durch alle EU-Mitgliedstaaten ratifiziertes Zusatzprotokoll zu dem Übereinkommen betreffend die Kontrollbehörden und den grenzüberschreitenden Datenverkehr (2001) an, durch das die Kontrollbehörden gestärkt werden und die Übermittlung personenbezogener Daten an Staaten oder Organisationen, die kein angemessenes Schutzniveau gewährleisten, untersagt wird.

Ein weiterer wichtiger Rechtsetzungsakt im Kontext des Europarats ist das Übereinkommen über Menschenrechte und Biomedizin (1997),[12] das allerdings noch nicht von allen Mitgliedstaaten der EU ratifiziert wurde. Artikel 10 dieses Übereinkommens bekräftigt erneut den in Artikel 8 EMRK geschützten und im Übereinkommen 108 wiederholten Grundsatz: „1. Jeder hat das Recht auf Wahrung der Privatsphäre in Bezug auf Angaben über seine Gesundheit. 2. Jeder hat das Recht auf Auskunft in Bezug auf alle über seine Gesundheit gesammelten Angaben. Will jemand jedoch keine Kenntnis erhalten, so ist dieser Wunsch zu respektieren. 3. Die Rechtsordnung kann vorsehen, dass in Ausnahmefällen die Rechte nach Absatz 2 im Interesse des Patienten eingeschränkt werden können". Zudem stellen nach Artikel 6 des Übereinkommens über Menschenrechte und Biomedizin die Gesundheit betreffende personenbezogene Daten eine besondere Kategorie von Daten dar, die als solche Sonderregeln unterliegen. Das Übereinkommen gestattet jedoch gewisse Einschränkungen des Rechts auf Privatsphäre, beispielsweise in Fällen, in denen eine Justizbehörde den Urheber einer Straftat identifizieren muss (auf der Verhinderung von Straftaten basierende Ausnahme) oder zur Ermittlung des Abstammungsverhältnisses (auf dem Schutz der Rechte anderer basierende Ausnahme).

Abschließend muss erwähnt werden, dass der Europarat die Grundsätze des Schutzes der personenbezogenen Daten natürlicher Personen auch in Empfehlungen und Resolutionen weiter ausgeführt hat. Diese Instrumente werden einstimmig vom Ministerausschuss angenommen; sie sind zwar nicht rechtlich bindend, enthalten aber Bezugsstandards für alle Mitgliedstaaten. Seit 1972 hat der Europarat zahlreiche Empfehlungen und Entschließungen in Bezug auf Datenschutzfragen angenommen.[13]

In diesem Zusammenhang verdient die Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich besondere Erwähnung, da sie durch die Gewährleistung des Schutzes sensibler personenbezogener Daten noch über das „Übereinkommen 108" hinausgeht.[14] Nach Grundsatz 2.4 der Grundsätze im Anhang zu dieser Empfehlung sind zu untersagen: die Sammlung von Daten über natürliche Personen allein aufgrund der Tatsache, dass sie einer bestimmten Rasse angehören, bestimmte religiöse Überzeugungen vertreten, ein bestimmtes sexuelles Verhalten zeigen oder bestimmte politische Meinungen vertreten beziehungsweise bestimmten Bewegungen oder Organisationen angehören, die nicht per Gesetz verboten sind. Die Sammlung von Daten betreffend diese Aspekte darf nur erfolgen, wenn sie für die Zwecke einer bestimmten

11 Siehe: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

12 Siehe: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CL=ENG.

13 Siehe Empfehlung Nr. R(95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste, insbesondere der Telefondienste (7. Februar 1995), Empfehlung Nr. R (97) 5 über den Schutz medizinischer Daten (13. Februar 1997), Empfehlung Nr. R (97) 18 über den Schutz der personenbezogenen Daten, die für statistische Zwecke erhoben und verarbeitet werden (30. September 1997), Empfehlung Nr. R (99) 5 über den Schutz des Privatlebens im Internet (23. Februar 1999) und Empfehlung Nr. R (2002) 9 über den Schutz von zu Versicherungszwecken erhobenen und verarbeiteten personenbezogenen Daten (18. September 2002).

14 Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich (17. September 1987).

Untersuchung absolut notwendig ist. Im Anhang zu dieser Empfehlung wird ferner eine Reihe weiterer Grundsätze festgelegt, mit denen die Sammlung, Speicherung, Verwendung, Übermittlung und Erhaltung personenbezogener Daten durch die Polizei geregelt werden soll. Der Präambel zufolge erkennt die Empfehlung die Notwendigkeit an, einen Mittelweg zwischen den Interessen des Einzelnen und seinem Recht auf Privatsphäre einerseits und den Interessen der Gesellschaft in Bezug auf die Verhinderung und Niederschlagung strafbarer Handlungen und die Aufrechterhaltung der öffentlichen Ordnung andererseits zu finden. Für diese Zwecke wird die einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte berücksichtigt.

In der Rechtsprechung des EGMR zum Schutz der Privatsphäre und des Privatlebens wurden verschiedentlich auch Fragen des Datenschutzes behandelt. Der EGMR hat in diesem Zusammenhang in Artikel 8 EMRK nicht nur negative Verpflichtungen für die Mitgliedstaaten (nämlich die Forderung des Verzichts auf Eingriffe in das Recht auf Privatsphäre) ermittelt, sondern auch auf positive Verpflichtungen hingewiesen, die den Erlass von Maßnahmen zur Sicherstellung der Achtung des Privatlebens auch im Bereich der Beziehungen von natürlichen Personen selbst („*the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves*") nach sich ziehen.[15]

In der Rechtssache *M.S./Schweden* machte der EGMR beispielsweise deutlich, dass der „Schutz personenbezogener Daten [...] von grundlegender Bedeutung für die Ausübung des durch Artikel 8 der Konvention garantierten Rechts auf Achtung des Privat- und Familienlebens" ist.[16] In der Rechtssache *Leander/Schweden* entschied der EGMR, dass die Speicherung von Informationen über das Privatleben einer natürlichen Person in einem Geheimdienstregister und die Freigabe dieser Informationen einen Eingriff in das durch Artikel 8 Absatz 1 garantierte Recht auf Achtung des Privatlebens darstelle.[17] Er betonte, dass der Gerichtshof in Anbetracht des Risikos, das ein System der geheimdienstlichen Überwachung zum Schutz der nationalen Sicherheit hinsichtlich der Untergrabung oder gar Zerstörung der Demokratie mit der Rechtfertigung ihrer Verteidigung darstelle, überzeugt sein müsse, dass angemessene und wirksame Garantien gegen Missbrauch vorhanden sind. In der Rechtssache *Z./Finnland* unterstrich der EGMR, dass der Schutz personenbezogener Daten, insbesondere medizinischer Daten, von grundlegender Bedeutung für die Ausübung des durch Artikel 8 der EMRK garantierten Rechts auf Achtung des Privat- und Familienlebens ist.[18] Er räumte jedoch ein, dass das Interesse an der Ermittlung und der Verfolgung einer Straftat sowie an der Öffentlichkeit von Gerichtsverfahren schwerer wiegen kann als das Interesse eines Patienten und der Gemeinschaft als Ganzes am Schutz medizinischer Daten, wenn nachgewiesen wurde, dass diesem Interesse eine übergeordnete Bedeutung zukommt.

In der Rechtssache *Rotaru/Rumänien* erkannte der EGMR ausdrücklich an, dass Artikel 8 EMRK die im Übereinkommen 108 verankerten Garantien im Bereich des Datenschutzes umfasst.[19] Er wiederholte den in der Rechtssache *Leander* vertretenen Grundsatz, dass die Speicherung von das Privatleben einer natürlichen Person betreffenden Informationen durch eine Behörde und die Nutzung dieser Informationen einen Eingriff in das Recht auf Achtung des Privatlebens darstellen, und führte ferner aus, dass ein solcher Eingriff auch bei Verweigerung der Möglichkeit zur Widerlegung der personenbezogenen Daten gegeben sei. In der Rechtssache *Amann/Schweiz* befand der Gerichtshof, dass eine von einer Behörde aufbewahrte Karte mit Daten über das Privatleben einer natürlichen Person ausreichte, um auf das Vorliegen eines Eingriffs in das Recht der Beschwerdeführerin auf Achtung ihres Privatlebens im Sinne von Artikel 8 zu schließen, ohne dass der Gerichtshof Vermutungen darüber anstellen musste, ob die gesammelten Informationen tatsächlich als sensible Daten zu bewerten waren.[20]

In der Rechtssache *K.U./Finnland* hat der EGMR kürzlich anerkannt, dass die einzelstaatlichen Gesetzgeber verpflichtet sind, einen Rahmen vorzusehen, um die Vertraulichkeit von Internet-Diensten mit der Verhinderung von Ordnungswidrigkeiten oder Straftaten und dem Schutz der Rechte und Freiheiten anderer in Einklang zu bringen. Da dieser Rahmen zum damaligen Zeitpunkt nicht vorhanden war, hatte Finnland nach Auffassung des EGMR das Recht auf Achtung des Privatlebens des Beschwerdeführers nicht geschützt, weil dem Erfordernis der Vertraulichkeit Vorrang vor dem physischen und moralischen Wohlergehen des Beschwerdeführers eingeräumt worden war; daher erkannte der EGMR auf einen Verstoß gegen Artikel 8.[21] In der Rechtssache *S. und Marper/Vereinigtes Königreich* urteilte der EGMR über die Rechtmäßigkeit der Aufbewahrung der Fingerabdrücke, Zellproben und DNA-Profile der Beschwerdeführer durch die britischen Behörden, nachdem die Strafverfahren gegen sie durch einen Freispruch bzw. ohne Verurteilung beendet wurden und obwohl die Beschwerdeführer die Vernichtung dieser Fingerabdrücke, Zellproben und DNA-Profile verlangt hatten. Der EGMR stellte fest, dass Zellproben zahlreiche sensible Informationen über eine natürliche Person enthalten, und urteilte daher, dass die Vorratsspeicherung von Zellproben und DNA-Profilen einen Eingriff in das Recht der Beschwerdeführer auf Achtung ihres Privatlebens im Sinne von Artikel 8 Absatz 1 darstellten; er führte weiter aus, dass es eine inakzeptable Aushöhlung des durch Artikel 8 gewährten Schutzes darstellen würde, wenn der Einsatz moderner wissenschaftlicher Verfahren im Strafrechtssystem um jeden Preis und ohne sorgfältige Abwägung der potenziellen Nutzaspekte des umfassenden Einsatzes solcher Verfahren gegen wichtige Interessen des Privatlebens zulässig wäre.[22]

In den drei französischen Rechtssachen aus dem Jahr 2009 wurde zwar einerseits die wesentliche Rolle des Schutzes personenbezogener Daten betont, die einer automatischen Verarbeitung unterzogen werden, insbesondere für polizeiliche Zwecke; andererseits stellte der EGMR aber auch fest, dass die Aufnahme der Kläger in die auf nationaler Ebene von der Polizei geführte Sexualstraftäter-Datenbank in der in diesem Fall gegebenen Form nicht im Widerspruch zu Artikel 8 stand.[23]

15 Siehe Rechtssache *X und Y/Niederlande*, Urteil vom 26. März 1985, Randnummer 23.
16 Siehe Urteil in der Rechtssache *M.S./Schweden* vom 27. August 1997.
17 Siehe Urteil in der Rechtssache *Leander/Schweden* vom 26. März 1987, Randnummer 48.
18 Siehe Urteil in der Rechtssache *Z./Finnland*, 25. Februar 1997, Randnummer 95.
19 Siehe Urteil in der Rechtssache *Rotaru/Rumänien* vom 4. Mai 2000, Randnummer 43.
20 Siehe Urteil in der Rechtssache *Amann/Schweiz* vom 16. Februar 2000, Randnummer 70.
21 Siehe Urteil in der Rechtssache *K. U./Finnland* vom 2. Dezember 2008.
22 Siehe Urteil in der Rechtssache *S. und Marper/Vereinigtes Königreich* vom 4. Dezember 2008.
23 Siehe Urteile in der Rechtssache *Bouchacourt/Frankreich*, *Gardel/Frankreich*, und *M.B./Frankreich* vom 17. Dezember 2009 (nicht endgültig).

3 Der Datenschutz im EU-Recht

Der Schutz personenbezogener Daten wird im primären EU-Verfassungsrecht als eigenständiges – von dem Recht auf Achtung des Privat- und Familienlebens unabhängiges, wenn auch mit ihm in Beziehung stehendes – Grundrecht anerkannt. Artikel 8 der Grundrechte-Charta der EU besagt: „1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. 2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. 3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."[24] Die Grundrechte-Charta der EU und die Verträge sind nach Artikel 6 des Vertrags über die Europäische Union „rechtlich gleichrangig".

In der EU-Datenschutzrichtlinie 95/46/EG werden personenbezogene Daten definiert als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann."[25]

Hinsichtlich der Behandlung des Schutzes personenbezogener Daten als eigenständiges Recht unterscheidet sich die Grundrechte-Charta der EU von anderen internationalen Dokumenten im Bereich der Menschenrechte, in denen zumeist kein spezifisches Recht auf Datenschutz erwähnt wird, sondern in denen der Schutz personenbezogener Daten überwiegend als Erweiterung des Rechts auf Privatsphäre behandelt wird.

3.1. Der Datenschutz in der früheren Gemeinschaftssäule

Die frühere, auf der Unterteilung in Säulen basierende Struktur der EU, die durch den Vertrag von Lissabon abgeschafft wurde, hatte tief greifenden Einfluss auf das Datenschutzsystem der EU. Innerhalb der einzelnen Säulen war der Datenschutz jeweils um gesonderte Gruppen von Instrumenten organisiert. Die frühere Unterteilung in Säulen führte zu Unsicherheiten darüber, welche Instrumente für spezifische Instanzen bei der Verarbeitung von Daten gelten.

Im Hinblick auf die frühere erste Säule der EU, d. h. die frühere Gemeinschaftssäule, besteht die wichtigste Zielsetzung darin, den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten in einem funktionierenden Binnenmarkt zu gewährleisten und zugleich die Grundrechte natürlicher Personen, insbesondere deren Recht auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten, zu schützen. Der Schutz personenbezogener Daten erfordert nicht nur, dass die Organe und Einrichtungen der EU und der Mitgliedstaaten auf illegale Eingriffe in die personenbezogenen Daten verzichten. Vielmehr besteht auch die ausdrückliche Verpflichtung, den Schutz personenbezogener Daten sicherzustellen.

Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachstehend die „Datenschutzrichtlinie") fungiert als wichtigstes Instrument der EU.[26] Dem EuGH zufolge übernahm die Datenschutzrichtlinie „auf Gemeinschaftsebene allgemeine Grundsätze (…), die in den Rechten der Mitgliedstaaten bereits anerkannt waren".[27] Das Datenschutzsystem der EU basiert auf den folgenden, in der Datenschutzrichtlinie verankerten Grundprinzipien: (i) Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen; (ii) die Zwecke der Verarbeitung müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden; (iii) [die Verarbeitung] hat den angestrebten Zwecken zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Zudem müssen die Daten sachlich richtig sein und, wenn nötig, auf den neuesten Stand gebracht werden; (iv) personenbezogene Daten können nur dann rechtmäßig verarbeitet werden, wenn bestimmte, in der Richtlinie festgelegte Kriterien für die Verarbeitung erfüllt sind (unter anderem, dass die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat). Für den Fall der Missachtung der Rechte der betroffenen Personen durch den Verantwortlichen der Verarbeitung ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen, die den betroffenen Zugang den Zugang zu den sie betreffenden personenbezogenen Daten und deren Berichtigung ermöglicht; (v) die Übermittlung personenbezogener Daten in Drittländer ist nur dann zulässig, wenn diese Länder ein angemessenes Schutzniveau gewährleisten; und (vi) die EU und ihre Mitgliedstaaten müssen eine oder mehrere unabhängige Stellen vorsehen, die mit der Gewährleistung der korrekten Anwendung der Vorschriften zum Schutz personenbezogener Daten beauftragt werden.

Die Datenschutzrichtlinie gilt für „jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten", bezeichnet als „Verarbeitung" von Daten. Nach Artikel 3 Absatz 1 gilt sie „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen". In Artikel 3 Absatz 2 werden die beiden Bereiche festgelegt, in denen die Richtlinie keine Anwendung findet: Erstens bei der Verarbeitung personenbezogener Daten, „die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich". Zweitens fällt auch die Verarbeitung von Daten, „die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird", nicht in den Anwendungsbereich dieser Richtlinie.

24 Ein Kommentar zu Artikel 8 der Charta ist zu finden unter: *Commentary of the Charter of Fundamental Rights of the EU, EU Network of Independent Experts on Fundamental Rights*, June 2006, siehe: http://ec.europa.eu/justice_home/doc_centre/rights/charter/docs/network_commentary_final%20_180706.pdf, S. 90.

25 Artikel 2 Buchstabe a der EU-Datenschutzrichtlinie 95/46/EG.

26 ABl. L 281 vom 23.11.1995, S. 31.

27 Siehe Rechtssache C- 369/98, *The Queen/Minister of Agriculture Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, Slg. 2000, S. I-6751, Randnummer 34.

Eine weitere wichtige Legislativmaßnahme der EU ist Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (die „Datenschutzrichtlinie für elektronische Kommunikation").[28] Mit dieser Richtlinie sollen die verschiedenen einzelstaatlichen Bestimmungen zum Schutz des Rechts auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation harmonisiert und gleichzeitig der freie Verkehr dieser Daten sowie elektronischer Kommunikationsgeräte und -dienste gewährleistet werden. Mit der EU-Richtlinie 2002/58/EG wird die Richtlinie 95/46/EG in Bezug auf die Verarbeitung personenbezogener Daten natürlicher Personen im Bereich der elektronischen Kommunikation näher spezifiziert und ergänzt und der Schutz der berechtigten Interessen von als Teilnehmer auftretenden juristischen Personen geregelt. Die Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des EG-Vertrags fallen.

Die Richtlinien 95/46/EG und 2002/58/EG sind an die Mitgliedstaaten gerichtet Dementsprechend gelten sie als solche nicht für die Organe und Einrichtungen der EU. Der Schutz personenbezogener Daten ist auch insoweit ein durch die Verträge gewährtes Recht, als Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union die für die Einrichtungen der Europäischen Union selbst geltenden Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr festlegt. Auf der Grundlage des früheren Artikels 286 EG-Vertrag (an dessen Stelle Artikel 16 AEUV getreten ist) wurde die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU und zum freien Datenverkehr erlassen.[29] Ziel der Verordnung ist der Schutz der Grundrechte und -freiheiten natürlicher Personen, insbesondere ihres Rechts auf Privatsphäre, bei der Verarbeitung personenbezogener Daten. Sie findet auf die Verarbeitung solcher Daten durch alle Organe und Einrichtungen der EU Anwendung, soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise den Anwendungsbereich des EU-Rechts betreffen. Durch diese Verordnung wurde im Jahr 2004 der Europäische Datenschutzbeauftragte (EDSB) eingesetzt.

Der EDSB setzt sich als unabhängige Kontrollinstanz für den Schutz personenbezogener Daten und der Privatsphäre ein und fördert vielversprechende Praktiken innerhalb der Organe und Einrichtungen der EU. Der EDSB überwacht die Verarbeitung personenbezogener Daten durch die Verwaltungen der EU, berät in Bezug auf für die Achtung der Privatsphäre maßgebliche Politiken und Rechtsvorschriften und arbeitet mit entsprechenden anderweitigen Stellen zusammen, um einen kohärenten Datenschutz zu gewährleisten. Im Rahmen dieser Überwachung soll sichergestellt werden, dass die Organe und Einrichtungen der EU personenbezogene Daten von EU-Bediensteten und anderen Personen rechtmäßig verarbeiten. Jedes Organ und jede Einrichtung sollte einen behördlichen Datenschutzbeauftragten (DSB) haben. Der DSB führt ein Register über alle Verarbeitungen und meldet dem EDSB Systeme mit spezifischen Risiken. Der EDSB prüft vorab, ob diese Systeme den Datenschutzerfordernissen entsprechen. Zudem hört er Beschwerden an und führt Untersuchungen durch. Somit überwacht der EDSB die Durchführung der Verordnung (EG) Nr. 45/2001 über den Datenschutz. Der EDSB berät die Europäische Kommission, das Europäische Parlament und den Rat zu Vorschlägen für neue Rechtsvorschriften und in vielen anderen Bereichen, die Auswirkungen auf den Datenschutz haben. Der EDSB arbeitet mit anderen Datenschutzinstanzen zusammen, um einen kohärenten Datenschutz in ganz Europa zu fördern. Die zentrale Plattform für die Zusammenarbeit mit einzelstaatlichen Kontrollinstanzen ist die Artikel-29-Datenschutzgruppe.[30]

Eine kürzlich angenommene Maßnahme ist die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden („Richtlinie über die Vorratsspeicherung von Daten").[31] Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder von Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter von ihnen erzeugter oder verarbeiteter Daten harmonisiert werden. Auf diese Weise soll sichergestellt werden, dass die Daten zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten (gemäß der Definition im einzelstaatlichen Recht des jeweiligen Mitgliedstaats) zur Verfügung stehen.

Der EuGH hat die Richtlinie 95/46/EG in zahlreichen Urteilen ausgelegt. Eine erste Reihe von Fragen, zu deren Beantwortung der Gerichtshof angerufen wurde, betraf den Anwendungsbereich dieser Richtlinie. In der Rechtssache *Österreichischer Rundfunk* wurde der Gerichtshof um eine Entscheidung darüber ersucht, ob die Datenschutzrichtlinie überhaupt auf die vom österreichischen Rechnungshof über die Gehälter der Arbeitnehmer bestimmter Rechtsträger ausgeübte Kontrolltätigkeit anwendbar sei.[32] In seinem Urteil stellte der EuGH fest, dass die Richtlinie anzuwenden sei: „Da somit alle personenbezogenen Daten zwischen den Mitgliedstaaten übermittelt werden können, verlangt die Richtlinie 95/46 grundsätzlich die Einhaltung von Regeln zum Schutz solcher Daten bei einer Verarbeitung im Sinne der Definition in Artikel 3." In ähnlicher Weise urteilte der Gerichtshof in der Rechtssache *Satakunnan Markkinapörssi und Satamedia,* dass die Verarbeitung personenbezogener Daten in Behördendateien, die nur in Medien veröffentlichtes Material als solches enthalten, in den Anwendungsbereich der Richtlinie 95/46 fällt.[33]

Eine zweite Reihe von Rechtsfragen betraf die Auslegung spezifischer Bestimmungen der Datenschutzrichtlinie. In der Rechtssache *Lindqvist* urteilte der EuGH über die Frage der im Internet erfolgten Verarbeitung personenbezogener Daten,[34] dass die Wiedergabe dieser Informationen im Internet eine „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten" darstelle. Er entschied jedoch, dass die Aufnahme

28 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, ABl. L 201 vom 31.7.2002, S. 37.

29 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. L 8 vom 12.1.2001, S. 1-22.

30 Diese Arbeitsgruppe wurde gemäß Artikel 29 der EU-Datenschutzrichtlinie 95/46/EG eingerichtet; siehe auch: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

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

32 Siehe verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Österreichischer Rundfunk*, Urteil vom 20. Mai 2003, Gerichtshof in voller Besetzung, Slg. 2003, S. I-4989.

33 Siehe Rechtssache C-73/07, *Satakunnan Markkinapörssi und Satamedia*, Urteil vom 16. Dezember 2008.

34 Siehe Rechtssache C-101/01, *Bodil Lindqvist*, Slg. 2003, S. I-12971.

personenbezogener Daten in eine Internetseite nicht als „Übermittlung in ein Drittland" im Sinne von Artikel 25 der Richtlinie 95/46 angesehen werden könne. Schließlich erließ der Gerichtshof jüngst eine sehr wichtige Entscheidung in Bezug auf das Diskriminierungsverbot bei der Verarbeitung personenbezogener Daten im Kontext der Unionsbürgerschaft.[35] Der EuGH urteilte, dass die unterschiedliche Behandlung der jeweiligen Staatsangehörigen von Mitgliedstaaten und anderen Unionsbürgern durch die zur Bekämpfung der Kriminalität vorgenommene systematische Verarbeitung der personenbezogenen Daten allein der Unionsbürger, die keine Staatsangehörigen des betreffenden Mitgliedstaats sind, eine durch Artikel 12 Absatz 1 EG-Vertrag untersagte Diskriminierung darstelle.

Der Gerichtshof hat eine Abwägung des Rechts auf Privatsphäre und Datenschutz gegen andere, innerhalb der Rechtsordnung der EU geschützte Grundrechte und Grundfreiheiten vorgenommen. In Fällen im Zusammenhang mit dem Schutz der Meinungsfreiheit – und insbesondere dem Journalismus – lässt der Gerichtshof die Bereitschaft zur Annahme entsprechender Ausnahmen vom Datenschutz erkennen; diesbezüglich hat sich der Gerichtshof sehr sensibel gezeigt. Im Spannungsfeld zwischen dem Recht auf Datenschutz und dem Recht auf Schutz des geistigen Eigentums hat der Gerichtshof ein eindeutiges Gutachten vermieden.

In der Rechtssache *Lindqvist*[36] musste der EuGH einen Mittelweg zwischen dem Recht auf Datenschutz und der unter anderem in Artikel 10 EMRK verankerten und innerhalb der Rechtsordnung der EU als allgemeiner Grundsatz des EU-Rechts geschützten Meinungsfreiheit finden. Nach Darlegung des Gerichtshofs „kommt den Grundrechten besondere Bedeutung zu, wie das Ausgangsverfahren zeigt, in dem es im Kern darum geht, die Meinungsfreiheit von Frau Lindqvist im Rahmen ihrer Arbeit als Katechetin und die Freiheit, Tätigkeiten auszuüben, die zum religiösen Leben beitragen, gegen den Schutz der Privatsphäre der Personen abzuwägen, über die Frau Lindqvist Daten auf ihre Website gestellt hat". In der Rechtssache *Satakunnan Markkinapörssi und Satamedia*[37] wurde der EuGH um eine Auslegung von Artikel 9 der Datenschutzrichtlinie ersucht, der den Mitgliedstaaten Abweichungen und Ausnahmen für die Verarbeitung personenbezogener Daten, die „allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, (…) nur insofern [gestattet], als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen". In diesem Fall erfasste Markkinapörssi öffentliche Daten bei den Steuerbehörden, um diese jährlich auszugsweise in den Regionalausgaben der Zeitschrift Veropörssi zu veröffentlichen, und gab diese Daten an Satamedia weiter, um die Daten über einen Kurzmitteilungsdienst zu verbreiten. Der EuGH führte aus, dass in Anbetracht der Bedeutung, die der Freiheit zur Meinungsäußerung in einer demokratischen Gesellschaft zukomme, die damit zusammenhängenden Begriffe, zu denen der des Journalismus gehöre, weit auszulegen seien. Er stellte dann klar, dass Tätigkeiten, die die Verarbeitung von Daten betreffen, die aus Dokumenten stammen, die nach den einzelstaatlichen Rechtsvorschriften öffentlich sind, als „journalistische Tätigkeiten" eingestuft werden können, wenn sie zum Zweck haben, „Informationen, Meinungen oder Ideen, mit welchem Übertragungsmittel auch immer, in der Öffentlichkeit zu verbreiten". Darüber hinaus urteilte der Gerichtshof, dass sich diese Tätigkeiten nicht auf Medienunternehmen beschränken, sondern bei jeglicher journalistischer Tätigkeit gegeben seien und dass diese Tätigkeiten mit einer Gewinnerzielungsabsicht verbunden sein könnten.

Mit ähnlichen Fragen befasste sich der EuGH in der Rechtssache *Promusicae*.[38] Er befand, dass „die Richtlinie 2002/58 nicht die Möglichkeit der Mitgliedstaaten ausschließt, eine Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen", und dass aus den Rechtsvorschriften zum geistigen Eigentum nicht hervorgehe, dass „die Mitgliedstaaten danach verpflichtet wären, im Hinblick auf die Sicherstellung eines effektiven Schutzes des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen". Er gelangte zu der Schlussfolgerung, dass „die Erfordernisse des Schutzes verschiedener Grundrechte, nämlich zum einen des Rechts auf Achtung des Privatlebens und zum anderen des Eigentumsrechts und des Rechts auf einen wirksamen Rechtsbehelf, miteinander in Einklang gebracht werden" müssten.

3.2. Datenschutz in der früheren zweiten und dritten Säule der EU

Hinsichtlich des Schutzes personenbezogener Daten im Rahmen von Tätigkeiten, die über den Geltungsbereich der früheren ersten Säule hinausgehen, gibt es nach wie vor ernstzunehmende Unsicherheiten und Defizite. Wenngleich die grundlegenden Vorschriften bezüglich des Schutzes personenbezogener Daten bei der Verarbeitung personenbezogener Daten innerhalb der früheren zweiten und dritten Säule befolgt werden müssen, fehlt ein allgemeiner Rechtsrahmen für den Schutz personenbezogener Daten in der früheren zweiten und dritten Säule. Stattdessen finden sich entsprechende Regelungen in einigen Ad-hoc-Sammlungen von Datenschutzvorschriften in verschiedenen Rechtsakten zur Verarbeitung personenbezogener Daten, etwa im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[39] Auch im Bereich der früheren zweiten und dritten Säule gab es verschiedene strukturelle Probleme und Unzulänglichkeiten, die die Möglichkeiten eines wirksamen Schutzes der Grundrechte ebenfalls beeinträchtigten. Im Hinblick auf die frühere dritte Säule war vor allem der Bereich der demokratischen Kontrolle problematisch. Die Rolle des Europäischen Parlaments beschränkte sich im Wesentlichen auf die Konsultation, und der Rat konnte sich über die Meinung des Parlaments hinwegsetzen. Überdies lag das Initiativrecht bei der Kommission und den Mitgliedstaaten gemeinsam, und für diese frühere zwischenstaatliche Säule galt das Einstimmigkeitsprinzip. Zweitens war innerhalb der früheren dritten Säule auch die gerichtliche Kontrolle durch

35 Rechtssache C-524/06, *Huber/Bundesrepublik Deutschland*, Urteil vom 16. Dezember 2008.

36 Siehe Rechtssache C-101/01, *Bodil Lindqvist*, Slg. 2003, S. I-12971.

37 Siehe Rechtssache C-73/07, *Satakunnan Markkinapörssi und Satamedia*, Urteil vom 16. Dezember 2008.

38 Rechtssache C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, Urteil vom 29. Januar 2008.

39 Zum Schutz personenbezogener Daten im Rahmen von Titel VI EUV (so genannte „dritte Säule") siehe beispielsweise das Übereinkommen zur Durchführung des Übereinkommens von Schengen von 1990, das spezifische, für das Schengener Informationssystem geltende Datenschutzbestimmungen enthält, ABl. L 239 vom 22.9.2000, S. 19; das Europol-Übereinkommen von 1995 und unter anderem die Vorschriften für die Übermittlung personenbezogener Daten durch Europol an Drittstaaten und Drittstellen, ABl. C 316 vom 27.11.1995, S. 2; den Beschluss über die Errichtung von Eurojust von 2002, ABl. L 63 vom 6.3.2002, S. und die Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust, ABl. C 68 vom 19.3.2005, S. 1.; das Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich von 1995, das Vorschriften zum Schutz personenbezogener Daten betreffend das Zollinformationssystem enthält, ABl. C 316 vom 27.11.1995, S. 34; und das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union aus dem Jahr 2000, insbesondere Artikel 23, ABl. C 197 vom 12.7.2000, S. 1 und 15.

den Gerichtshof begrenzt. Gemäß dem früheren Artikel 35 Absatz 1 EUV hatte der Gerichtshof im Wege der Vorabentscheidung über die Gültigkeit und die Auslegung der Rahmenbeschlüsse und Beschlüsse, über die Auslegung der Übereinkommen und über die Gültigkeit und die Auslegung der dazugehörigen Durchführungsmaßnahmen zu entscheiden. Diese Zuständigkeit unterlag der Anerkennung durch die Mitgliedstaaten, welche die Möglichkeit, ein Vorabentscheidungsersuchen an den Gerichtshof zu richten, weiter auf bestimmte einzelstaatliche Gerichte beschränken konnten. Drittens war im Vergleich zur ersten Säule auch die beratende Rolle von Datenschutzbehörden begrenzt (z. B. die Rolle des Datenschutzbeauftragten). Beispielsweise bekräftigt die Europäische Kommission, dass sie sich gemäß Artikel 28 Absatz 2 der Verordnung 45/2001) verpflichtet fühlt, bei der Annahme eines Vorschlags für Rechtsvorschriften, die sich auf den Schutz personenbezogener Daten auswirken können, den Europäischen Datenschutzbeauftragten zu konsultieren; die Europäische Kommission teilte sich das Initiativrecht innerhalb der dritten Säule jedoch mit den Mitgliedstaaten, die ihrerseits nicht an eine entsprechende Verpflichtung gebunden waren. Die Situation innerhalb der zweiten Säule war sogar noch schlechter, da es innerhalb des Rahmens der gemeinsamen Außen- und Sicherheitspolitik keine Möglichkeit einer gerichtlichen Kontrolle gab.

In den letzten Jahren ist der Austausch personenbezogener Daten zwischen den Strafverfolgungsbehörden in den verschiedenen Mitgliedstaaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit allgemein üblich geworden. Diesbezüglich beinhaltet das „Haager Programm", das am 5. November 2004 als Reaktion auf den „Kampf gegen den Terror" angenommen wurde, den „Verfügbarkeitsgrundsatz", dem zufolge Informationen, die bestimmten Behörden in einem Mitgliedstaat zur Verfügung stehen, auch gleichwertigen Behörden in anderen Mitgliedstaaten zugänglich gemacht werden müssen. Es ist offenkundig, dass der „Verfügbarkeitsgrundsatz" ernst zu nehmende Auswirkungen auf den Schutz personenbezogener Daten haben kann und dass angemessene Sicherheitsvorkehrungen erforderlich sind.

Vor diesem Hintergrund wurde der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, begrüßt.[40] Der Beschluss ist das erste horizontale Datenschutzinstrument im Bereich der von Polizei- und Justizbehörden verwendeten personenbezogenen Daten. Der Rahmenbeschluss findet auf den grenzüberschreitenden Austausch personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit Anwendung. Er enthält Vorschriften für die Weiterleitung personenbezogener Daten an Drittländer sowie die Übermittlung an Privatpersonen in den Mitgliedstaaten. Der Beschluss gestattet den EU-Staaten auch, Bestimmungen zum Schutz personenbezogener Daten zu erlassen, die strenger sind als die Bestimmungen dieses Instruments. Der Rahmenbeschluss an sich kann jedoch nicht gewährleisten, dass die Garantien des Rechtes auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten bei der Verarbeitung personenbezogener Daten im Rahmen der zweiten und dritten Säule umfassend erfüllt werden. Da sein Anwendungsbereich nur grenzüberschreitende Datenströme zwischen den Strafvollzugsbehörden der Mitgliedstaaten erfasst, gilt er nicht für die Verarbeitung von Daten durch die Strafvollzugsbehörden innerhalb der einzelnen Mitgliedstaaten. Der Rahmenbeschluss ist von den Mitgliedstaaten der EU bis zum 27. November 2010 umzusetzen, indem sie die erforderlichen Maßnahmen treffen; zu diesen Maßnahmen zählt auch die Benennung einer oder mehrerer öffentlicher Stellen, die für die diesbezügliche Beratung und die Überwachung der Anwendung im jeweiligen Hoheitsgebiet zuständig sind.

Der Schutz personenbezogener Daten war zudem einer der Bereiche, in denen die frühere Säulenstruktur der EU kontinuierlich zu divergierenden Ansichten hinsichtlich der Zuordnung verschiedener Arten der Verarbeitung zu den einzelnen Säulen Anlass gab. Das Urteil des EuGH in den Rechtssachen *Passenger Name Record* (*PNR*) zeigte, welche Probleme für das Datenschutzsystem der EU aus der früheren Säulenstruktur resultierten.[41] Die Rechtssachen betrafen das zwischen den Vereinigten Staaten und der EU geschlossene Abkommen über die Übermittlung von Daten der Reservierungs- und Abfertigungssysteme (so genannte „*Passenger Name Records*", im Folgenden: *PNR*-Daten oder „Fluggastdatensätze") von Fluggesellschaften, die Flüge in die oder aus den Vereinigten Staaten von Amerika durchführen. Nach einer von der Kommission am 14. Mai 2004 gemäß Artikel 25 der Datenschutzrichtlinie angenommenen Angemessenheitsentscheidung nahm der Rat am 17. Mai 2004 einen Beschluss an, der den Abschluss des Abkommens mit den Vereinigten Staaten ermöglichte. Das Europäische Parlament klagte vor dem Gerichtshof auf Nichtigerklärung der Angemessenheitsentscheidung der Kommission und des Ratsbeschlusses über den Abschluss des Abkommens, unter anderem aufgrund eines Verstoßes gegen wesentliche Grundsätze der Datenschutzrichtlinie und das Recht auf Privatsphäre. Der Gerichtshof erklärte die Angemessenheitsentscheidung schon deswegen für nichtig, weil ihr Gegenstand nicht in den Anwendungsbereich der Datenschutzrichtlinie fällt. Er führte aus, dass sich die Übermittlung von PNR-Daten auf eine die „öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich" betreffende Verarbeitung personenbezogener Daten gemäß Artikel 3 Absatz 2 der Richtlinie 95/46 beziehe und dass die Angemessenheitsentscheidung daher nicht gemäß dieser Richtlinie angenommen werden konnte. In ähnlicher Weise erklärte der EuGH den Beschluss des Rates über den Abschluss des Abkommens für nichtig, weil dieser nicht gemäß Artikel 95 EG-Vertrag erlassen werden konnte; das Abkommen betraf nämlich „die gleiche Datenübermittlung wie die Angemessenheitsentscheidung und damit eine Verarbeitung von Daten, die nicht in den Anwendungsbereich der Richtlinie fällt": insoweit wurde eine Zuständigkeit der EU für den Abschluss des Abkommens verneint. Da das Urteil des Gerichtshofs eine Verlagerung des *PNR*-Abkommens von der früheren ersten Säule auf die frühere dritte Säule bewirkte (mit erheblichen Folgen hinsichtlich der gerichtlichen Überprüfung und der demokratischen Kontrolle), ergab sich durch das Urteil des Gerichtshofs ein Schlupfloch bezüglich des Rechts des Einzelnen auf Datenschutz („*a loophole in the right of data protection*").[42] Vor allen Dingen aber musste die EU infolge der Entscheidung des EuGH ein neues Abkommen mit den Vereinigten Staaten unter Berücksichtigung einer angemessenen Rechtsgrundlage schließen. 2007 veröffentlichte die Kommission einen Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von PNR-Daten für die Zwecke der Strafverfolgung.[43] Die FRA wurde vom französischen Ratsvorsitz um ein Gutachten zu diesem Vorschlag ersucht; sie übermittelte dieses Gutachten am 28. Oktober 2008.[44] Sie vertrat die Ansicht, dass der

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

41 Verbundene Rechtssachen C-317/04 und C-318/04, *Europäisches Parlament/Rat und Kommission*, Urteil der Großen Kammer vom 30. Mai 2006, Slg. 2006, S. I-4721.

42 Siehe E. Guild und E. Brouwer, *The Political Life of Data – The ECJ decision on the PNR Agreement between the EU and the US*, (2006) Centre for European Policy Studies No. 109.

43 KOM(2007) 654.

44 Siehe: http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.

Mehrwert und die Notwendigkeit des Vorschlags im Zusammenhang mit der Verwendung von PNR-Daten erläutert werden müsse, dass ungenaue Begriffe vermieden werden sollten und dass eine hinreichende verfahrenstechnische Gewähr gegeben sein müsste. Außerdem empfahl die FRA das ausdrückliche Verbot der Verwendung diskriminierender ethnischer Profile („*ethnic Profiling*").

In der Rechtssache *Irland/Europäisches Parlament und Rat* wurde der EuGH erneut um eine Entscheidung hinsichtlich der problematischen Aufteilung des Datenschutzsystems der EU auf die verschiedenen Säulen ersucht.[45] Im Einzelnen beantragte Irland die Nichtigerklärung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Telekommunikationsdaten; begründet wurde der Antrag mit der Ansicht, dass Artikel 95 EG nicht die richtige Rechtsgrundlage für diesen Rechtsakt sei. Hauptziel dieser Rechtsvorschrift sei die Förderung der Ermittlung, Feststellung und Verfolgung schwerer Straftaten, einschließlich des Terrorismus, und dementsprechend hätte die Vorschrift gemäß der dritten Säule angenommen werden müssen. Der Gerichtshof teilte diese Ansicht jedoch nicht und entschied, dass die Richtlinie auf der richtigen Rechtsgrundlage erlassen worden sei, weil sowohl ihr Ziel als auch ihr Inhalt unter Artikel 95 EG-Vertrag fallen. Der EuGH differenzierte zwischen der Rechtssache *Irland/Europäisches Parlament und Rat* und dem *PNR*-Urteil, weil sich Richtlinie 2006/24 auf die Tätigkeiten der Dienstanbieter im Binnenmarkt bezieht und keine Regelung der Handlungen staatlicher Stellen zu Strafverfolgungszwecken enthält, wie es in der Sache *PNR* der Fall war. Der Gerichtshof stellte jedoch ausdrücklich klar, dass sich die von Irland erhobene Klage (und damit sein Urteil) „allein auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge von mit der Richtlinie 2006/24 verbundenen Eingriffen in das Recht auf Privatsphäre".[46] In einigen Mitgliedstaaten wurden Zweifel bezüglich der Vereinbarkeit dieser Richtlinie mit bestimmten Grundrechten geäußert. In Rumänien beispielsweise rief ein Gericht das Verfassungsgericht an, um im Zusammenhang mit einem von einer NRO gegen eine Telekommunikationsgesellschaft angestrengten Datenschutzverfahren die mutmaßliche Verfassungswidrigkeit des rumänischen Gesetzes über die Vorratsspeicherung von Daten feststellen zu lassen.[47] Am 8. Oktober 2009 bewertete das rumänische Verfassungsgericht das Gesetz zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten als verfassungswidrig und sah einen Verstoß gegen das Grundrecht auf Schutz der Privatsphäre als gegeben.[48] In seiner Begründung nahm das Gericht nicht nur auf die Rechtsvorschriften zur Umsetzung der Richtlinie in Rumänien Bezug, sondern stellte auch die Vereinbarkeit der eigentlichen Richtlinie mit den Grundrechten in Frage. In Deutschland ist gegenwärtig vor dem Bundesverfassungsgericht eine Rechtssache im Zusammenhang mit der Vereinbarkeit der deutschen Rechtsvorschriften zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten mit den Grundrechten anhängig. Das Verfassungsgericht hat eine einstweilige Verfügung erlassen, mit der die Rechtsvorschriften zur Umsetzung der Richtlinie bis zur endgültigen Entscheidung in dieser Sache teilweise ausgesetzt werden.[49] Am 2. März 2010 hat das Bundesverfassungsgericht die deutschen Rechtsvorschriften zur Umsetzung der EU-Richtlinie über die Vorratsspeicherung von Daten als nicht verfassungsgemäß bewertet.[50] In diesem Zusammenhang sollte die Europäische Union die Vereinbarkeit der EU-Richtlinie über die Vorratsspeicherung von Daten (Richtlinie 2006/24/EG) mit den Grundrechten möglicherweise proaktiv vor dem Hintergrund der neuen Grundrechtestandards des Vertrags von Lissabon (siehe unten) überprüfen. Ein weiteres Urteil des Europäischen Gerichtshofs in Bezug auf die Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit den Grundrechten wäre wünschenswert, um in allen EU-Mitgliedstaaten Rechtssicherheit gewährleisten zu können.

Die wichtigste Beschränkung, der sich die EU derzeit bei der Gewährleistung eines wirksamen und umfassenden Datenschutzes gegenübersieht, resultiert aus der früheren, auf der Unterteilung in Säulen basierenden Verfassungsarchitektur der EU. In der früheren ersten Säule der EU ist der Datenschutz zwar hoch entwickelt, in der früheren dritten Säule kann das Datenschutzsystem jedoch nicht als zufrieden stellend betrachtet werden. Bislang umfasste die frühere dritte Säule der EU Bereiche wie die polizeiliche Zusammenarbeit, die Terrorismusbekämpfung und strafrechtliche Fragen, in denen der Datenschutz besonders wichtig und unverzichtbar ist.

3.3. Der Vertrag von Lissabon

Im Hinblick auf das Grundrecht des Datenschutzes stellt der Vertrag von Lissabon einen erheblichen Fortschritt für die EU dar, da er eine Reihe wichtiger Verbesserungen in Bezug auf den Datenschutz auf EU-Ebene enthält. Eine erste bedeutsame Verbesserung besteht darin, dass der Vertrag von Lissabon der Charta der Grundrechte Rechtsverbindlichkeit verleiht. Artikel 8 der Charta über den Schutz personenbezogener Daten wird eine Rolle spielen können, die weit über die förmliche und symbolische Verkündung als Grundrecht hinausgeht. Die Anerkennung des Datenschutzes als eigenständiges Grundrecht mit voller Bestandskraft als Bestandteil des primären EU-Rechts bedeutet, dass der Datenschutz eine wichtigere Rolle spielen wird, wenn eine Abwägung gegenüber anderen Werten und Interessen (z. B. Sicherheits- oder Marktinteressen) vorgenommen wird und durch den EU-Gesetzgeber und den EuGH Prioritäten festgelegt werden. Eine zweite wichtige Verbesserung ist die Abschaffung der früheren „Säulenstruktur". Damit wurden im Rahmen des Vertrags von Lissabon die strukturellen Probleme ausgeräumt, die vorher im Zusammenhang mit der dritten Säule in Bezug auf das Beschlussfassungsverfahren und den Kontrollbereich bestanden. So wurde im Raum der Freiheit, der Sicherheit und des Rechts die Beschlussfassung mit qualifizierter Mehrheit eingeführt, die Rolle des Europäischen Parlaments wurde gestärkt, und der EuGH verfügt in diesem Raum über umfassende Zuständigkeit. Es ist jedoch darauf hinzuweisen, dass für das Vereinigte Königreich und für Polen gemäß Protokoll Nr. 30 zum Vertrag von Lissabon gewisse Sonderregelungen gelten. Mit diesem Protokoll sollten die Auswirkungen der Grundrechte-Charta der EU auf britisches und polnisches Recht begrenzt werden. Und in ähnlicher Weise sollten mit Ziffer 2 der Schlussfolgerungen des Ratsvorsitzes

45 Rechtssache C-301/06 *Irland/Europäisches Parlament und Rat*, Urteil der Großen Kammer vom 10. Februar 2009.
46 *Irland/Europäisches Parlament und Rat*, Randnummer 57.
47 www.mondonews.ro/Legea-298-de-stocare-a-datelor-telefonice-ajunge-la-CCR+id-5439.html.
48 Rechtssache Rumänien/Curtea Constituțională, Entscheidung Nr. 1258 des rumänischen Verfassungsgerichts vom 8. Oktober 2009 (siehe: www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf).
49 Deutsches Bundesverfassungsgericht, Pressemitteilung Nr. 37/2008 vom 19. März 2008.
50 In seinem Urteil vom 2. März 2010 hat das Bundesverfassungsgericht das Gesetz zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten in Deutschland unter Hinweis auf die Unverhältnismäßigkeit von mit diesem Gesetz auferlegten Verpflichtungen als nicht verfassungskonform bewertet. Insbesondere hat das Gericht festgestellt, dass § 113 TKG (Telekommunikationsgesetz) die Sicherheit der gespeicherten Daten nicht garantiert werde sowie dass die Bestimmungen nicht hinreichend transparent seien, weil sie eine unmittelbare Verwendung der Daten für die Untersuchung, Aufdeckung und Verfolgung einer Reihe von Straftaten vorsehen, die nicht eindeutig definiert seien; und dass der mit diesem Gesetz verbundene Rechtsschutz den verfassungsrechtlichen Anforderungen nicht entspreche (siehe: www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html).

vom 29. und 30. Oktober 2009 die Auswirkungen der EU-Charta auch auf das tschechische Recht begrenzt werden; dort wurde vereinbart, dass den EU-Verträgen ein Protokoll bezüglich einer Änderung von Protokoll Nr. 30 wie folgt beigefügt werden soll: „Der Titel, die Präambel und der verfügende Teil des Protokolls Nr. 30 werden so geändert, dass sie in der gleichen Weise auf die Tschechische Republik Bezug nehmen wie auf Polen und auf das Vereinigte Königreich."[51] Erklärung Nr. 20 zum Vertrag von Lissabon besagt, dass immer dann, wenn Bestimmungen über den Schutz personenbezogener Daten zu erlassen sind, die sich unmittelbar auf die nationale Sicherheit auswirken könnten, dieser Umstand „gebührend" zu berücksichtigen ist. In Erklärung Nr. 21 heißt es, dass es sich aufgrund des spezifischen Charakters der Bereiche justizielle Zusammenarbeit in Strafsachen und polizeiliche Zusammenarbeit als erforderlich erweisen könnte, in diesen Bereichen spezifische Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr zu erlassen. Die Frage der konkreten Auswirkungen dieser Protokolle und Erklärungen für den Schutz personenbezogener Daten bleibt streitig und wird erst dann geklärt werden können, wenn eine diesbezügliche Rechtsprechung des Gerichtshofs erfolgt.

51 www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/110889.pdf.

4 Vergleichender Überblick

Dieser zentrale Abschnitt des Berichts bietet einen vergleichenden Überblick über die nationalen Datenschutzbehörden, die innerstaatlichen Verfahren für die Umsetzung der Datenschutzvorschriften und die Rechtsbehelfe in den Mitgliedstaaten zur Sanktionierung und zum materiellen Ausgleich von Verstößen gegen die Datenschutzvorschriften sowie über die Sensibilisierung der EU-Bürger für ihre Datenschutzrechte. Die hier erläuterten Informationen beruhen auf den 27 von den Fralex-Teams durchgeführten einzelstaatlichen Studien, denen die von der FRA erarbeiteten allgemeinen Leitlinien zugrunde liegen. (Alle Studien sind auf der Website der FRA unter der Adresse http://fra.europa.eu als Hintergrundmaterial öffentlich zugänglich.) Auf der Grundlage dieser Studien wurde dieser vergleichende Bericht verfasst. Die nationalen Studien stammen vom Februar 2009.

4.1. Datenschutzbehörden

Alle Mitgliedstaaten der EU haben gemäß Artikel 28 Absatz 1 Satz 1 der Datenschutzrichtlinie eine einzelstaatliche Kontrollstelle benannt, die für die allgemeine Überwachung der Anwendung der datenschutzrechtlichen Bestimmungen und die Sicherstellung ihrer Befolgung im jeweiligen Hoheitsgebiet zuständig ist. Mehrere Mitgliedstaaten (z. B. Österreich und die Niederlande) haben eine Datenschutzbehörde mit allgemeiner Zuständigkeit und mehrere weitere, branchenspezifische Kontrollstellen (für die Bereiche Gesundheit, Post, Telekommunikation usw.) eingerichtet. Manche Staaten mit föderaler oder regionaler Organisation von Befugnissen (z. B. Deutschland oder Spanien) wiederum haben eine staatliche Kontrollstelle und mehrere Kontrollstellen mit entsprechender Funktion auf regionaler oder teilstaatlicher Ebene eingerichtet.[52] Da zudem in manchen Ländern (z. B. in Rumänien) vor der Einrichtung von Datenschutzbehörden die Zuständigkeit für den Schutz des Rechts auf Privatsphäre bei behördlichen Bürgerbeauftragten lag, kommt in manchen Mitgliedstaaten (z. B. in Finnland) weiterhin dem Bürgerbeauftragte maßgebliche Bedeutung für den Schutz personenbezogener Daten zu.

Dieser Abschnitt bietet eine vergleichende Übersicht. Vielversprechende Praktiken in diesem Zusammenhang werden in Abschnitt 6.1 behandelt.

4.1.1. Unabhängigkeit

Die Mitgliedstaaten der EU haben sich bemüht, Artikel 28 Absatz 1 Satz 2 der Datenschutzrichtlinie nachzukommen; gemäß dieser Bestimmung müssen die Mitgliedstaaten sicherstellen, dass ihre nationalen Datenschutzbehörden die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Die Auslegung dieser Bestimmung der Datenschutzrichtlinie war Gegenstand von Schlussanträgen von Generalanwalt Mazák. In diesen Schlussanträgen wird auf die Relativität des Begriffs „Unabhängigkeit" abgestellt, da bestimmt werden muss, gegenüber wem und in welchem Maß diese Unabhängigkeit gegeben sein muss. In Bezug auf Datenschutzbehörden wird erklärt, dass bei der Beurteilung ihrer Unabhängigkeit der Zweck dieser Stellen berücksichtigt werden muss.[53]

In verschiedenen Ländern geben jedoch normative oder praktische Hindernisse Anlass zu Bedenken hinsichtlich der tatsächlichen Unabhängigkeit nationaler Datenschutzbehörden von der staatlichen Politik. Die Gewährleistung der Unabhängigkeit wird faktisch primär durch das Verfahren der Berufung und Amtsenthebung der Mitarbeiter der Datenschutzbehörden sichergestellt. Die Kontrolle über finanzielle Ressourcen stellt ein weiteres maßgebliches Element für die Gewährleistung der Autonomie der Kontrollstellen dar.

In mehreren Mitgliedstaaten (z. B. in Deutschland und in Slowenien) werden Mitarbeiter der Datenschutzbehörden durch die gesetzgebende Versammlung gewählt, zuweilen (etwa in Griechenland) sogar im Wege von Verfahren, die einen Konsens zwischen der Mehrheit und der Opposition erfordern: Mit gewissen Ausnahmen (z. B. in Ungarn, wo eine verfassungsrechtliche Praxis den Parlamentsparteien die Möglichkeit bietet, die Posten der Mitarbeiter der Datenschutzbehörde nach eigenem Ermessen untereinander zu verteilen) stellt dies ein hohes Maß an Unabhängigkeit der gewählten Mitarbeiter sicher. In verschiedenen Mitgliedstaaten dagegen werden Mitarbeiter der Datenschutzbehörden ohne Beteiligung der parlamentarischen Opposition direkt von der Regierung ernannt (z. B. Irland, Luxemburg). Verschiedentlich (z. B. im Vereinigten Königreich[54] sowie in Litauen und in Estland) hat dies zu schwerwiegenden Bedenken hinsichtlich der tatsächlichen Unabhängigkeit der Datenschutzbehörde geführt. Zu ähnlichen Bedenken kann es in Ländern kommen, in denen die Kontrollstelle dem Justizministerium angegliedert ist (z. B. Dänemark, Lettland). Andere Mitgliedstaaten (z. B. Belgien, Frankreich, Portugal, Spanien) schließlich sehen für die Berufung der Mitarbeiter der einzelstaatlichen Datenschutzbehörde ein kombiniertes Verfahren vor, an dem zugleich die Exekutive, die Legislative und die Judikative oder andere organisierte gesellschaftliche Gruppen (z. B. der Oberste Rat der Universitäten in Spanien) mitwirken. In derartigen

52 Zu Vergleichszwecken werden in diesem Bericht jedoch nur die Datenschutzbehörden auf gesamtstaatlicher Ebene analysiert. Es ist zu beachten, dass in Deutschland auf Länderebene ähnliche Datenschutzbehörden mit Kontrollbefugnissen für den privaten und öffentlichen Bereich sowie für die Rundfunkanstalten und für die Kirchen bestehen. Darüber hinaus gibt es in manchen Bundesländern Kontrollstellen, die nur für die Überwachung des privaten Bereichs zuständig sind. Diese Überwachungsgremien auf Länderebene werden in diesem Bericht nicht berücksichtigt.

53 Schlussanträge des Generalanwalts Mazák, Rechtssache C-518/07, *Kommission der Europäischen Gemeinschaften/Bundesrepublik Deutschland*, vom 22. Oktober 2009; die Kommission hat dieses Vertragsverletzungsverfahren/Deutschland wegen der falschen Umsetzung der EU-Datenschutzrichtlinie durch die Kontrollstellen im privaten Sektor eingeleitet (mangelnde Unabhängigkeit). Der Europäische Gerichtshof (Große Kammer) hat am 9. März 2010 in der Rechtssache C-518/07, *Kommission der Europäischen Gemeinschaften/Deutschland*, in den Randnummern 18 und 19 festgestellt: „Was erstens den Wortlaut von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 angeht, ist angesichts des Fehlens einer Definition in der Richtlinie auf den gewöhnlichen Sinn der Wendung ‚in völliger Unabhängigkeit' abzustellen. In Bezug auf öffentliche Stellen bezeichnet der Begriff ‚Unabhängigkeit' in der Regel eine Stellung, in der gewährleistet ist, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann. Entgegen dem Standpunkt der Bundesrepublik Deutschland deutet nichts darauf hin, dass das Unabhängigkeitserfordernis allein das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen beträfe. Im Gegenteil wird der Begriff ‚Unabhängigkeit' durch das Adjektiv ‚völlig' verstärkt, was eine Entscheidungsgewalt impliziert, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei sie unmittelbar oder mittelbar, entzogen ist."

54 Im Vereinigten Königreich hat das Parlament seit 2009 eine beratende Rolle, und vor der Berufung findet vor dem Rechtsausschuss eine öffentliche Anhörung der ausgewählten Bewerber statt. Die Ansichten des Ausschusses sind zwar nicht bindend, werden jedoch generell vor der Berufung berücksichtigt.

Fällen muss jedoch unbedingt gewährleistet werden, dass nicht *de facto* die Regierung die unmittelbare oder mittelbare Kontrolle über die Mehrzahl der berufenen Mitarbeiter hat und ein pluralistisches Berufungsverfahren so letztlich seines Zweckes beraubt wird.

In mehreren Mitgliedstaaten (z. B. in Italien) haben Mitarbeiter von Datenschutzbehörden eine Amtszeit von sieben Jahren, wobei eine Amtsenthebung oder erneute Berufung für eine zweite Amtszeit untersagt ist. In manchen Ländern (z. B. in Polen und Slowenien) können Mitarbeiter von Datenschutzbehörden nur bei besonderem Fehlverhalten und nur unter Einhaltung des gleichen Verfahrens, das auch bei ihrer Berufung zur Anwendung gekommen ist, vorzeitig ihres Amtes enthoben werden. Diese technischen Lösungen gewährleisten ein hohes Maß an Unabhängigkeit der Kontrollstellen, indem die Einflussnahme und der Druck der politischen Kräfte gemindert werden. In anderen Mitgliedstaaten dagegen kann die Regierung die Datenschutzbeauftragten direkt ihres Amtes entheben; dies ist allerdings hinsichtlich der tatsächlichen Unabhängigkeit der Kontrollstelle, insbesondere in Bezug auf die Einhaltung der Datenschutzbestimmungen durch Regierungsstellen, als bedenklich zu bewerten.

Die Autonomie der Kontrollstelle wird besonders gestärkt, wenn (wie in Griechenland und Portugal) die Existenz und der Aufgabenbereich einer unabhängigen, mit der Kontrolle der Einhaltung der Datenschutzbestimmungen beauftragten Behörde explizit in der Verfassung verankert sind. Für weitere wichtige Garantien hinsichtlich der institutionellen Unabhängigkeit wird dann gesorgt, wenn die Datenschutzbehörde eine eigene Rechtspersönlichkeit erhält (z. B. in Malta und Spanien) und ihr die Möglichkeit eingeräumt wird, Gerichtsverfahren vor dem einzelstaatlichen Verfassungsgericht anzustrengen (z. B. in Slowenien).

4.1.2. Ressourcen

In den meisten Mitgliedstaaten der EU erhalten die Datenschutzbehörden die für ihre Funktion nötigen Ressourcen aus dem Staatshaushalt (z. B. in Estland, Frankreich, Italien und in den Niederlanden), häufig aus dem Haushalt des Justizministeriums. In manchen Mitgliedstaten können die Kontrollstellen ihre finanziellen Ressourcen jedoch durch die Einnahmen aus den Meldungen der Auftragsverarbeiter und/oder durch die bei Verstößen gegen Datenschutzbestimmungen verhängten finanziellen Sanktionen erheblich erhöhen (z. B. in Luxemburg und in Malta). Im Vereinigten Königreich sind Meldegebühren die einzige Einnahmequelle für die Datenschutztätigkeit der Kontrollstelle.

In vielen Mitgliedstaaten (insbesondere z. B. in Frankreich, Italien, Österreich, Portugal und Rumänien) wurden Probleme in Bezug auf unzureichende Finanzausstattung der Kontrollstellen hervorgehoben. In anderen Ländern, in denen die Datenschutzbehörde derzeit finanziell relativ gut ausgestattet ist, sind für die kommenden Jahre Haushaltskürzungen vorgesehen (z B. in Dänemark und in Irland). In Anbetracht der den Datenschutzbehörden sowohl durch EU-Recht als auch durch einzelstaatliches Recht übertragenen Aufgaben stellen die unzureichende Personalausstattung und fehlende Finanzmittel eine beträchtliche Herausforderung für die Wirksamkeit der einzelstaatlichen Kontrollsysteme dar, die den Schutz der Grundrechte der betroffenen Personen gefährden könnte. Die Mitgliedstaaten sollten daher dafür Sorge tragen, dass die nationalen Datenschutzbehörden über hinreichende Ressourcen verfügen, um ihren Aufgaben ordnungsgemäß nachkommen zu können.

4.1.3. Befugnisse

Die Mitgliedstaaten der EU waren verpflichtet, ihre einzelstaatlichen Kontrollstellen mit den allgemeinen Befugnissen von Artikel 28 Absatz 2 (Befugnis zur Beratung von Legislativ- oder Verwaltungsbehörden bei der Ausarbeitung von Rechtsvorschriften oder Rechtsverordnungen bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten), Artikel 28 Absatz 3 (Untersuchungsbefugnis, Einwirkungsbefugnis und Klagerecht oder Anzeigebefugnis) und Artikel 28 Absatz 4 (Befugnis zur Befassung mit Eingaben) der Datenschutzrichtlinie auszustatten. Wie die nachstehende Erhebung deutlich macht, wurden diese Bestimmungen der Datenschutzrichtlinie jedoch nicht in allen Mitgliedstaaten vollständig umgesetzt; daher verfügen einige nationale Datenschutzbehörden nur über begrenzte Instrumente zur Erfüllung ihrer Kontrollaufgaben. Dieses Problem muss von den betreffenden Ländern gelöst werden.

Generell können bei der Analyse der Befugnisse der verschiedenen nationalen Datenschutzbehörden zwei allgemeine Tendenzen unterschieden werden, in denen die Konzepte zum Ausdruck kommen, die die Mitgliedstaaten bei der Umsetzung der Datenschutzrichtlinie anwenden. Während mehrere Länder (z. B. Finnland, Irland, Schweden und das Vereinigte Königreich) die präventive und proaktive Rolle der Kontrollstellen betont haben, indem sie den Schwerpunkt auf deren *Ex-ante*-Rolle bei der Gewährleistung des Schutzes personenbezogener Daten gelegt haben, haben andere Mitgliedstaaten (z. B. Griechenland, Lettland und die Tschechische Republik) der *Ex-post*-Durchsetzungs- und Kontrollfunktion der Datenschutzbehörden Priorität gewährt und diesen eine reaktive Pflicht zur Überwachung der Einhaltung der Datenschutzbestimmungen übertragen. Entsprechend unterscheidet sich die Art der den Kontrollstellen übertragenen Befugnisse, wobei entweder „weichen" Präventionsinstrumenten in den erstgenannten Fällen bzw. „härteren" Maßnahmen in den letztgenannten Fällen der Vorzug gegeben wird. Diese Unterschiede dürfen jedoch keinesfalls überbewertet werden. Es gibt nämlich Länder (z. B. Dänemark, Italien, die Niederlande und Slowenien), die einen Mittelweg eingeschlagen haben, indem sie ihren nationalen Datenschutzbehörden Befugnisse zur aktiven Unterstützung und Gewährleistung der Einhaltung der Datenschutzbestimmungen übertragen und sie gleichzeitig zur Verfolgung und Bestrafung von Verstößen ermächtigt haben. Überdies sind – wie in den nächsten vier Unterabschnitten erläutert – mehrere gemeinsame Merkmale festzustellen, die sich mit diesen Unterscheidungen zwischen Ländern nicht vereinbaren lassen.

4.1.3.1. Untersuchungsbefugnisse

Nach Artikel 28 Absatz 3 Satz 1 der Datenschutzrichtlinie verfügen Kontrollstellen über Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen. Die nachstehende Tabelle 1 belegt den Grad der Umsetzung der oben genannten Bestimmungen in den verschiedenen einzelstaatlichen Rechtsvorschriften zur Einrichtung der Datenschutzbehörden, wobei angegeben wird, ob die Kontrollstellen über die folgenden Befugnisse verfügen: a) Aufforderung des Auftragsverarbeiters/des für die Verarbeitung Verantwortlichen/der betroffenen Person zur Vorlage von Informationen oder Unterlagen; b) Aufforderung des Auftragsverarbeiters/des für die Verarbeitung Verantwortlichen zur Gewährung des Zugangs zu Datenbanken und Archivierungssystemen; c) Durchführung von Durchsuchungen

und Beschlagnahmen in den Räumlichkeiten des Auftragsverarbeiters/des für die Verarbeitung Verantwortlichen ohne richterliche Anordnung;
d) Durchführung von Durchsuchungen und Beschlagnahmen in den Räumlichkeiten des Auftragsverarbeiters/des für die Verarbeitung Verantwortlichen nach Erlangung einer richterlichen Anordnung;
e) Durchführung von Audits zur Kontrolle der Einhaltung der Bestimmungen durch den Auftragsverarbeiter/für die Verarbeitung Verantwortlichen, um sicherzustellen, dass die Datenverarbeitung in Übereinstimmung mit den einschlägigen Rechtsvorschriften erfolgt.

Tabelle 1: Untersuchungsbefugnisse

Mitgliedstaat	Anforderung von Informationen und Unterlagen	Zugang zu Datenbanken und Archivierungssystemen	Durchsuchung von Räumlichkeiten und Beschlagnahme ohne richterliche Anordnung	Durchsuchung von Räumlichkeiten und Beschlagnahme mit richterlicher Anordnung	Durchführung von Audits
Belgien	●	●	●		●
Bulgarien	●	●	●		●
Dänemark	●	●	●		●
Deutschland	●	●	●	●*	●
Estland	●	●	●		●
Finnland	●	●	●		●
Frankreich	●	●		●	●
Griechenland	●	●	●		●
Irland	●	●	●		●
Italien	●	●	●**	●	●
Lettland	●	●	●		●
Litauen	●	●	●		●
Luxemburg	●	●	●		●
Malta	●	●		●	●
Niederlande	●	●	●		●
Österreich	●	●	●		●
Polen	●	●	●		●
Portugal	●	●	●		●
Rumänien	●	●			●
Schweden	●	●	●		●
Slowakei	●	●	●		●
Slowenien	●	●	●		●
Spanien	●	●	●		●
Tschechische Republik	●	●	●		●
Ungarn	●	●	●		●
Vereinigtes Königreich	●			●	●***
Zypern	●	●	●		●

*Anmerkungen: *Diese Feststellung beschränkt sich auf den Bundesdatenschutzbeauftragten. Sie bezieht sich nicht auf die Datenschutzbeauftragten auf Länderebene und die für den privaten Bereich zuständigen Kontrollstellen.*
***Normalerweise ist in Italien keine gerichtliche Anordnung erforderlich, wenn eine Durchsuchung in der Wohnung einer Person oder in einer anderen privaten Wohnstätte mit Zustimmung dieser Person durchgeführt wird. Ansonsten ist eine richterliche Genehmigung erforderlich.*
****Die Datenschutzbehörde im Vereinigten Königreich kann Prüfungen nur auf Ersuchen des für die Verarbeitung Verantwortlichen durchführen; gegen den Willen eines für die Verarbeitung Verantwortlichen können keine Prüfungen vorgenommen werden. Die Befugnis kann somit nicht zur Kontrolle der Einhaltung der gesetzlichen Bestimmungen genutzt werden.*

Wie aus Tabelle 1 hervorgeht, sind die Datenschutzbehörden in der überwiegenden Mehrheit aller Mitgliedstaaten befugt, die Einhaltung der Datenschutzbestimmungen durch private und öffentliche Auftragsverarbeiter zu überwachen und insbesondere bei den Beteiligten Audits durchzuführen, Untersuchungen vorzunehmen, die Erteilung von Informationen anzuordnen, die Gewährung des Zugangs zu geschäftlichen Daten und Unterlagen anzuordnen sowie Daten und Unterlagen zu kopieren. Diese Befugnisse können von Amts wegen oder auf Ersuchen oder Antrag einer betroffenen Person, die Verstöße gegen ihre Rechte im Zusammenhang mit ihren personenbezogenen Daten geltend macht, ausgeübt werden. In der großen Mehrzahl der Mitgliedstaaten können Kontrollstellen im Rahmen der Ausübung ihrer Funktionen und zur Aufdeckung von Verstößen gegen die Datenschutzbestimmungen (gegebenenfalls mit Hilfe der Polizei) Räumlichkeiten und etwaige sonstige Orte, an denen eine Datenverarbeitung erfolgt, betreten, die nötige Ausrüstung beschlagnahmen, Untersuchungen durchführen und Beweismittel an sich nehmen; diese Möglichkeit besteht auch ohne Zustimmung des für die Datenverarbeitung Verantwortlichen und ohne die Notwendigkeit der vorherigen Beantragung einer richterlichen Anordnung.

4.1.3.2. Einwirkungsbefugnisse

Nach Artikel 28 Absatz 3 Satz 1 zweiter Spiegelstrich der Datenschutzrichtlinie verfügen Kontrollstellen über Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, vor der Durchführung der Verarbeitung sensibler Daten Gutachten abzugeben und für eine geeignete Veröffentlichung der Gutachten zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten. Die nachstehende Tabelle 2 enthält Informationen zum Grad der Umsetzung der oben genannten Bestimmung in den verschiedenen einzelstaatlichen Rechtsvorschriften, wobei angegeben wird, ob die Kontrollstellen über die folgenden Befugnisse verfügen: a) Registrierung der von den für die Verarbeitung Verantwortlichen gemeldeten Datenverarbeitungen; b) Genehmigung von Verarbeitungen, die voraussichtlich spezifische Risiken in Bezug auf die Rechte und Freiheiten betroffener Personen bergen werden, nachdem eine Vorabkontrolle der Vereinbarkeit dieser Verarbeitungen mit den Anforderungen der Datenschutzbestimmungen vorgenommen wurde; c) Unterbrechung der Verarbeitung personenbezogener Daten; d) Anordnung der Löschung oder Vernichtung von Daten; e) Verwarnung oder Ermahnung des für die Verarbeitung Verantwortlichen (d. h. durch Anordnung der Einführung spezifischer technischer und organisatorischer Maßnahmen zur Verhütung von Verstößen gegen relevante Rechtsvorschriften).

Tabelle 2: Einwirkungsbefugnisse

Mitgliedstaat	Registrierung von Verarbeitungen	Genehmigung von Verarbeitungen, die voraussichtlich spezifische Risiken bergen	Unterbrechung von Verarbeitungen	Anordnung der Löschung oder Vernichtung von Daten	Verwarnung oder Ermahnung des für die Verarbeitung Verantwortlichen
Belgien	●	●			
Bulgarien	●	●	●	●	●
Dänemark	●	●	●	●	●
Deutschland	●	●	●*		●
Estland	●	●	●	●	●
Finnland	●	●	●	●	●
Frankreich	●	●	●	●	●
Griechenland	●	●	●	●	●
Irland	●	●	●	●	●
Italien	●	●	●	●	●
Lettland	●		●	●	●
Litauen	●	●	●	●	●
Luxemburg	●	●	●	●	●
Malta	●	●	●	●	●
Niederlande	●	●	●	●	●
Österreich	●	●	●	●	●
Polen	●	●	●	●	●
Portugal	●	●	●	●	●
Rumänien	●	●	●	●	●
Schweden	●	●	●		●
Slowakei	●	●	●	●	●
Slowenien	●	●	●	●	●
Spanien	●		●	●	●
Tschechische Republik	●	●	●	●	●
Ungarn	●	●	●	●	●
Vereinigtes Königreich	●		●	●	●
Zypern	●		●	●	●

*Anmerkung: *Seit dem 1. September 2009 ist den Kontrollstellen freigestellt, unter bestimmten Bedingungen die Fortsetzung von Verarbeitungsvorgängen zu unterbinden.*

Tabelle 2 lässt eine gewisse Konvergenz der Datenschutzbehörden der EU-Mitgliedstaaten hinsichtlich der Einwirkungsbefugnis erkennen. Mit der begrenzten Ausnahme der Vorabkontrolle der Verarbeitung sensibler Daten, die in manchen Ländern nicht de jure oder de facto vorgesehen ist, sind alle Kontrollstellen verpflichtet, ein Register der Meldungen der Datenverarbeitungen zu führen. Abgesehen von Belgien und teilweise Deutschland können sie zudem: anordnen, dass ein privater für die Verarbeitung Verantwortlicher eine gegen die Datenschutzbestimmungen verstoßende Datenverarbeitung abbricht und spezifische Daten, die Gegenstand einer solchen Verarbeitung sind, berichtigt, löscht oder sperrt; privaten für die Verarbeitung Verantwortlichen die Nutzung eines festgelegten Verfahrens in Verbindung mit der Datenverarbeitung untersagen, wenn ein erhebliches Risiko besteht, dass Daten unter Verstoß gegen die geltenden Rechtsvorschriften verarbeitet werden; anordnen, dass private für die Verarbeitung Verantwortliche spezifische technische und organisatorische Sicherheitsmaßnahmen durchführen müssen, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die Weitergabe an unbefugte Personen, den Missbrauch von Daten und andere Formen der unrechtmäßigen Verarbeitung von Daten erforderlich sind; und schließlich ein Verbot oder eine einstweilige Verfügung gegen Auftragsverarbeiter erlassen, die gegen die einschlägigen Rechtsvorschriften verstoßen.[55]

4.1.3.3. Befugnis zur Befassung mit Eingaben und Klagerecht/Anzeigebefugnis

Nach Artikel 28 Absatz 4 Satz 1 der Datenschutzrichtlinie sollten Kontrollstellen über die nötigen Befugnisse verfügen, damit sich jede Person oder ein sie vertretender Verband zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten mit einer Eingabe an jede Kontrollstelle wenden kann; dabei ist die betroffene Person darüber zu informieren, wie mit der Eingabe verfahren wurde. Nach Artikel 28 Absatz 3 Satz 1 dritter Spiegelstrich müssen Datenschutzbehörden über das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Datenschutzbestimmungen verfügen. Schließlich haben Kontrollstellen nach Artikel 28 Absatz 3 Satz 1 zweiter Spiegelstrich die Befugnis, die Parlamente oder andere politische Institutionen zu befassen. Die nachstehende Tabelle 3 illustriert den Grad der Umsetzung der oben genannten Bestimmung in den Mitgliedstaaten, wobei angegeben wird, ob die Kontrollstellen über die folgenden Befugnisse verfügen: a) Befassung mit und Prüfung von Klagen oder Beschwerden von betroffenen Personen; b) Anzeigebefugnis bei den Polizei- oder Justizbehörden; c) direkte Befassung der Justizbehörden als klagende Partei (d. h. Klagerecht im eigentlichen Sinne); d) Möglichkeit der unmittelbaren Entscheidung über die Feststellung eines Verstoßes (einschließlich der Möglichkeit zur Verhängung von Sanktionen) und somit Übernahme einer quasirichterlichen Funktion; und e) Befassung der Parlamente oder anderer politischer Institutionen, insbesondere durch den Vorschlag legislativer und regulatorischer Maßnahmen zur Änderung der einschlägigen Datenschutzbestimmungen, um die wichtigsten, aus der Anwendung dieser Bestimmungen resultierenden Probleme anzugehen und die Entwicklung computergestützter Verarbeitungsverfahren zu berücksichtigen.

55 Die Feststellung beschränkt sich auf die Zuständigkeit der Datenschutzbeauftragten der Länder und/oder der für den privaten Bereich zuständigen Kontrollstellen. Sie bezieht sich nicht auf den Bundesdatenschutzbeauftragten.

Tabelle 3: Befugnis zur Befassung mit Eingaben und Klagerecht

Mitgliedstaat	Befassung mit und Prüfung von Klagen oder Beschwerden	Anzeigebefugnis bei Polizei- oder Justizbehörden	Direkte Befassung der Justizbehörden	Unmittelbarer Erlass einer Entscheidung über die Eingabe	Befassung der nationalen Parlamente
Belgien	●	●	●	●	●
Bulgarien	●	●	●	●	
Dänemark	●	●		●	
Deutschland	●	●	●*	●*	●
Estland	●			●	●
Finnland	●	●	●	●	●
Frankreich	●	●		●	●
Griechenland	●	●		●	●
Irland	●		●		
Italien	●	●		●	●
Lettland	●		●	●	
Litauen	●	●		●	●
Luxemburg	●	●	●	●	
Malta	●	●	●	●	●
Niederlande	●	●		●	
Österreich	●		●	●	
Polen	●	●		●	
Portugal	●	●		●	
Rumänien	●	●	●	●	
Schweden	●	●	●		
Slowakei	●	●		●	●
Slowenien	●	●	●	●	
Spanien	●	●		●	
Tschechische Republik	●	●	●	●	
Ungarn	●	●			●
Vereinigtes Königreich	●	●			
Zypern	●	●		●	

*Anmerkung: *Diese Feststellung bezieht sich nicht auf den Bundesdatenschutzbeauftragten in Deutschland, sondern auf die Datenschutzbehörden auf Länderebene.*

Aus der Tabelle werden gewisse Unterschiede zwischen den Datenschutzbehörden der einzelnen EU-Mitgliedstaaten deutlich. Alle Kontrollstellen haben die Befugnis zur Befassung mit Eingaben von Beteiligten, die einen Verstoß gegen ihre Rechte im Zusammenhang mit ihren personenbezogenen Daten geltend machen, und sind dementsprechend verpflichtet, dem Beschwerdeführer innerhalb einer festgelegten Zeit eine Antwort zukommen zu lassen. Erweist sich eine Eingabe am Ende einer Untersuchung als begründet, können allerdings nur manche nationale Datenschutzbehörden eigenständig ein Gerichtsverfahren vor einem zuständigen Gericht anstrengen (in Slowenien sogar vor dem Verfassungsgericht), oder unmittelbar eine quasirichterliche Funktion übernehmen und unmittelbar über die Eingabe des Klägers entscheiden (als alternatives Forum zu ordentlichen Gerichten). Entscheidungen der administrativen Kontrollstellen mit quasirichterlichen Befugnissen sind in jedem Fall stets vor ordentlichen Gerichten anfechtbar. Dies ergibt sich als notwendige Konsequenz aus dem in Artikel 28 Absatz 3 Satz 2 der Datenschutzrichtlinie vorgesehenen Rechtsweg.

4.1.3.4. Beratungsbefugnisse

Nach Artikel 28 Absatz 2 der Datenschutzrichtlinie sollten Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten von einzelstaatlichen Gesetzgebern und Verwaltungen angehört werden. Aus dem Zweck der Datenschutzrichtlinie kann somit auf eine allgemeine Befugnis der Datenschutzbehörden geschlossen werden, an Datenverarbeitungen beteiligte private Parteien zu beraten und zu informieren und allgemeine sektorspezifische Empfehlungen abzugeben. Schließlich enthält Artikel 25 der Datenschutzrichtlinie spezifische Vorschriften zur Regelung der Übermittlung personenbezogener Daten in Nicht-EU-Länder (d. h. Drittländer), die möglicherweise Raum für ein Einwirken einzelstaatlicher Kontrollstellen lassen. Die nachstehende Tabelle 4 enthält Informationen zu den Beratungsbefugnissen der nationalen Datenschutzbehörden und erläutert, ob die Kontrollstellen: a) vor der Inkraftsetzung von Rechtsvorschriften oder Rechtsverordnungen, die Auswirkungen auf die datenschutzrelevanten Rechte von Personen haben, de jure oder de facto vom Gesetzgeber und/oder von Verwaltungsstellen stets angehört werden; b) vor der Inkraftsetzung von Rechtsvorschriften oder von Rechtsverordnungen, die Auswirkungen auf die datenschutzrelevanten Rechte von Personen haben, nach freiem Ermessen des Gesetzgebers und/oder der Verwaltungsstellen angehört werden können; c) die Parteien beraten und von diesen konsultiert werden (d. h. diese über ihre Rechte und Pflichten unterrichten); d) allgemeine Empfehlungen und Gutachten zu den Möglichkeiten einer Verbesserung der Umsetzung und Einhaltung der Datenschutzbestimmungen in spezifischen Sektoren abgeben (d. h. die Ausarbeitung von Verhaltenskodizes unterstützen); und e) die Übermittlung von personenbezogenen Daten in Drittländer genehmigen.

Tabelle 4: Beratungsbefugnisse

Mitgliedstaat	Müssen durch den Gesetzgeber oder durch Verwaltungsstellen angehört werden	Können durch den Gesetzgeber oder durch Verwaltungsstellen angehört werden	Beraten und informieren an der Datenverarbeitung beteiligte Parteien	Geben allgemeine Empfehlungen und Gutachten ab	Genehmigen die Übermittlung von Daten in Drittländer
Belgien	●	●	●	●	
Bulgarien	●		●	●	
Dänemark		●	●	●	●
Deutschland	●	●	●	●	●*
Estland	●		●	●	
Finnland	●	●	●	●	
Frankreich	●	●	●	●	●
Griechenland	●	●	●	●	●
Irland		●	●	●	●
Italien	●	●	●	●	●
Lettland	●		●	●	
Litauen		●	●	●	●
Luxemburg	●		●	●	●
Malta		●	●	●	●
Niederlande	●		●	●	●
Österreich	●		●	●	●
Polen		●	●	●	
Portugal	●		●	●	●
Rumänien		●	●	●	●
Schweden	●	●	●	●	●
Slowakei		●**	●	●	●
Slowenien		●	●	●	●
Spanien	●		●	●	●
Tschechische Republik		●	●	●	
Ungarn		●	●	●	●***
Vereinigtes Königreich		●	●	●	●****
Zypern	●*****		●	●	●

*Anmerkungen: *Deutsche Kontrollstellen können Genehmigungen erteilen, dies ist jedoch nicht in allen Fällen vorgeschrieben oder notwendig.*

***In der Slowakei wird die Datenschutzbehörde vor der Inkraftsetzung von Rechtsvorschriften mit Auswirkungen auf den Datenschutz de facto immer angehört, wenngleich dies durch das Gesetz nicht zwingend vorgeschrieben ist.*

****Es gibt Hinweise darauf, dass diese Befugnis durch das Fehlen einer wirksamen Durchsetzung unterlaufen wird.*

*****In der Praxis scheint diese Befugnis, wenn überhaupt, selten genutzt zu werden. Siehe nationale thematische Studie zur Bewertung von Datenschutzmaßnahmen sowie der zuständigen Einrichtungen im Vereinigten Königreich (http://fra.europa.eu (24.2.2010)).*

******Abschnitt 23 Ziffer (i) des Gesetzes 138(I)/2001 wird von der Datenschutzbehörde Zyperns derart ausgelegt, dass er ihr das Recht einräumt, bei der Erörterung von Rechtsverordnungen angehört zu werden. In der Praxis wird der Datenschutzbeauftragte ausnahmslos immer dann vom Gesetzgeber und den Verwaltungsstellen angehört, wenn es zu Problemen in Bezug auf den Schutz personenbezogener Daten kommt.*

Wie aus Tabelle 4 hervorgeht, haben alle Mitgliedstaaten ihren einzelstaatlichen Kontrollstellen die Befugnis übertragen, private Parteien hinsichtlich der Anwendung der datenschutzrechtlichen Bestimmungen zu beraten. Datenschutzbehörden haben auch die quasi-legislative Befugnis, allgemeine Rechtsverordnungen für spezifische Sektoren zu erarbeiten, die Ausarbeitung privater Verhaltenskodizes zu fördern und Gutachten und Empfehlungen für im Bereich des Datenschutzes tätige öffentliche und private Akteure abzugeben. Diese Maßnahmen sind jedoch meist nicht rechtsverbindlich. Gleichzeitig gestehen viele Mitgliedstaaten den Kontrollstellen bei der Beratung der Exekutive und der Legislative im Hinblick auf Gesetzesvorlagen zum Schutz personenbezogener Daten eine Konsultationsfunktion zu. Ihre Ratschläge zu Gesetzesvorlagen und Verordnungsentwürfen sind daher optional oder (wie in Deutschland, Frankreich, Griechenland, Italien und Österreich) nur bei der Ausarbeitung von Durchführungsvorschriften rechtlich absolut erforderlich. Dies ist insoweit bedauerlich, als eine Beratung bereits in einem frühen Stadium dazu beitragen könnte, künftige Probleme zu vermeiden. Das Fehlen von Gutachten der Datenschutzbehörden vor der Inkraftsetzung von Rechtsvorschriften oder Rechtsverordnungen, die möglicherweise nachteilige Auswirkungen auf den Schutz personenbezogener Daten haben können, kann jedoch ein Anzeichen dafür sein, dass der Bedeutung des Schutzes der Privatsphäre bei politischen Entscheidungen nicht in vollem Umfang Rechnung getragen wird. Daher empfiehlt sich die Sicherstellung einer kohärenteren Einbeziehung von Kontrollstellen in den Prozess der Politikgestaltung seitens der Mitgliedstaaten.

4.1.4. Maßnahmen

Die Kontrollstellen der EU-Mitgliedstaaten beteiligen sich gemeinsam an einer Reihe von Tätigkeiten zur Bewertung des Standes der einzelstaatlichen Rechtsvorschriften über die Privatsphäre sowie zur Verbreitung der Kultur des Schutzes personenbezogener Daten. Zunächst haben Datenschutzbehörden die Aufgabe, die breite Öffentlichkeit und die staatlichen Institutionen über die Herausforderungen hinsichtlich des Rechts auf Schutz der Privatsphäre, die zur Bewältigung dieser Herausforderungen von der Datenschutzbehörde ergriffenen Maßnahmen und die zur Verbesserung der Verteidigung dieses Rechtes nötigen Schritte der jeweiligen Kontrollstelle zu unterrichten. Nach Artikel 28 Absatz 5 der Datenschutzrichtlinie sind die Kontrollstellen verpflichtet, regelmäßig einen Bericht über ihre Tätigkeit vorzulegen und zu veröffentlichen. Alle Datenschutzbehörden veröffentlichen daher Jahresberichte über die Situation im Hinblick auf den Schutz des Rechtes auf Privatsphäre im jeweiligen innerstaatlichen Rechtssystem, manche von ihnen (z. B. Italien) veröffentlichen sogar monatliche Bulletins mit den in jüngster Zeit erlassenen Entscheidungen oder Rechtsverordnungen. In einigen Ländern (z. B. in Frankreich, Italien, Spanien und im Vereinigten Königreich) wird der Jahresbericht öffentlich vorgestellt (in einigen Ländern dem Gesetzgeber), und die Massenmedien sind in der Lage, über dieses Ereignis zu berichten.

Einzelstaatliche Kontrollstellen haben eine besondere Verpflichtung, die EU-Bürger für das Recht auf den Schutz der Privatsphäre und der personenbezogenen Daten zu sensibilisieren. Dieses Unterfangen ist insoweit von besonderer Bedeutung, als die Wirksamkeit von Datenschutzbestimmungen nur dann sichergestellt werden kann, wenn sich jeder Einzelne seiner Grundrechte bewusst ist und aktiv zu deren Gewährleistung beiträgt. Wie im Folgenden erläutert, ist sich die breite Öffentlichkeit in mehreren Mitgliedstaaten (z. B. in Malta oder in Polen) entweder ihrer Rechte nicht bewusst bzw. setzt einfach voraus, dass das Recht auf Privatsphäre gut geschützt ist und dass nur in begrenztem Umfang Maßnahmen zur Verbesserung des Systems ergriffen werden müssen (z. B. in Dänemark oder in Finnland), oder ist der Auffassung, dass Datenschutzrechte anderen Rechten, beispielsweise dem Recht auf Information, untergeordnet werden sollten (z. B. in Schweden). Datenschutzbehörden engagieren sich daher direkt im Bereich der Sensibilisierung. Mit wenigen Ausnahmen (z. B. in Bulgarien, Litauen und in der Slowakei) betreiben sie spezialisierte, benutzerfreundliche Websites, auf denen alle relevanten Rechtsvorschriften, Gutachten und Entscheidungen der Datenschutzbehörde verfügbar sind und kontinuierlich aktualisiert werden. In vielen Ländern (z. B. in den Niederlanden und in Slowenien) werden von den Kontrollstellen Konferenzen, Initiativen und Sonderprogramme finanziert, um spezifische Bevölkerungsgruppen (Schüler und Studenten, Arbeitnehmer usw.) gezielt anzusprechen.

Auf EU-Ebene kooperieren die einzelstaatlichen Kontrollstellen im Rahmen der gemäß Artikel 29 Absatz 1 Satz 1 der Datenschutzrichtlinie eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (der so genannten „Artikel-29-Datenschutzgruppe"). Nach Artikel 29 Absatz 2 umfasst die Gruppe den Europäischen Datenschutzbeauftragten (EDSB), je einen Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einen Vertreter der Europäischen Kommission. Die Gruppe ist unabhängig und hat beratende Funktion. Nach Artikel 30 Absatz 1 soll die Gruppe alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften prüfen, um zu einer einheitlichen Anwendung beizutragen; zum Schutzniveau in der EU und in Drittländern gegenüber der Kommission Stellung nehmen; die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen beraten, die sich auf diese Rechte und Freiheiten auswirken; und Gutachten zu den auf EU-Ebene erarbeiteten Verhaltensregeln abgeben. Die nationalen Datenschutzbehörden nehmen generell auf die Gutachten und Empfehlungen der Gruppe Bezug und berücksichtigen die Gutachten und Empfehlungen; diese sind besonders hilfreich für die Entwicklung eines gemeinsamen EU-Standards für den Schutz personenbezogener Daten, der von allen einzelstaatlichen Kontrollstellen geteilt wird.[56]

4.2. Einhaltung der Standards

Dieser Abschnitt bietet einen vergleichenden Überblick. Vielversprechende Praktiken in diesem Zusammenhang sind in Abschnitt 6.2 beschrieben.

4.2.1. Datenschutz-Registrierungen und Genehmigungsverfahren

Laut Artikel 2 der Datenschutzrichtlinie umfasst die Bezeichnung „Verarbeitung personenbezogener Daten" („Verarbeitung") jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die

56 Im Vereinigten Königreich werden Gutachten und Empfehlungen der Gruppe von der nationalen Datenschutzbehörde nicht als bindend betrachtet, wenngleich die nationale Datenschutzbehörde die Gutachten und Empfehlungen der Gruppe verschiedentlich als informelle Leitlinien berücksichtigt.

Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten von Daten. Darüber hinaus sind in den Artikeln 5 bis 8 der Datenschutzrichtlinie die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, die Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten sowie besondere Kategorien der Verarbeitung solcher Daten festgelegt. Diesbezüglich sehen die Artikel 18 bis 20 die Pflicht zur Meldung bei der Kontrollstelle und die Vorabkontrolle von Verarbeitungen vor, die spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können.

Die Beurteilung der Einhaltung von Datenschutzstandards (z. B. Regeln für Datenschutz-Registrierungen und Datenschutz-Genehmigungsverfahren) beruhte weitgehend auf den einzelstaatlichen thematischen Studien. Zum überwiegenden Teil stützten sich diese Studien auf Angaben zur Anzahl der Registrierungen und Genehmigungen für die Jahre 2000-2007. Mehrere Studien beinhalteten Analysen und qualitative Bewertungen, die sowohl auf diesen Zahlen als auch auf Kontakten mit den jeweiligen nationalen Datenschutzbehörden basierten. Diese Zahlen dienten als Indikatoren für die Beurteilung der Einhaltung der Standards. Weitere Indikatoren sind die Praktiken der nationalen Datenschutzbehörden, der Grad der Einhaltung einzelstaatlicher Rechtsvorschriften und Beispiele für Verstöße gegen die Richtlinie.

Die meisten Mitgliedstaaten der EU (Bulgarien, Dänemark, Deutschland, Estland, Finnland, Griechenland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowenien, Spanien, die Tschechische Republik und Zypern) haben einen Rechtsrahmen erarbeitet, durch den die Vorgaben der Datenschutzrichtlinie wirksam umgesetzt werden. „Wirksame Umsetzung" bedeutet, dass die einzelstaatlichen Rechtsvorschriften *prima facie* den Anforderungen der Richtlinie entsprechen. Die Wirksamkeit der tatsächlichen Umsetzung durch die einzelstaatlichen Rechtsvorschriften ist von Mitgliedstaat zu Mitgliedstaat verschieden und wird in den folgenden Absätzen eingehender analysiert. Andererseits gibt es in fünf Mitgliedstaaten (in Belgien, Frankreich, in der Slowakei, in Ungarn und im Vereinigten Königreich) Hinweise auf Unzulänglichkeiten der Gesetze, die zu Unstimmigkeiten zwischen dem durch die Datenschutzrichtlinie geschaffenen allgemeinen System und den einzelstaatlichen Bestimmungen führen. Die Beurteilung der Einhaltung der Standards ist jedoch verhältnismäßig problematisch. In vielen Fällen können die nationalen Datenschutzbehörden aus Personalmangel keine systematische und statistische Darstellung der Situation vor Ort liefern. Aber auch wenn diese statistischen Daten vorliegen, sind sie nicht immer kohärent und ausreichend, um die Situation ordnungsgemäß darstellen zu können. Es war daher unmöglich, zu einer EU-weiten und umfassenden Gesamtbeurteilung des Grades der Einhaltung der Standards und/oder der in den Gesetzen und in der Praxis problematischen Bereiche zu gelangen. Aus diesem äußerst uneinheitlichen Bild wurden Beispiele für offenkundige Fälle von Nichteinhaltung der Standards aus den einzelstaatlichen thematischen Studien herausgegriffen, um einige der aufgetretenen Probleme zu verdeutlichen.

Bulgarien hat die maßgeblichen Bestimmungen der Datenschutzrichtlinie umgesetzt; im Bereich der Registrierung zeigt die Praxis der für die Verarbeitung personenbezogener Daten Verantwortlichen jedoch, dass die einzelstaatliche Datenschutzbehörde bei Aufnahme ihrer Tätigkeit nicht hinreichend für den Aufbau der administrativen Kapazitäten zur Erfüllung ihrer Aufgaben bereit war.[57] Die einzelstaatliche Datenschutzbehörde ist noch nicht in der Lage, die große Zahl von Registrierungsanträgen effektiv zu bearbeiten. Die Zahl der Anträge steht insoweit im Missverhältnis zur Anzahl der Registrierungen, als die Anzahl der Registrierungen im Vergleich zur Anzahl der Registrierungsanträge nach wie vor unverhältnismäßig niedrig ist.[58]

In Polen ist den einzelstaatlichen Rechtsvorschriften zufolge jede mit der Verarbeitung von Daten befasste Stelle verpflichtet, eine Datei mit personenbezogenen Daten bei der einzelstaatlichen Datenschutzbehörde registrieren zu lassen, die über begrenzte Befugnisse zur Untersuchung von seitens besonderer staatlicher Stellen (z. B. Nachrichtendiensten) verarbeitete Daten verfügt. Auch wenn eine Daten verarbeitende Stelle nicht zur Registrierung der Datenverarbeitung verpflichtet ist, muss sie die Voraussetzungen für die Möglichkeit einer Datenverarbeitung erfüllen. Die Verarbeitung sensibler Daten ist generell untersagt; bestehende Ausnahmen sind zum großen Teil durch die Bestimmungen der Datenschutzrichtlinie gedeckt. Das wichtigste festgestellte Problem ist die fehlende Sensibilisierung Daten verarbeitender Stellen für die Registrierungspflicht. In zahlreichen Fällen wurden Dateien mit personenbezogenen Daten von diesen Stellen nicht registriert; zudem treten in der Registrierungsphase zahlreiche Fehler auf. Die Verarbeitung sensibler Daten hat in zwei signifikanten Fällen zu Problemen geführt. Einer dieser Fälle bezieht sich auf die Erhebung von Daten über Roma-Kinder. In diesem Fall ordnete die einzelstaatliche Datenschutzbehörde die Löschung der Daten über Roma-Kinder an, deren Verarbeitung ohne ihr Wissen und ihre Zustimmung erfolgt war.[59] Der zweite Fall betraf die Verarbeitung der Daten von Wahlkandidaten, die verschiedenen nationalen und ethnischen Minderheiten angehörten. Die einzelstaatliche Datenschutzbehörde ordnete die Aussetzung der Verarbeitung von Daten an, die aus nicht amtlichen Quellen ohne Zustimmung der betroffenen Personen gewonnen worden waren.[60] Der Bericht der einzelstaatlichen Datenschutzbehörde aus dem Jahr 2007 machte auf die mangelnde Einhaltung der Datenschutzstandards in bestimmten Bereichen der öffentlichen Verwaltung aufmerksam.[61] Im Bereich der öffentlichen Sicherheit waren hinsichtlich des Datenschutzes keine besonderen Defizite festzustellen, und die Einrichtungen scheinen die Bestimmungen der Rechtsvorschriften zu befolgen. Bei verschiedenen gewerblichen Bereichen, Einrichtungen im Gesundheitswesen, Banken und Finanzinstituten wurde allerdings festgestellt, dass Daten verarbeitende Stellen die gesetzlichen Bestimmungen nicht vollständig erfüllten.

In Griechenland führte die Legislative anfänglich ein universelles Meldesystem ein und verzichtete damit auf die in der Datenschutzrichtlinie vorgesehene Möglichkeit der Einführung von Ausnahmen und Vereinfachungen bei den Registrierungs- und Meldeverfahren. Diese

57 Im Dezember 2003 sahen sich vier Mitarbeiter der einzelstaatlichen Datenschutzbehörde mit 227 251 Anträgen konfrontiert. Jahresbericht der Kommission für den Schutz personenbezogener Daten der Republik Bulgarien 2002-2003, S. 11-12, abrufbar auf Bulgarisch unter: www.cpdp.bg/godishniotcheti.html.

58 Beispielsweise belief sich im Jahr 2006 die Zahl der Anträge auf 274 446, die der Registrierungen dagegen auf 31 970. Jahresbericht der Kommission für den Schutz personenbezogener Daten der Republik Bulgarien 2006, S. 17, siehe: www.cpdp.bg/godishniotcheti.html (Bulgarisch).

59 Entscheidung vom 12. Oktober 2007, Aktenzeichen: GI-DEC-DOLiS-218/07/5787, 5788.

60 Entscheidung vom 23. November 2007, Aktenzeichen: GI-DOLiS-430/103/07/6592.

61 Dazu zählten die Aufbewahrung von Daten unter unsachgemäßen Bedingungen (z. B. in nicht abschließbaren Regalen und Schubladen), der Einsatz von IT-Systemen, die häufig nicht die gesetzlich vorgeschriebenen technischen Anforderungen erfüllten, der vereinzelte Einsatz von IT-Systemen, die unbefugten Personen den Zugriff auf Dateien gestatteten, die Nutzung der im Verlauf von Verwaltungsverfahren erhobenen Daten für andere Ziele als den angegebenen Zweck und – in einzelnen Fällen – die Veröffentlichung personenbezogener Daten auf einer Website ohne vorherige Zustimmung.

Möglichkeit zur Einführung von Ausnahmen wurde mit einer späteren Änderung des Gesetzes geschaffen; diese Änderung führte zu einem drastischen Rückgang der Meldezahlen. Der griechische Gesetzgeber hat die in der Datenschutzrichtlinie vorgesehene Option der Benennung eines internen Datenschutzbeauftragten nicht aufgegriffen. Aufgrund der inhärenten asymmetrischen Machtverhältnisse in der Arbeitgeber-Arbeitnehmer-Beziehung lehnt die einzelstaatliche Datenschutzbehörde die Zustimmung der betroffenen Person als alleinige Legitimation einer Verarbeitung personenbezogener Daten ab.[62] Hinsichtlich der Befolgung der Entscheidungen der einzelstaatlichen Datenschutzbehörde ist festzustellen, dass die für die Verarbeitung Verantwortlichen die betreffenden Entscheidungen in der großen Mehrzahl aller Fälle befolgen. Ein Verstoß gegen die Standards, der große Bekanntheit erlangte und schwerwiegende Bedenken und öffentliche Empörung hervorrief, war der Einsatz von CCTV-Systemen zum Filmen politischer Demonstrationen durch die griechische Polizei, entgegen verbindlicher anderweitiger Entscheidungen der einzelstaatlichen Datenschutzbehörde über den Einsatz von Kameras im öffentlichen Raum,[63] noch bevor das Plenum des Staatsrats über das Gesetz zum Schutz personenbezogener Daten entschieden hatte.[64] Überdies wurde den Prüfern der Datenschutzbehörde der Zutritt zu den Räumlichkeiten der Polizei zum Zweck der Kontrolle der Befolgung der Entscheidungen der Datenschutzbehörde verweigert. Der Vorsitzende und die meisten Mitglieder der Datenschutzbehörde reichten danach ihren Rücktritt ein.

Im Zusammenhang mit dem Vereinigten Königreich untersucht die Europäische Kommission Meldungen zufolge die mutmaßliche nicht ordnungsgemäße Umsetzung von 11 der 34 Artikel der Richtlinie; dieser Anteil entspricht fast einem Drittel der Bestimmungen der Richtlinie.[65] Wenngleich die Regierung des Vereinigten Königreichs noch immer geltend macht, die Richtlinie vollständig umgesetzt zu haben, wurden zahlreiche Unzulänglichkeiten aufgezeigt.[66] Und nochmals problematischer ist die Darstellung der einzelstaatlichen Datenschutzbehörde dahingehend, dass sie nicht als ihre Aufgabe ansieht, die Auslegung des einzelstaatlichen Gesetzes in einer der Kommissionsrichtlinie entsprechenden Weise sicherzustellen oder aufzuzeigen, an welchen Stellen das einzelstaatliche Gesetz möglicherweise die Anforderungen der Datenschutzrichtlinie nicht erfüllt.[67]

Deutschland hat die Datenschutzrichtlinie sowohl auf Bundes- als auch auf Länderebene umgesetzt. Nichtöffentliche Stellen sind verpflichtet, automatisierte Datenverarbeitungen vorab der Kontrollstelle oder dem zuständigen Datenschutzbeauftragten zu melden. Öffentliche Stellen des Bundes haben diese der einzelstaatlichen Datenschutzbehörde zu melden. Die Registrierungspflicht gilt nicht, wenn der für die Verarbeitung Verantwortliche einen internen Datenschutzbeauftragten benannt hat. Eine erhebliche Anzahl privatwirtschaftlicher Unternehmen, die gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet sind, scheint dieser Verpflichtung nicht nachzukommen, und Unternehmen, die der allgemeinen Verpflichtung zur Benennung eines Datenschutzbeauftragten nachkommen, dürften für die effiziente und effektive Arbeit der benannten Personen nicht unbedingt förderlich sein. Zudem kann nicht außer Acht gelassen werden, dass in den meisten mittleren Unternehmen noch immer verschiedene Probleme im Bereich des Datenschutzes bestehen; diese Probleme sind darauf zurückzuführen, dass die benannten Datenschutzbeauftragten – sofern eine Benennung denn überhaupt erfolgt ist – aus Zeitgründen die für ihre eigene Weiterbildung oder für die Erfüllung ihrer Aufgaben die möglicherweise erforderlichen datenschutzrelevanten Veränderungen der Unternehmenspraktiken nicht initiieren können. Die Skandale der letzten Zeit, in die sowohl private als auch öffentliche Einrichtungen verwickelt waren, deuten auf ausgedehnte, ernstzunehmende und massenhafte Verstöße gegen das Recht auf Datenschutz und Schutz der Privatsphäre hin.[68] In den betreffenden Fällen geht es unter anderem um schwere Verstöße gegen das Recht auf Privatsphäre, indem Mitarbeiter per Video ausspioniert oder heimlich beobachtet wurden oder indem am Arbeitsplatz nach Computerprofilen von Mitarbeitern gesucht wurde. In anderen Fällen wurde in beispiellosem Umfang mit Daten gehandelt, ohne dass die betroffenen Personen vorab eine entsprechende Genehmigung erteilt hatten.[69] In vielen Fällen wird das Problem durch das Fehlen angemessener Maßnahmen (z. B. im Bereich der Strafverfolgung) verschärft.

62 Ein Ansatz, der auch von der Europäischen Kommission im Bericht *Possible content of a European framework on protection of workers' personal data* (Mögliche Inhalte eines europäischen Rahmens zum Schutz der personenbezogenen Daten von Arbeitnehmern), Brüssel 2002, vertreten wird.

63 Entscheidung 58/2005 der nationalen Datenschutzbehörde *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*, www.dpa.gr/portal/page?_pageid=33,15453&_dad=portal&_schema=PORTAL.

64 Das griechische Ministerium für öffentliche Ordnung stellte einen Antrag beim Staatsrat, durch den es die Entscheidungen der Datenschutzbehörde aufzuheben versuchte.

65 „Europe claims UK botched one third of Data Protection Directive" (Europa behauptet, das Vereinigte Königreich habe ein Drittel der Datenschutzrichtlinie verdorben), Out-Law News, 17. September 2007, abrufbar unter: www.out-law.com/page-8472; wenngleich dies an sich ein Presse-Artikel ist, basiert er auf Informationen, die im Rahmen des Gesetzes über die Informationsfreiheit direkt von den betroffenen Behörden stammen, und sowohl die Regierung des Vereinigten Königreichs als auch die Kommission bestätigten, dass verschiedene Fragen erörtert würden, ohne jedoch genaue Angaben zu machen. Die Informationen der Out-Law News zeigten jedoch, dass „es sich bei den Artikeln der Richtlinie, die den Behauptungen der Kommission zufolge nicht ordnungsgemäß umgesetzt wurden, um die Artikel 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 und 28 handelt (...). Diese Artikel beziehen sich auf: die in der Richtlinie verwendeten Begriffsbestimmungen (z. B. die Bedeutung des Begriffs ‚personenbezogene Daten'); den Geltungsbereich der Anwendung der Richtlinie auf manuelle Dateien; die Bedingungen, unter denen sensible personenbezogene Daten verarbeitet werden können; die Unterrichtung der betroffenen Personen über eine Verarbeitung nach Treu und Glauben; die Rechte, die betroffenen Personen gewährt werden; die Anwendung von Ausnahmen von diesen Rechten; die Fähigkeit jeder Person, im Falle einer Verletzung ihrer Rechte Rechtsbehelfe nutzen zu können; die Haftung von Organisationen für Verstöße gegen das Datenschutzgesetz; die Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union; und die Befugnisse des Informationsbeauftragten."

66 Zum Beispiel D. Korff (2008) *UK Data Sharing: European Conflict* (Datenaustausch im Vereinigten Königreich: ein europäischer Konflikt), in: *Data Protection Law & Policy*, S. 12 ff; andere Fragen wurden in einer in der nächsten Fußnote genannten Anfrage angesprochen; siehe auch R. Thomas und M. Walport (2008) *Data Sharing Review Report* (Überprüfungsbericht zum Thema Datenaustausch), siehe: www.justice.gov.uk/docs/data-sharing-review-report.pdf.

67 Eine Frage eines Sonderausschusses des Unterhauses während einer Anhörung zur Einführung der elektronischen Patientenakte im staatlichen Gesundheitsdienst während einer Sitzung im Mai 2007 beantwortete Jonathan Bamford, der stellvertretende Informationsbeauftragte, wie folgt: „Die Frage, ob die Datenschutzrichtlinie der EU durch das Datenschutzgesetz des Vereinigten Königreichs ordnungsgemäß umgesetzt wird, ist vom Justizministerium zu klären; das Justizministerium ist dafür zuständig, dass wir die Richtlinie in britisches Recht umsetzen. Wenn Bedenken über gewisse Unterschiede bestehen, muss das Justizministerium auf diesen Punkt reagieren. Es ist Aufgabe des Informationsbeauftragten, das Datenschutzgesetz des Vereinigten Königreichs umzusetzen. (...) Wenn Sie ernsthafte Bedenken [in Bezug auf eine eventuell nicht ordnungsgemäße Umsetzung der Richtlinie durch das Gesetz] haben, sollten Sie im Rahmen dieser Anfrage meiner Ansicht nach unbedingt mit dem Justizministerium sprechen." Antwort auf Frage 176 in der Anhörung des Sonderausschusses am 10. Mai 2007; vollständige Niederschrift siehe: www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm.

68 www.heise.de/tp/r4/artikel/28/28579/1.html, www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302,350317, www.tagesschau.de/inland/datenschutz110.html, www.sol.de/news/welt/tagesthema/Datenschutz;art7325,2705543, www.ruhrnachrichten.de/nachrichten/politik/blickpunkt/art302,433610, http://ez.omg.de/?id=20&nid=29923, www.handelsblatt.com/unternehmen/handel-dienstleister/rasterfahndung-bei-der-bahn;2136145.

69 Siehe: www.aufrecht.de/news/view/article/illegaler-handel-mit-adress-und-kontodaten-sprengt-alle-grenzen.html.

4.2.2. Benennung interner Datenschutzbeauftragter

In Bezug auf die Benennung interner Datenschutzbeauftragter sehen die meisten einzelstaatlichen Gesetze allgemeine Anforderungen vor; spezifische Kenntnisse oder einschlägige Erfahrungen werden nicht verlangt. In Dänemark, Griechenland und Italien sehen die Rechtsvorschriften die Benennung von Datenschutzbeauftragten nicht vor. In Belgien enthält der maßgebliche Königliche Erlass keine Aussagen zur Politik für die Benennung interner Datenschutzbeauftragter. In der Erläuterung zum Königlichen Erlass vom 13. Februar 2001 zur Ausführung des Datenschutzgesetzes erklärt die Regierung explizit, dass die Idee der Benennung einer solchen Person in Belgien keine Unterstützung erfahren habe. In Österreich begründet die Gesetzgebung keinerlei Verpflichtung zur Benennung interner Datenschutzbeauftragter, aber im öffentlichen Sektor setzen sich die Gewerkschaften für die Benennung interner Datenschutzbeauftragter ein. Bei den übrigen Mitgliedstaaten sind im Wesentlichen zwei Kategorien zu unterscheiden: a) Mitgliedstaaten, deren einzelstaatliche Gesetzgebung bestimmte zu erfüllende Anforderungen vorsieht, und b) Mitgliedstaaten, in denen dies nicht der Fall ist. Die einzelstaatliche Gesetzgebung mancher Mitgliedstaaten (Bulgarien, Estland, Finnland,[70] Irland, Litauen, Portugal, Rumänien, Schweden, Slowenien, Vereinigtes Königreich und Zypern[71]) enthält keine Anforderungen für die Benennung von Datenschutzbeauftragten. In den anderen Mitgliedstaaten (Deutschland, Frankreich, Lettland, Luxemburg, Malta, Niederlande, Polen, Slowakei, die Tschechische Republik und Ungarn) enthält die einzelstaatliche Gesetzgebung ausdrückliche Bestimmungen zur Unabhängigkeit bzw. zu angemessenen einschlägigen Kenntnissen und Erfahrungen der Datenschutzbeauftragten. Es ist anzumerken, dass diese Anforderungen nicht weiter ausgeführt werden. Die einzigen Ausnahmen sind Ungarn und Lettland, wo ein interner Datenschutzbeauftragter einen Hochschulabschluss in Rechtswissenschaften, Verwaltungswissenschaften oder Informationstechnologie bzw. eine gleichwertige Qualifikation vorweisen muss, damit er innerhalb der Organisation als für die Verarbeitung Verantwortlicher oder technischer Auftragsverarbeiter benannt oder bevollmächtigt werden kann.

Bei der Beurteilung der Anforderungen für die Benennung von Datenschutzbeauftragten muss berücksichtigt werden, dass die Rechtsvorschriften der EU keine spezifischen verpflichtenden Standards vorsehen. Es ist jedoch offensichtlich, dass die Benennung von Personen mit besonderen Fachkenntnissen und/oder einer besonderen Sensibilisierungsfunktion dazu beiträgt, die Befolgung und die vollständige Umsetzung der geltenden Rechtsvorschriften sicherzustellen. Ungeachtet der Fähigkeiten und des Kenntnisstands der Datenschutzbeauftragten ist zu betonen, dass die Praxis ihrer Einstellung durch einen Teilbereich der Exekutive nicht zur Unabhängigkeit der nationalen Datenschutzbehörden beiträgt. Ferner hat sich ein Mitgliedstaat (Irland) für die Verabschiedung von Leitlinien entschieden, und zwei weitere Mitgliedstaaten (Schweden und die Slowakei) haben besondere Schulungsmaßnahmen für die Datenschutzbeauftragten vorgesehen. Abschließend ist festzustellen, dass in Bezug auf die Einhaltung der Standards in diesem Bereich keine Belege verfügbar sind.

4.3. Sanktionen, Schadensersatz und Rechtsfolgen

Alle Mitgliedstaaten der EU haben Kapitel III der Datenschutzrichtlinie über „Rechtsbehelfe, Haftung und Sanktionen" in ihren Rechtssystemen umgesetzt. Dieses Kapitel verpflichtet die nationalen Datenschutzbehörden zur Einführung angemessener und wirksamer Rechtsbehelfe, um die Achtung der durch die Rechtsvorschriften zum Schutz der personenbezogenen Daten garantierten Rechte sicherzustellen; außerdem ist dort die Einführung geeigneter und angemessener Sanktionen bei Verstößen gegen die Rechtsvorschriften zum Schutz der personenbezogenen Daten und die Einführung von Maßnahmen vorgesehen, die Entschädigungszahlungen an die von einer unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten betroffenen Personen sicherstellen sollen. Da jedoch die Bestimmungen der Datenschutzrichtlinie in Bezug auf Rechtsbehelfe, Sanktionen und Haftung nur das von den Mitgliedstaaten zu verfolgende Ziel festlegen, ohne jedoch detaillierte Anwendungskriterien vorzugeben, weisen die einzelstaatlichen Datenschutzgesetzen eine Reihe von Unterschieden auf. Diese betreffen sowohl die Möglichkeit, Rechtsansprüche durchzusetzen und Entschädigungen zu erwirken, als auch die Verurteilung und Bestrafung der Urheber von Verstößen gegen das Recht auf Schutz personenbezogener Daten.

4.3.1. Rechtsbehelfe

Durch Artikel 22 der Datenschutzrichtlinie wird die allgemeine Verpflichtung der Mitgliedstaaten kodifiziert, „unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens (…) [vorzusehen,] dass jede Person bei der Verletzung der Rechte, die ihr (…) garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann". In Tabelle 5 sind die verschiedenen Methoden ausgeführt, mit denen die Einhaltung der Bestimmungen des EU-Rechts in den einzelstaatlichen Rechtssystemen sichergestellt werden soll. Dies sind: a) administrative Rechtsbehelfe vor der Datenschutzbehörde; b) außergerichtliche Rechtsbehelfe vor der Kontrollstelle (als Alternative zu einem gerichtlichen Vorgehen; nach Anstrengung eines außergerichtlichen Verfahrens sind Klagen vor einer Justizbehörde ausgeschlossen); c) gerichtliche Rechtsbehelfe, die durch eine Klage vor ordentlichen Gerichten eingelegt werden.

70 Spezifische Bestimmungen betreffend die Benennung von Datenschutzbeauftragten finden sich nur im Gesetz über die elektrische Verarbeitung von Kundendaten im Sozial- und Gesundheitswesen sowie im Gesetz über elektronische ärztliche Verordnungen (*Laki sähköisestä lääkemääräyksestä, Lag om elektroniska recept*, Gesetz Nr. 61/2007). Diese Gesetze schreiben vor, dass Sozial- und Gesundheitsdienstleister, Apotheken, die Sozialversicherungseinrichtung Finnlands (KELA) und die Nationale Behörde für medizinrechtliche Angelegenheiten (TEO) Datenschutzbeauftragte zu benennen haben.

71 Die Datenschutzbestimmungen in Zypern enthalten eine Bestimmung, gemäß der die Mitarbeiter der nationalen Datenschutzbehörde in Zypern über die durch Rechtsverordnungen festzulegenden Qualifikationen verfügen müssen. Diese Rechtsverordnungen wurden allerdings noch nicht erlassen.

Tabelle 5: Rechtsbehelfe

Mitgliedstaat	Administrative Rechtsbehelfe vor der Datenschutzbehörde	Außergerichtliche Rechtsbehelfe vor der Datenschutzbehörde	Gerichtliche Rechtsbehelfe vor ordentlichen Gerichten
Belgien		●	●
Bulgarien	●		●
Dänemark	●		●
Deutschland	●		●
Estland	●		●
Finnland	●		●
Frankreich	●		●
Griechenland	●	●	●
Irland	●		●
Italien	●	●	●
Lettland	●		●
Litauen	●		●
Luxemburg	●		●
Malta	●		●
Niederlande	●		●
Österreich	●		●
Polen	●		●
Portugal	●		●
Rumänien	●		●
Schweden	●		●
Slowakei	●		●
Slowenien	●		●
Spanien	●		●
Tschechische Republik	●		●
Ungarn	●*		●
Vereinigtes Königreich	●		●
Zypern	●		●

*Anmerkung: *In Ungarn hat die Datenschutzbehörde begrenzte Befugnisse in Bezug auf die Bereitstellung administrativer Rechtsbehelfe, verfügt jedoch nicht über die Möglichkeit, diese durchzusetzen.*

Natürliche Personen in allen Mitgliedstaaten können eine Klage im Zusammenhang mit einem spezifischen Verstoß oder eine allgemeinere Beschwerde vor der einzelstaatlichen Datenschutzbehörde erheben, um auf einen Verstoß hinzuweisen. Ein wesentlicher Grundsatz der Rechtsstaatlichkeit ist das ebenfalls in allen Mitgliedstaaten anerkannte Recht, vor ordentlichen Gerichten ein Verfahren anzustrengen, um eine gerichtliche Entscheidung über den Rechtsstreit zu erlangen. Dies kann häufig im Wege vereinfachter Verfahren geschehen (z. B. in Belgien oder Italien). Faktisch besteht zwar in mehreren Ländern (z. B. in Estland, Finnland, Lettland und Österreich) theoretisch die Möglichkeit zur Nutzung von Rechtsbehelfen; diese Möglichkeiten werden in der Praxis von Klägern aber nicht genutzt. Nur in Belgien, Griechenland und Italien haben betroffene Personen die Option, Rechtsstreitigkeiten entweder vor Gericht vorzutragen oder entsprechende Beschwerden bei den Datenschutzbehörden einzureichen, die in einem quasigerichtlichen Verfahren möglicherweise einen rasch wirksamen und kostengünstigen Rechtsbehelf bieten können.

4.3.2. Sanktionen

Nach Artikel 24 der Datenschutzrichtlinie sind die Mitgliedstaaten verpflichtet, Sanktionen für Verstöße gegen die Datenschutzbestimmungen festzulegen. Die Umsetzung dieser allgemeinen Bestimmung auf einzelstaatlicher Ebene hat jedoch zu signifikanten Unterschieden zwischen den verschiedenen Rechtssystemen geführt. Der Einfluss der einzelstaatlichen Gesetzgebung und der Rechtspraxis auf dem Gebiet des Straf- und Verwaltungsrechts ist in diesem Bereich besonders relevant und hat sowohl das anfänglich von den Gesetzgebern der Mitgliedstaaten bei der Ausarbeitung der einschlägigen Rechtsvorschriften angewandte Konzept als auch das anschließend bei der Auslegung und Durchsetzung der maßgeblichen Rechtsvorschriften von den Verwaltungs- und Justizbehörden zugrunde gelegte Konzept geprägt. Da ein umfassender Vergleich der einzelstaatlichen verwaltungs- und strafrechtlichen Vorschriften im Zusammenhang mit Sanktionen (und Strafen) für Verletzungen des Rechts auf Datenschutz nicht praktikabel ist, konzentriert sich die Analyse hier auf die zur Anwendung von Sanktionen befugten Einrichtungen sowie auf die wichtigsten Sanktionen, die diese Einrichtungen anwenden können.

Die Datenschutzbehörden können verschiedene Sanktionen verhängen. Über die in Abschnitt 3.1.3.2 genannten Sanktionen (Verwarnung oder Verweis des Auftragsverarbeiters/für die Verarbeitung Verantwortlichen, Anordnung der Aussetzung der Verarbeitung personenbezogener Daten sowie Sperrung und Löschung spezifischer Daten) hinaus sind Kontrollstellen befugt, auch finanzielle Sanktionen zu verfügen. Gerichte können ebenfalls Geldstrafen sowie Freiheitsstrafen bzw. alternative Sanktionen wie Freiheitsstrafen auf Bewährung oder gemeinnützige Arbeit verhängen. Aus der nachstehenden Tabelle 6 geht hervor, welche Konsequenzen eine Nichteinhaltung der Datenschutzbestimmungen in den einzelnen Rechtssystemen haben kann: a) von den Datenschutzbehörden verhängte Geldbußen; b) von Gerichten verhängte Geldstrafen; c) von Gerichten verhängte Freiheitsstrafen und entsprechende Alternativen. Der Aspekt der Schadensersatzpflicht wird später in diesem Dokument erörtert.

Tabelle 6: Sanktionen

Mitgliedstaat	Von den Datenschutzbehörden verhängte Geldbußen	Von den Justizbehörden verhängte Geldstrafen	Von den Justizbehörden verhängte Freiheitsstrafen
Belgien		●	
Bulgarien	●		
Dänemark		●	●
Deutschland	●*	●	●
Estland	●	●	●
Finnland	●	●	●
Frankreich	●	●	●
Griechenland	●	●	●
Irland	●	●	
Italien	●	●	●
Lettland	●		
Litauen		●	
Luxemburg	●	●	
Malta	●	●	●
Niederlande	●	●	●
Österreich		●	●
Polen		●	●
Portugal	●		●
Rumänien	●	●	
Schweden		●	●
Slowakei	●	●	●
Slowenien	●	●	●
Spanien	●		
Tschechische Republik	●		
Ungarn		●	●
Vereinigtes Königreich		●	●
Zypern	●	●	

*Anmerkung: *Im Jahr 2008 wurden beispielsweise Bußgelder in Höhe von 1,4 Mio. EUR gegen das Handelsunternehmen LIDL verhängt und von diesem akzeptiert.*

Wie aus Tabelle 6 ersichtlich, sind Datenschutzbehörden nur in manchen Mitgliedstaaten befugt, finanzielle Sanktionen anzuwenden (wobei ihre Entscheidungen in jedem Fall vor Verwaltungsgerichten angefochten werden können). In anderen Mitgliedstaaten (z. B. in Belgien und im Vereinigten Königreich) können sie nur gütliche Lösungen mit den Parteien aushandeln, die die betreffenden Verstöße begehen. Die Wirksamkeit der von den Kontrollstellen angewandten Verwaltungssanktionen hat jedoch in mehreren Mitgliedstaaten zu Bedenken geführt, da die Höhe der Geldbußen als zu gering und ihre Verhängung als zu selten angesehen wird, um eine abschreckende Wirkung zu erzielen. In anderen Mitgliedstaaten (z. B. Dänemark, Frankreich, Österreich und Vereinigtes Königreich) dagegen hat sich die Rechtspraxis der Justizbehörden als zu wenig abschreckend erwiesen. Dementsprechend wurden in manchen der Mitgliedstaaten (z. B. in Estland) von den Justizbehörden bislang keinerlei strafrechtliche Sanktionen verhängt.

4.3.3. Schadensersatz

Nach Artikel 23 Absatz 1 der Datenschutzrichtlinie haben die Mitgliedstaaten vorzusehen, dass „jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadensersatz zu verlangen". Die einzelstaatlichen Rechtsvorschriften zur zivilrechtlichen Haftung unterscheiden sich jedoch abhängig davon, ob sich die Mitgliedstaaten für eine spezifische Regelung der Schadensersatzpflicht in Datenschutzsachen entschieden haben oder einfach den üblichen Rahmen für die zivilrechtliche Haftung auf den Bereich des Schutzes personenbezogener Daten ausgedehnt haben. In der nachstehenden Tabelle 7 sind die wichtigsten Lösungen dargestellt, für die sich die Mitgliedstaaten zur Umsetzung dieser Bestimmung der Datenschutzrichtlinie entschieden haben: a) Erweiterung des üblichen Rahmens der zivilrechtlichen Haftung (wobei der Kläger sowohl die Beweislast für den erlittenen Schaden als auch das Prozesskostenrisiko trägt); b) Erweiterung des bestehenden Rahmens der zivilrechtlichen Haftung, jedoch mit Beweislastumkehr (wobei der für die Verarbeitung Verantwortliche von der Haftung ganz oder teilweise freigestellt werden kann, wenn er nachweist, dass er nicht für das Ereignis verantwortlich ist, das zu dem Schaden geführt hat); c) Einführung eines speziellen Rahmens für die zivilrechtliche Haftung.

Tabelle 7: Schadensersatz

Mitgliedstaat	Erweiterung des bestehenden Rahmens der zivilrechtlichen Haftung	Bestehender Rahmen der zivilrechtlichen Haftung mit Beweislastumkehr	Spezieller Rahmen der zivilrechtlichen Haftung
Belgien	●		
Bulgarien	●		
Dänemark		●	
Deutschland		●	●
Estland	●		
Finnland	●		
Frankreich	●		
Griechenland			●
Irland	●		
Italien		●	
Lettland	●		
Litauen	●		
Luxemburg	●		
Malta	●		
Niederlande	●		
Österreich	●		
Polen	●		
Portugal	●		
Rumänien	●		
Schweden		●*	●
Slowakei	●		
Slowenien	●		
Spanien	●		
Tschechische Republik	●		
Ungarn			●
Vereinigtes Königreich	●		
Zypern	●		

*Anmerkung: *Im schwedischen Datenschutzgesetz gibt es besondere Vorschriften für Schadensersatz; das Verfahren fällt jedoch unter den bestehenden Rahmen für Zivilsachen.*

Wie aus Tabelle 7 hervorgeht, ist in allen Fällen Schadensersatz zu zahlen, in denen ein Schaden dadurch entsteht, dass personenbezogene Daten nicht gemäß den Datenschutzvorschriften verarbeitet werden. In den meisten Mitgliedstaaten kann Schadensersatz theoretisch im Wege von Standard-Gerichtsverfahren erlangt werden, die durch allgemeine Vorschriften zur zivilrechtlichen Haftung geregelt werden; allerdings war in einer Reihe von Staaten nicht festzustellen, dass in Datenschutzsachen Schadensersatz zugesprochen wurde (z. B. in Lettland, Malta, Portugal und Zypern), oder die Justizbehörden wurden nur mit einer sehr geringen Zahl von Schadensersatzverfahren befasst (z. B. in Estland und in Finnland). In mehreren Mitgliedstaaten gelten die allgemeinen Bestimmungen für die Haftung auch für Datenschutzsachen, abgesehen von der Umkehrung der Beweislast, die vom Kläger auf den Beklagten (den Auftragsverarbeiter/für die Verarbeitung Verantwortlichen) übergeht. Schließlich wurde in einigen Ländern ein besonderer Rahmen für die Erlangung von Schadensersatz geschaffen. Insbesondere gilt in Deutschland und Griechenland für Auftragsverarbeiter/für die Verarbeitung Verantwortliche eine verschuldensunabhängige Haftung (allerdings nur für öffentliche Auftragsverarbeiter/für die Verarbeitung Verantwortliche). Somit unterliegt die Haftpflicht nicht der Voraussetzung der Absicht oder Fahrlässigkeit, sondern folgt einfach aus dem Vorliegen eines durch einen Verstoß gegen die Rechtsvorschriften entstandenen Schadens. Berichten zufolge können in Belgien manche Gerichte Schadensersatz nach einem beschleunigten Verfahren vor dem Vorsitzenden des Gerichts erster Instanz zusprechen. In Schweden kann das Justizministerium Schadensersatz für durch Regierungs- oder Verwaltungsstellen begangene Verstöße ohne Gerichtsverfahren zusprechen. In Ungarn fallen für Gerichtsverfahren in Datenschutzsachen keine Gerichtskosten und -gebühren an, und für die Beurteilung der Verantwortung bzw. Haftpflicht des Auftragsverarbeiters/für die Verarbeitung Verantwortlichen gilt eine der verschuldensunabhängigen Haftung ähnliche Bestimmung.

Je nach Gesetzgebung und Gerichtspraxis im Bereich der zivilrechtlichen Haftung werden die Schadensersatzpflichten von Auftragsverarbeitern/für die Verarbeitung Verantwortlichen, die gegen das Recht auf Schutz der personenbezogenen Daten verstoßen haben, in den einzelnen Mitgliedstaaten verfahrens- und materiellrechtlich unterschiedlich quantifiziert; entsprechend ist eine Analyse im Rahmen dieses vergleichenden Berichts nicht möglich. Zudem ist die Spanne der in Datenschutzsachen zugesprochenen Schadensersatzzahlungen für die meisten Mitgliedstaaten (Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowenien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern) nicht bekannt. Es ist jedoch zu unterstreichen, dass in der Gesetzgebung oder in der Gerichtspraxis einer Reihe von Mitgliedstaaten (Deutschland, Griechenland, Italien, Litauen, Schweden, Slowenien, Ungarn und Vereinigtes Königreich) auch Schadensersatzleistungen für immaterielle Schäden (z. B. zugefügtes Leid) zugesprochen werden können, entweder allein oder zusammen mit Schadensersatzleistungen für materielle Schäden.

4.3.4. Besondere Datenschutzvorschriften bei Arbeitsverhältnissen

Besonders dringend ist die Notwendigkeit der Achtung der Grundrechte und der Würde der betroffenen Person bei Beschäftigungsverhältnissen. Einerseits ist der Schutz der Privatsphäre und der personenbezogenen Daten der Arbeitnehmer von grundlegender Bedeutung und Voraussetzung für die Gewährleistung des Grundrechts auf gewerkschaftliche Organisation und auf Teilnahme an Kollektivmaßnahmen. Andererseits kommen einige der fortschrittlichsten Technologien für die Überwachung und Kontrolle des Verhaltens von Personen (beispielsweise die Überwachung mit Kameras und die Fernüberwachung des E-Mail-Verkehrs) überwiegend im Berufsleben zum Einsatz. Daher sollten die Mitgliedstaaten weitere Rechtsvorschriften über den Datenschutz bei Beschäftigungsverhältnissen erlassen, um die inhärente Ungleichheit der Parteien des Arbeitsvertrags auszugleichen, indem für den Arbeitgeber strengere Verpflichtungen in Bezug auf die Einhaltung der datenschutzrechtlichen Bestimmungen vorgeschrieben werden.

Während die Datenschutzrichtlinie in Artikel 8 Absatz 1 die Verarbeitung personenbezogener Daten untersagt, aus denen die Gewerkschaftszugehörigkeit hervorgeht, hat eine Reihe von Mitgliedstaaten (Belgien, Finnland, Griechenland, Irland, Italien, Lettland, Luxemburg, Polen, Portugal, Niederlande, Slowakei, Slowenien, Spanien, Tschechische Republik und Ungarn) zudem besondere Bestimmungen erlassen (entweder im Arbeitsrecht oder im allgemeinen Datenschutzrecht), um bei Beschäftigungsverhältnissen einen höheren Standard für die Achtung des Rechts auf Schutz der Privatsphäre und der personenbezogenen Daten zu gewährleisten. Diese Bestimmungen legen eine Rolle für die Datenschutzbehörden fest, die die Befugnis zur Ausarbeitung allgemeiner Rechtsverordnungen und Leitlinien, insbesondere für Privatunternehmen, erhalten. Neben der Beratung der Arbeitnehmer in Datenschutzfragen sind Gewerkschaften sowohl im Vorfeld bei der Aushandlung von Vereinbarungen mit den Arbeitgebern über die Einführung von Systemen zur Erfassung von Belegschaftsdaten als auch rückwirkend bei der Überwachung der Einhaltung der diesbezüglich relevanten Bestimmungen häufig direkt beteiligt.

Nichtsdestoweniger sind verschiedene Unzulänglichkeiten in Bezug auf den Datenschutz im Beschäftigungsbereich offenkundig. Zunächst fehlen in mehreren Mitgliedstaaten (Bulgarien, Dänemark, Deutschland, Estland, Frankreich, Litauen, Malta, Österreich, Rumänien, Schweden, Vereinigtes Königreich und Zypern) im Bereich der privatwirtschaftlichen Beschäftigung noch immer besondere Rechtsvorschriften zur Verbesserung des Schutzes von Arbeitnehmern. Darüber hinaus sind das Fehlen einer Überwachungsfunktion für Gewerkschaften (z. B. Irland, Lettland und Tschechische Republik), die Ermessensbefugnis des Arbeitgebers hinsichtlich der Entscheidung über das Ziel der Verarbeitung personenbezogener Daten (z. B. Polen) und die Freistellung von Kleinunternehmen von der Einhaltung der strengen Standards für die Datenverarbeitung im Beschäftigungsbereich (z. B. Niederlande) als problematisch zu bewerten, selbst wenn entsprechende Rechtsvorschriften bestehen. Schließlich war in anderen Ländern (z. B. Finnland) der Schutz personenbezogener Daten im Kontext des Arbeitsverhältnisses bisher zwar zufriedenstellend, durch kürzlich erfolgte, aber noch nicht umgesetzte Gesetzesreformen würden die bestehenden Standards jedoch erheblich gesenkt, indem Arbeitgebern gestattet würde, unter bestimmten Bedingungen die Adressen der von Arbeitnehmern gesendeten und empfangenen E-Mails sowie die Art von Dateianhängen der E-Mails (nicht jedoch den Inhalt der E-Mails selbst) zu überwachen.[72] Gemäß der finnischen Gesetzesvorlage erhalten Unternehmen das Recht, Identifikationsdaten in ihren Kommunikationsnetzwerken zu verarbeiten, um den Verrat von Geschäftsgeheimnissen, die unerlaubte Verwendung, Industriespionage und bestimmte andere Straftaten zu ermitteln, zu verhindern und zu untersuchen.

72 Siehe Gesetzesvorlage HE 48/2008 vp der finnischen Regierung.

4.4. Rechtsbewusstsein

In diesem Abschnitt werden die Ergebnisse von Eurobarometer-Umfragen und anderen in den Mitgliedstaaten durchgeführten Studien/Umfragen dargestellt, um einen Überblick über das Rechtsbewusstsein der Öffentlichkeit in Bezug auf den Datenschutz zu vermitteln. Ferner werden Verbindungen zwischen dem Rechtsbewusstsein und den folgenden Aspekten untersucht:

- Datenschutzbehörden sowie den Befugnissen, des Aufgabenbereichs, der Ressourcen und der Tätigkeiten von Datenschutzbehörden,
- Verfahren, die auf eine Befolgung der datenschutzrechtlichen Bestimmungen schließen lassen,
- Verfahren in Bezug auf Sanktionen, Schadensersatz und Rechtsfolgen in Datenschutzsachen.

In Abschnitt 5.1.4 werden Defizite in Bezug auf das Rechtsbewusstsein erörtert, und in Abschnitt 6.3 werden vielversprechende Praktiken im Zusammenhang mit dem Rechtsbewusstsein beschrieben.

Im Februar 2008 wurden zwei Flash-Eurobarometer-Umfragen veröffentlicht: Nr. 225 *„Data Protection in the European Union: Citizens' perceptions"* (Datenschutz in der Europäischen Union: Die Wahrnehmungen der Bürger)[73] und Nr. 226 *„Data Protection in the European Union: Data controllers' perceptions"* (Datenschutz in der Europäischen Union: Die Wahrnehmungen der für die Verarbeitung Verantwortlichen).[74]

Die Themen der ersten Umfrage umfassten die allgemeinen Einschätzungen und Vorbehalte der Bürger in Bezug auf den Datenschutz; das Vertrauen, das sie in verschiedene Arten von Organisationen setzten, die sich im Besitz ihrer personenbezogenen Daten befanden; den Grad der Aufklärung über die Datenschutzrechte der Bürger und ihre Kenntnis der nationalen Datenschutzbehörden; die empfundene Sicherheit der Datenübermittlung über das Internet und die Nutzung von Werkzeugen zur Verbesserung der Datensicherheit; und die Einstellung der Bürger zur Beschränkung ihrer Datenschutzrechte angesichts des internationalen Terrorismus. Bei der Umfrage wurden 27 000 Personen in den 27 EU-Mitgliedstaaten befragt (1 000 Befragungen je Land), hauptsächlich in Form von Telefonbefragungen über Festnetzanschlüsse. (In neun Mitgliedstaaten wurde eine reine Festnetz-Telefonbefragung für unzureichend gehalten; daher umfasste die Stichprobe eine Mischung aus Telefonbefragungen und persönlichen Befragungen.)

Die Umfrage gelangte zu folgenden Ergebnissen:

- Die meisten Befragten in der gesamten EU zeigten sich sehr oder ziemlich besorgt darüber, wie ihre personenbezogenen Daten verwaltet werden. Der Grad der Besorgnis war jedoch der gleiche wie bei einer früheren Eurobarometer-Umfrage aus dem Jahr 1991.
- Das Vertrauen der Befragten in Bezug auf den Schutz personenbezogener Daten war gegenüber medizinischen Diensten, Ärzten und öffentlichen Einrichtungen am größten.
- Die meisten Befragten stellten in Frage, ob die einzelstaatlichen Rechtsvorschriften in ihrem Land die Nutzung personenbezogener Daten im Internet bewältigen können.
- Während die meisten Befragten anscheinend ihre Rechte in Bezug auf die Nutzung personenbezogener Daten kannten und wussten, dass einschlägige Rechtsvorschriften bestehen, war durchschnittlich nur 28 % der Befragten in den 27 EU-Mitgliedstaaten die Existenz der jeweiligen einzelstaatlichen Datenschutzbehörde bekannt.

Die Aufgabe der zweiten Umfrage war die Ermittlung der Wahrnehmungen von für die Verarbeitung Verantwortlichen in Bezug auf den Datenschutz in den 27 Mitgliedstaaten der EU. Die Themen dieser Umfrage umfassten die Wahrnehmungen in Bezug auf die einzelstaatlichen Datenschutzbestimmungen; innerbetriebliche Verfahren im Zusammenhang mit Datenschutz und Übermittlung personenbezogener Daten; jüngste Erfahrungen in Bezug auf Privatsphäre und Datenschutz; die Zukunft des Rechtsrahmens für den Datenschutz; und den Datenschutz angesichts des internationalen Terrorismus.

Diese Umfrage gelangte zu folgenden Ergebnissen:

- Eine Mehrheit (56 %) der innerhalb ihres Unternehmens für Datenschutzfragen verantwortlichen Personen gab an, mit den Bestimmungen des einzelstaatlichen Datenschutzrechts gut oder einigermaßen vertraut zu sein.
- Der gleiche Anteil (56 %) der Befragten betrachtete das Schutzniveau, das ihr jeweiliges einzelstaatliches Datenschutzrecht den Bürgern bietet, als „mittel", 28 % als „hoch" und 11 % als „gering".
- 50 % der Befragten bewerteten die bestehenden Rechtsvorschriften als ziemlich oder völlig ungeeignet für die Bewältigung der zunehmenden Menge an ausgetauschten personenbezogenen Daten.
- Die überwiegende Mehrheit (91 %) der Befragten betrachtete die Anforderungen des Datenschutzrechts als notwendig. Ein Drittel der Befragten (35 %) sagte, dass die Anforderungen in gewisser Hinsicht zu streng seien.
- In Bezug auf die Angemessenheit der Harmonisierung einzelstaatlicher Gesetze zur Berücksichtigung des freien Verkehrs personenbezogener Daten und in Bezug auf die bestehenden Unterschiede bei der Auslegung des Datenschutzrechts in den verschiedenen EU-Mitgliedstaaten waren die Meinungen geteilt: Zu beiden Fragen hatte ein großer Teil der Befragten keine klare Meinung.
- 13 % der Befragten in den 27 EU-Mitgliedstaaten gaben an, dass sie in regelmäßigem Kontakt mit der einzelstaatlichen Datenschutzbehörde stehen – die Ergebnisse reichten allerdings von 41 % der Befragten in Italien bis zu 1 % in Österreich.
- Die am häufigsten genannten Gründe für die Kontaktaufnahme mit der einzelstaatlichen Datenschutzbehörde waren ein entsprechender Beratungsbedarf (bei 60 % der in regelmäßigem Kontakt mit der Datenschutzbehörde stehenden Befragten) und die Übermittlung von Mitteilungen (56 %).
- Zu den verfügbaren statistischen Daten der Mitgliedstaaten ist zunächst einmal festzustellen, dass einzelstaatliche Umfragen nur für 12 der 27 Mitgliedstaaten der EU verfügbar sind. Diese Umfragen wurden in manchen Fällen von den nationalen Datenschutzbehörden in Auftrag gegeben. Die gestellten Fragen, die Anzahl der Befragten, die Methodik, die Stichprobenauswahl und die Endergebnisse sind äußerst unterschiedlich und ermöglichen nicht immer eine Zuordnung der Ergebnisse zu den Themen dieser vergleichenden Studie.

Einzelstaatliche Umfragen zum Rechtsbewusstsein sind zwar für einige Länder (Dänemark, Finnland, Frankreich, Irland, Lettland, die Niederlande, Österreich,

73 *Data Protection in the European Union: Citizens' perceptions*, Flash Eurobarometer Nr. 225 (http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf).

74 *Data Protection in the European Union: Data controllers' perceptions*, Flash Eurobarometer Nr. 226 (http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf).

Schweden, die Slowakei, Slowenien, Spanien, Ungarn, und Vereinigtes Königreich) verfügbar, für die verbleibenden Länder (Belgien, Bulgarien, Deutschland, Estland, Griechenland, Italien, Litauen, Luxemburg, Malta, Polen, Portugal, Rumänien, Tschechische Republik und Zypern) jedoch nicht.

In der Slowakei werden regelmäßig öffentliche Umfragen zum Schutz personenbezogener Daten durchgeführt. Die Ergebnisse dieser Umfragen kommen in den von der einzelstaatlichen Datenschutzbehörde veröffentlichten Berichten zum Ausdruck. Zwei der Umfragen (durchgeführt in den Jahren 2005[75] und 2007[76]) wurden auf der Website der Datenschutzbehörde veröffentlicht.[77] Beide Umfragen umfassen eine national repräsentative Zufallsstichprobe von Befragten ab einem Alter von 18 Jahren. (In der Umfrage aus dem Jahr 2005 betrug die Netto-Stichprobengröße 1 283 Befragte, und bei der Umfrage aus dem Jahr 2007 lag diese bei 1 131 Befragten). In der Umfrage aus dem Jahr 2007 erklärten 51 % der Befragten, dass sie sich ihres Rechts auf Datenschutz bewusst seien, und 50 % der Befragten erkannten das Amt für den Schutz personenbezogener Daten als zuständige einzelstaatliche Datenschutzbehörde an (das sind 5 % mehr als in der vorigen Befragung im Jahr 2005). Basierend auf den Ergebnissen der Umfragen ist festzustellen, dass die Öffentlichkeit nach wie vor nicht vollständig über die Themen im Zusammenhang mit dem Schutz personenbezogener Daten informiert ist und dass diese nicht umfassend debattiert werden.

In Lettland wurden in den Jahren 2003 und 2005 zwei Umfragen durchgeführt (beide basierten auf einer geschichteten Zufallsstichprobe von etwa 1 000 dauerhaft in Lettland ansässigen Befragten). Die für die vorliegende vergleichende Untersuchung relevanten Ergebnisse lauten: 29,5 % der Befragten (23,3 % im Jahr 2003) wussten von der Existenz der einzelstaatlichen Datenschutzbehörde; 19,5 % der Befragten (14,5 % im Jahr 2003) erklärten, bereits in einer Situation gewesen zu sein, in der ihre Daten unvorschriftsmäßig verarbeitet wurden, wodurch ihnen ein vermeintlicher finanzieller oder moralischer Schaden entstanden sei; 13,5 % der Befragten (6,4 % im Jahr 2003) erklärten, mit einer Situation konfrontiert gewesen zu sein, in der mehr personenbezogene Angaben von ihnen verlangt worden seien als erforderlich; 22,9 % der Befragten haben versucht, Informationen über sich selbst von Einrichtungen oder Unternehmen zu erhalten. Die betreffenden Befragten waren dabei meist (66,2 %) erfolgreich, während 32,5 % der Befragten dieser Gruppe die gewünschten Informationen verweigert wurden. Die Ergebnisse der Umfrage zeigen, dass die Sensibilisierung für den Datenschutz sowohl in staatlichen Einrichtungen als auch in der allgemeinen Öffentlichkeit verbessert werden sollte.

In Schweden führt die einzelstaatliche Datenschutzbehörde regelmäßig Forschungsarbeiten im Bereich des öffentlichen und privaten Sektors sowie verschiedener gesellschaftlicher Gruppen durch. Es sind drei Studien neueren Datums verfügbar. Die erste bezieht sich auf die Sensibilisierung der Gesundheitsbehörden auf Provinzebene für Datenschutzbestimmungen betreffend die Zugänglichkeit von Patientendaten.[78] Bei der zweiten handelt es sich um die Auswertung eines Fragebogens zur Haltung von Arbeitgebern hinsichtlich der Nutzung von Internet und E-Mail durch ihre Arbeitnehmer sowie zur Überwachung durch Verarbeitung biometrischer Daten und durch Kameras; dieser Fragebogen wurde an 103 nach dem Zufallsprinzip ausgewählte Unternehmen und Behörden gesandt.[79] Die dritte Studie über die Sensibilisierung für das Datenschutzgesetz und die Datenschutzrechte sowie die diesbezüglichen Einstellungen konzentrierte sich auf junge Menschen zwischen 14 und 18 Jahren (533 Befragte, wobei in der Stichprobenauswahl Quoten für bestimmte Personengruppen berücksichtigt wurden), die einen Online-Fragebogen ausfüllten.[80] Die Ergebnisse dieser Umfragen wurden durch die einzelstaatlichen Studien weder vorgestellt noch analysiert; insoweit sind entsprechende Anmerkungen nicht möglich.

In Dänemark sind zwei Studien verfügbar. In einer kürzlich von Privacy and Security Technology (PRISE) durchgeführten Studie mit dem Titel *Privacy enhancing shaping of security research and technology* (Gestaltung von Sicherheitsforschung und -technologie für eine verbesserte Privatsphäre) wurde die Notwendigkeit einer öffentlichen Debatte über Fragen der Einführung neuer Sicherheitstechnologien festgestellt. Eine zweite, bei der es sich um eine Umfrage von *Det Kriminalpræventive Råd* (Rat für Verbrechensverhütung) aus dem Jahr 2005 zur CCTV-Überwachung handelt (mit 994 befragten Personen), kommt zu dem Ergebnis, dass die Dänen der CCTV-Überwachung generell positiv gegenüberstehen. Frauen scheinen sich dieser Umfrage zufolge mehr Sorgen um Kriminalität zu machen als Männer. Bürger mit einem höheren Bildungsstand scheinen in Bezug auf Eingriffe in die Privatsphäre stärker besorgt zu sein als andere.[81] Generell lässt die Umfrage darauf schließen, dass sich die dänische Bevölkerung hinsichtlich der Frage der Privatsphäre keine besonderen Gedanken zu machen scheint. Die dänische Bevölkerung hat generell ein grundlegendes Vertrauen in den Umgang der Regierung und der Behörden mit dem Datenschutz und ist der Auffassung, dass Fragen der Verbrechensverhütung und der Sicherheit wichtiger sind als der immaterielle und abstrakte Begriff der Privatsphäre.

Die nationale Datenschutzbehörde Irlands führte im Jahr 2008 eine Umfrage durch (eine Folgemaßnahme zu ähnlichen Forschungsarbeiten in den Jahren 1997, 2002 und 2005); Grundlage war eine Stichprobe von 1 000 Befragten, die in persönlichen Gesprächen im Rahmen einer übergreifenden Studie Auskünfte erteilten.[82] Eines der wichtigsten Ergebnisse der Umfrage war, dass fast zwei Drittel der Bevölkerung (65 %) angaben, ihre Privatsphäre sei in der einen oder anderen Form verletzt worden; am häufigsten wurde die Übermittlung bzw. Zustellung unerbetener Werbenachrichten genannt.[83] Aus verschiedenen zur Wahl stehenden Themen wurden ein gutes Gesundheitswesen (89 % der Befragten) und die Verbrechensverhütung (87 %) als die wichtigsten Themen für die Befragten bezeichnet; danach erst wurde der Schutz personenbezogener Informationen genannt (84 %). Während die Hälfte der Befragten der Ansicht ist, dass sowohl im öffentlichen als auch im privaten Sektor angemessene Kontrollen bestehen, um die Arbeitgeber am Zugriff auf personenbezogene Informationen zu unangemessenen Zwecken zu hindern, hatte einer von fünf Befragten Zweifel an der Wirksamkeit dieser Kontrollen. Die Befragten messen der Kranken- und Finanzgeschichte sowie den Kreditkartendetails die höchste Bedeutung hinsichtlich der Vertraulichkeit bei. 58 % der Befragten war die einzelstaatliche Datenschutzbehörde bekannt. Die einzelstaatliche

75 www.dataprotection.gov.sk/buxus/docs/sprava_5_2005_prieskum_vm1.pdf.
76 www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf.
77 www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421.
78 Zusammenfassung auf Englisch abrufbar unter: Report 2005:1 www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf.
79 Monitoring in Working Life, Report 2005: 3, englische Zusammenfassung abrufbar unter: www.datainspektionen.se/-Documents/rapport-monworklife-summary.pdf.
80 www.datainspektionen.se/Documents/rapport-ungdom-2009.pdf.
81 TV-overvågning – Fakta om TV-overvågning i Danmark. Det Kriminalpræventive Råd, Februar 2005. In dänischer Sprache abrufbar unter: www.dkr.dk/ftp_files/WEBDOX/PDF/dkr_mat_083.pdf.
82 Die vollständige Umfrage ist abrufbar unter: www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm.
83 Bericht mit den Ergebnissen der Umfrage abrufbar unter: www.dataprotection.ie/docs/Public_Awareness_Survey_2008_Report/821.htm.

Datenschutzbehörde erklärte, dass die Ergebnisse der Befragung genutzt würden, um die künftige Arbeit des Amtes zu gestalten.[84]

In Frankreich gibt die *Commission Nationale de l'Informatique et des Libertés* (CNIL) jährlich Umfragen in Auftrag, um die Sensibilisierung der Bürger für die Organisation und für ihre Rechte zu beobachten. Diese Umfragen nutzen eine repräsentative Stichprobe von 1 000 Befragten im Alter ab 18 Jahren. Gemäß dieser Umfrage aus dem Jahr 2007 sehen 61 % der Franzosen in der Erfassung von Daten einen Verstoß gegen ihr Recht auf Schutz der Privatsphäre und wünschen demzufolge einen verstärkten Schutz.[85] Überdies gaben 32 % der Befragten in einer ähnlichen Umfrage im Juni 2004 an, die einzelstaatliche Datenschutzbehörde zu kennen; dieser Anteil erhöhte sich auf 37 % im Dezember 2005, 39 % im Dezember 2006 und 50 % im November 2007.[86] Einer von zwei Befragten ist über die Aufgaben der Datenschutzbehörde informiert. Allerdings erklärten nur 26 %, dass sie das Gefühl hatten, über ihre Rechte im Hinblick auf den Schutz personenbezogener Daten ausreichend informiert worden zu sein, während 72 % der Befragten meinten, dass sie nicht ausreichend informiert seien.[87]

Im Juli 2008 wurde in Österreich eine Erhebung auf Grundlage einer Straßenumfrage mit persönlichen Befragungen von 1 213 Personen (unter Verwendung von Quoten für die Befragten) zum Thema Vertrauen der österreichischen Bevölkerung in den Datenschutz veröffentlicht.[88] Dieser Umfrage zufolge sind Themen wie Datenschutz oder Überwachung in der österreichischen Bevölkerung weitgehend unbekannt: 77 % der Befragten räumten ein, in Bezug auf derartige Themen mehr oder weniger nachlässig zu sein; 92 % erklärten, nicht zu wissen, ob über sie (personenbezogene) Daten erhoben werden, und wenn ja, von wem; 76 % der Befragten waren der Meinung, dass die österreichische Bevölkerung nicht hinreichend über den Datenschutz, die Risiken des Datenmissbrauchs oder die fraglichen rechtlichen Voraussetzungen informiert sei. In Bezug auf die Videoüberwachung erklärten 55 % der Befragten, dass sie gewöhnt seien, dass Videokameras Veranstaltungen und das Verhalten praktisch aller Personen überwachen und aufzeichnen; sie betrachteten dies eher als einen Aspekt des modernen Lebens denn als eine Bedrohung für die Grundrechte. In einer weiteren Studie zur Videoüberwachung des öffentlichen Raumes (mit 1 237 Befragten, unter Verwendung derselben Methodik wie in der oben genannten Studie) erklärten bis zu 81 % der Befragten, dass sie auf Passanten gerichtete Videokameras akzeptieren, und 90 % räumten ein, dass sie sich an die allgegenwärtigen Überwachungskameras gewöhnt haben.[89]

Für Spanien sind zwei Studien verfügbar. Die erste trägt den Titel „Studie zum Grad der Anpassung kleiner und mittlerer spanischer Unternehmen an das Ausführungsgesetz zum Schutz personenbezogener Daten und die neue gesetzliche Regelung".[90] Sie bestätigt, dass 96 % der kleinen und mittleren spanischen Unternehmen Dateien mit personenbezogenen Daten haben und dass 78 % davon in Form von elektronischen Dateien vorliegen, so dass sie alle in den Anwendungsbereich der Datenschutzbestimmungen fallen (die Ergebnisse basieren auf Telefonbefragungen einer geschichteten Stichprobe von 250 kleinen und mittleren Unternehmen (Unternehmen mit weniger als 50 Mitarbeitern)). Kleine und mittlere spanische Unternehmen zeigen eine positive Einstellung gegenüber dem Datenschutz: 82 % der befragten Unternehmen bestätigten, dass ihnen die Notwendigkeit der Einhaltung der relevanten Bestimmungen bewusst sei, während 79 % ihre Absicht bekräftigten, wirtschaftliche Mittel und/oder Humanressourcen für die Einhaltung der Datenschutzbestimmungen vorzusehen. Außerdem existiert eine wichtige Studie der lokalen baskischen Stelle für den Schutz personenbezogener Daten, die im Juni 2008 durchgeführt wurde und sich mit der sozialen Wahrnehmung des Datenschutzes im Baskenland befasst (auf der Grundlage einer geschichteten Zufallsstichprobe von 600 telefonisch befragten Personen).[91] Diese Studie besagt, dass 37 % der Bevölkerung dieser autonomen Gemeinschaft sehr oder relativ besorgt darüber sind, wie die Behörden und die privaten Unternehmen die personenbezogenen Daten der Bürger verwenden.

In den Niederlanden wurden die Wahrnehmungen und das Bewusstsein der Bürger hinsichtlich der Privatsphäre und des Datenschutzes in verschiedenen Umfragen untersucht.[92] In einer Umfrage aus dem Jahr 1989 schienen die Bürger der Meinung zu sein, dass die Privatsphäre ebenso wichtig sei wie eine gute Gesundheitsversorgung, eine saubere Umwelt oder die Bekämpfung von Arbeitslosigkeit und Kriminalität.[93] In einer Umfrage aus dem Jahr 1999 wurden drei Gruppen von Bürgern unterschieden: 1) Bürger, die die Informationstechnologie für notwendig halten und keine Probleme in Bezug auf Privatsphäre und Datenschutz sehen (19 %); 2) Bürger, die der Ansicht sind, dass die zunehmende Nutzung der Informationstechnologien zunehmend Probleme in den Bereichen Privatsphäre und Datenschutz nach sich zieht (35 %); und 3) Bürger, die die Informationstechnologien als Gefährdung für Privatsphäre und Datenschutz betrachten (47 %).[94] Einer Umfrage aus dem Jahr 2007 mit dem Schwerpunkt Freiheit und Solidarität zufolge waren 51 % der Befragten der Ansicht, dass die niederländische Regierung das Grundrecht auf Privatsphäre ausreichend schützte, während 43 % meinten, dass die Regierung ihre Privatsphäre besser schützen sollte. (Die Ergebnisse der Umfrage von 2007 basieren auf einer Zufallsstichprobe von Haushalten aus einem Internet-Haushaltsgremium, und die Umfrage erfolgte auf dem Wege der computergestützten Selbstbefragung (*computer-assisted self-interviewing*, CASI); die Befragten waren in der Altersgruppe ab 13 Jahre, und die Netto-Stichprobengröße lag bei 967 Befragten.)[95] Im Januar 2009 wurden die Ergebnisse einer von der einzelstaatlichen Datenschutzbehörde in Auftrag gegebenen Umfrage veröffentlicht (diese basierte auf einer Online-Umfrage mit 2 016 Befragten). In dem Bericht „Nichts zu verbergen und dennoch bange" wird die Einstellung der niederländischen Bürger im Hinblick auf die Erfassung und Verarbeitung

84 Pressemitteilung vom 12.8.2008, abrufbar unter: www.dataprotection.ie/viewdoc.asp?DocID=815.

85 CNIL, 25.1.2008, „61 % der Franzosen glauben, dass die Erstellung von Computerdateien einen Verstoß gegen ihr Recht auf Privatsphäre darstellt", siehe: www.cnil.fr.

86 CNIL, Jahresbericht 2007, S. 39.

87 CNIL, Jahresbericht 2007, S. 39.

88 Vertrauen der ÖsterreicherInnen in den Datenschutz, abrufbar unter: www.oekonsult.eu/datensicherheit2008.pdf.

89 Big Brother. Gefahr oder Normalität, abrufbar unter: www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf.

90 *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos y el nuevo Reglamento de Desarrollo,* Instituto Nacional de Tecnologías de la Comunicación (Nationales Institut für Kommunikationstechnologien), Juli 2008, abrufbar unter: www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_pymes..

91 *La protección de datos personales;* diese Studie ist abrufbar unter: www.avpd.euskadi.net/s04- 5249/es/contenidos/informacion/estudio/es_cuali/adjuntos/informe.pdf.

92 Siehe auch Sjaak Nouwt (2005), *Privacy voor doe-het-zelvers*, Den Haag: Sdu, ITeR Series Vol. 73. http://arno.uvt.nl/show.cgi?fid=41691.

93 Holvast, Jan, Henny van Dijk und Gerrit Jan Schep (1989), *Privacy Doorgelicht*, Den Haag: SWOKA.

94 Smink, G. C. J., A. M. Hamstra und H. M. L. van Dijk (1999), *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut, Werkdocument 68.

95 Dieter Verhue, Harmen Binnema & Rogier van Kalmthout (2008), *Nationaal Vrijheidsonderzoek. Meting 2008.* Opiniedeel, April 2008, S. 36; siehe: www.4en5mei.nl/mmbase/attachments/158819/p4751_vrijheidsonderzoek_opiniedeel_v4_read_only.doc.

ihrer personenbezogenen Daten bewertet.[96] Die meisten Bürger geben ihre personenbezogenen Daten generell relativ bereitwillig preis; dies bedeutet jedoch nicht, dass sich die Bürger ihrer Privatsphäre nicht bewusst wären. Die meisten Bürger sind sich ihrer Privatsphäre durchaus bewusst, und die Bereitwilligkeit zur Preisgabe personenbezogener Daten kann eher als Anerkenntnis des Unvermeidlichen bzw. gewissermaßen als Resignation denn als Ausdruck des Vertrauens in die ordnungsgemäße Verwendung der Daten betrachtet werden. Insbesondere in den Gruppengesprächen zeigten sich die Befragten erschrocken, wenn sie mit den Risiken der Verarbeitung personenbezogener Daten konfrontiert wurden. Trotzdem wurde eine Verhaltensänderung als zu aufwändig betrachtet. Kontrolle und Transparenz schienen für die Akzeptanz der Datenverarbeitung wichtig zu sein, und die Bürger äußerten Interesse an einer regelmäßigen Übersicht über ihre registrierten personenbezogenen Daten. Zudem werden Informationen über technologisch-gesellschaftliche Entwicklungen als wichtig und hilfreich für die Ausprägung des erforderlichen Datenschutzbewusstseins angesehen. Abschließend wurde festgestellt, dass das Vertrauen in eine ordnungsgemäße Nutzung und Verarbeitung personenbezogener Daten durch die Regierung erheblich größer ist als das Vertrauen in eine derartige Nutzung und Verarbeitung durch private Unternehmen und Einrichtungen.

Der Volksbefragung in Slowenien zufolge wurde die einzelstaatliche Datenschutzbehörde als vertrauenswürdigste staatliche Institution eingestuft.[97] Zu den Themen dieser vergleichenden Studie sind keine weiteren Umfragen verfügbar.

In Ungarn wurde 2005 eine Umfrage (eine repräsentative Stichprobe mit 1 000 Befragten) zur Bekanntheit der Verfassung und zu Kenntnissen über die Verfassung durchgeführt.[98] 8,1 % der Befragten waren der Meinung, dass das Recht auf Privatsphäre im Rahmen der derzeitigen Verfassung überhaupt nicht geschützt werden kann; 56,5 % hielten einen Schutz in geringerem Maße für möglich, und 33,5 % sind der Meinung, dass die Privatsphäre in höchstem Maße geschützt sei. Auf die Frage, ob der Umfang geändert werden müssen, in dem das Privatleben geschützt werde, bewerteten 38,9 % der Befragten das Schutzniveau für angemessen, und 58,3 % verlangten ein höheres Schutzniveau.[99] Im Jahr 2008 wurde vom Amt der Bürgerbeauftragten eine Umfrage zur Anerkennung und Würdigung der Bürgerbeauftragten in Auftrag gegeben.[100] Den Ergebnissen dieser Umfrage (mit Stichprobe von 1 000 Befragten) zufolge erhöhte sich der Anteil der Bürger, die sich aktiv über die Bürgerbeauftragten informiert hatten, von 15 % im Jahr 1998 auf 32 % im Jahr 2007; 59 % der Befragten kannten die einzelstaatliche Datenschutzbehörde; 11 % der Befragten waren sich sicher und weitere 28 % vermuteten, dass sie im Falle einer Verletzung ihrer Rechte einen Rechtsbehelf bei den Bürgerbeauftragten einlegen würden. In Bezug auf das Vertrauen der Öffentlichkeit erreichten die Bürgerbeauftragten unter den wichtigsten öffentlichen Einrichtungen den dritten Platz; dabei gaben 52 % der Befragten an, dass sie den Bürgerbeauftragten vertrauen.

Die Datenschutzbehörde des Vereinigten Königreichs hat die Sensibilisierung der Öffentlichkeit für den Datenschutz in Umfragen untersucht. Den neuesten Ergebnissen zum Thema Sensibilisierung der Öffentlichkeit zufolge ging der Anteil der Befragten, die die bestehenden Gesetze als hinreichenden Schutz der personenbezogenen Daten bewerteten, um zehn Prozentpunkte zurück (von 49 % 2006 auf 39 % 2007). Bei der Umfrage im Jahr 2007 wurden 1 223 Personen telefonisch befragt. Der Stichprobenplan umfasste Quoten für die Befragten, um sicherzustellen, dass bestimmte Gruppen in Bezug auf Geschlecht, Alter, Ethnizität und andere Variablen repräsentiert waren. Gemäß den Ergebnissen von Umfragen im Zeitraum 2004-2007 hat sich der Anteil der Befragten erhöht, die über ihr Recht auf Dateneinsicht informiert waren (wenn diese auf das Thema angesprochen wurden); 2004 waren 74 % und 2007 90 % der Befragten über ihr Anrecht auf Einsicht in die Daten informiert, die Organisationen über sie speichern. Tatsächlich hatten 17 % der Befragten von diesem Recht Gebrauch gemacht und bei einer Organisation Einsicht in ihre personenbezogenen Daten beantragt. Bei der Bewertung einer Liste typischer möglicher Vorbehalte der Bürger in Bezug auf den Umgang mit ihren personenbezogenen Daten gaben 83 % bis 94 % der Befragten jeweils an, sehr oder ziemlich besorgt zu sein. Die stärksten Bedenken betrafen die Weitergabe und den Verkauf von personenbezogenen Angaben an andere Organisationen sowie die Sicherheitsaspekte der Speicherung personenbezogener Angaben.[101]

Ergänzend zu den oben genannten Forschungsergebnissen besteht die wichtigste Erkenntnis der Eurobarometer-Umfragen darin, dass die nationalen Datenschutzbehörden den meisten EU-Bürgern nach wie vor relativ unbekannt sind. Dies kann als grundlegendes Problem betrachtet werden und erklärt weitgehend die fehlenden Kenntnisse hinsichtlich der ihnen übertragenen Befugnisse. Dieses Wissensdefizit geht mit einem mangelnden Rechtsbewusstsein und fehlenden Kenntnissen über die Befugnisse, den Aufgabenbereich, die Ressourcen und die Tätigkeiten der Datenschutzbehörden einher.

Informationen über das Rechtsbewusstsein – einschließlich der Kenntnisse über Verfahren, die eine Einhaltung der Datenschutzbestimmungen belegen, sowie über Praktiken in Bezug auf Sanktionen, Schadensersatz und Rechtsfolgen – stammen vorwiegend aus Umfragen (z. B. Eurobarometer-Umfragen). Die oben genannte, in Spanien vom Nationalen Institut für Kommunikationstechnologien durchgeführte Umfrage enthält Angaben im Zusammenhang mit der Sensibilisierung für die aus dem einzelstaatlichen Recht resultierenden Registrierungspflichten. Wie bereits erläutert, bestätigten 82 % der befragten Unternehmen, dass ihnen die Notwendigkeit der Einhaltung der maßgeblichen Bestimmungen bewusst sei, während 79 % ihre Absicht bekräftigten, wirtschaftliche Mittel und/oder Humanressourcen für die Einhaltung der Datenschutzbestimmungen vorzusehen. Diese Zahlen sind ermutigend, wenn man berücksichtigt, dass der Eurobarometer-Umfrage zufolge 56,1 % der innerhalb von Unternehmen für Datenschutzfragen zuständigen Personen mit den Bestimmungen des Datenschutzrechts einigermaßen vertraut waren und 30,2 % erklärten, dass sie mit diesen Bestimmungen nicht sehr vertraut seien, während nur 13,1 % angaben, dass sie mit den Bestimmungen sehr vertraut seien.

96 J. Koffijberg u. a. (2009), *Niets te verbergen en toch bang; Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan, Veröffentlichung Nummer 1774; siehe: www.cbpweb.nl/downloads_rapporten/rap_2009_niets_te_verbergen_en_toch_bang.pdf.

97 Siehe: www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=621.

98 Durchgeführt vom Institut Eötvös Károly in Zusammenarbeit mit der Fakultät für Rechtssoziologie der Universität Eötvös Lóránd.

99 László Majtényi, *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága.* (Die Informationsfreiheit. Datenschutz und Zugang zu öffentlichen Daten), 2006, Budapest, Complex Kiadó. S. 58-61.

100 Szonda Ipsos Media, Meinungs- und Marktforschungsinstitut, www.obh.hu/szonda_ipsos_OBH.doc.

101 *Report on Information Commissioner's Office Annual Track 2007*, S. 7, Randnummer 4.2. Abrufbar unter: www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_track_2007_individuals_report.pdf; umfassende Angaben zu den Fragen und Antworten der Umfrage sind im Hauptteil dieses Berichts zu finden.

5 Analyse von Defiziten

In diesem Abschnitt des Berichts werden die wichtigsten Defizite des Systems für den Schutz personenbezogener Daten auf EU-Ebene und auf einzelstaatlicher Ebene analysiert. Dabei liegt der Schwerpunkt zunächst auf den Herausforderungen in den Bereichen Datenschutzbehörden, Einhaltung der Bestimmungen der einschlägigen Rechtsvorschriften, Rechtsbehelfe, Schadensersatz und Sanktionen bei Verletzungen des Rechts auf Privatsphäre und Datenschutz sowie Maßnahmen zur Sensibilisierung für die bestehenden Rechte. Anschließend werden dann die wichtigsten Bereiche ermittelt, die von der Anwendung der Datenschutzgesetze ausgeschlossen oder freigestellt sind beziehungsweise aus sonstigen Gründen nicht berührt werden.

5.1. Unzulänglichkeiten im Datenschutzrecht

5.1.1. Datenschutzbehörden

Im Zusammenhang mit der Organisation, der Funktionsweise und der praktischen Arbeitsweise der Datenschutzbehörden sind verschiedene Defizite festzustellen. Auf struktureller Ebene besteht ein wichtiges Problem in der mangelnden Unabhängigkeit mehrerer Kontrollstellen. In verschiedenen Mitgliedstaaten (z. B. in Estland, Irland, Lettland, Litauen und im Vereinigten Königreich) bestehen Vorbehalte hinsichtlich der tatsächlichen Fähigkeit der Mitarbeiter der Datenschutzbehörden, ihre Aufgaben in völliger Unabhängigkeit auszuführen. Eine der wichtigsten Erklärungen für diesen Mangel steht mit dem Verfahren für die Berufung oder Ernennung der Mitarbeiter im Zusammenhang: Wenn die ausschließliche Befugnis zur Auswahl der leitenden Mitarbeiter bei der Regierung liegt und Vorschläge, Nachprüfungen oder Zustimmungen des Gesetzgebers nicht vorgesehen sind, erhöht sich die Gefahr einer faktischen Subordination oder Marginalisierung der Kontrollstellen beträchtlich (siehe auch Abschnitt 3.1.1). Dieses Problem könnte durch eine Reform des Berufungs-/Ernennungsverfahrens gelöst werden. Durch eine weitere Änderung der Datenschutzrichtlinie könnte die Anforderung der Unabhängigkeit (die derzeit in Artikel 28 Absatz 1 der Richtlinie festgelegt ist) möglicherweise spezifischer und genauer gefasst werden.

Auf funktionaler Ebene stellen der Personalmangel und das Fehlen angemessener Finanzmittel mehrerer Kontrollstellen ein erhebliches Problem dar. In vielen Mitgliedstaaten sind die Datenschutzbehörden aufgrund der begrenzten wirtschaftlichen Mittel und Humanressourcen nicht in der Lage, ihre Aufgaben vollständig auszuführen. Dies ist der Fall in Bulgarien, Frankreich, Griechenland, Italien, Lettland, den Niederlanden, Österreich, Portugal, Rumänien, der Slowakei und Zypern. Für die Kontrollstellen sind jedoch finanzielle Unabhängigkeit und Fachkräfte nicht nur unverzichtbar, um einen wirksamen Schutz des Rechts auf Datenschutz zu gewährleisten, sondern stellen auch eine Voraussetzung für eine echte Unabhängigkeit vom Willen der Regierung dar. Gesetzesreformen könnten darauf ausgerichtet sein, die Haushaltskontrolle und das Humanressourcenmanagement der Datenschutzbehörden zu verbessern (z. B. indem ihnen die direkte Einstellung von Fachkräften ermöglicht wird).

Auf operativer Ebene sind die begrenzten Befugnisse mehrerer Kontrollstellen problematisch. In manchen Mitgliedstaaten sind die Datenschutzbehörden nicht in vollem Umfang mit Untersuchungs-, Einwirkungs-, Beratungs- und Befassungsbefugnissen nach Artikel 28 Absätze 2, 3 und 4 der Datenschutzrichtlinie ausgestattet. In Österreich, Ungarn und Polen können die Kontrollstellen ihre Entscheidungen zur Verwarnung des Auftragsverarbeiters/für die Verarbeitung Verantwortlichen nicht durchsetzen, um so dessen unrechtmäßiges Verhalten zu beenden. In Belgien und Deutschland können sie weder die Sperrung, Löschung oder Vernichtung von Daten anordnen noch ein vorübergehendes oder endgültiges Verarbeitungsverbot verhängen. Im Vereinigten Königreich und in Frankreich haben sie ohne vorherige richterliche Anordnung keinen Zutritt zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden. In vielen Ländern (z. B. in Frankreich, in Griechenland, in Irland, in Italien, in Litauen, Malta, in Österreich, in Polen, Rumänien, Slowenien, in der Tschechischen Republik, sowie im Vereinigten Königreich) wiederum werden Kontrollstellen vom Gesetzgeber bei der Ausarbeitung von Gesetzen, die sich auf die Privatsphäre und den Datenschutz auswirken können, nur willkürlich konsultiert, weil keine konkrete entsprechende Verpflichtung für den Gesetzgeber besteht. Eine unvollständige Umsetzung der Anforderungen der Datenschutzrichtlinie verstößt nicht nur gegen geltendes EU-Recht, sondern ist auch als erhebliches Defizit des jeweiligen einzelstaatlichen Systems für den Schutz personenbezogener Daten zu betrachten, das die Wirksamkeit des Systems beeinträchtigen kann. Da das EU-Recht im Hinblick auf die Befugnisse der Datenschutzbehörden besonders eindeutig ist, sollten die einzelstaatlichen Rechtsvorschriften gegebenenfalls geändert werden, um die einzelstaatlichen Bestimmungen mit den auf EU-Ebene festgelegten Anforderungen in Einklang zu bringen.

5.1.2. Einhaltung der Standards

Betrachtet man den Grad der tatsächlichen Einhaltung der einschlägigen Datenschutzbestimmungen, insbesondere im Hinblick auf die Registrierungspflicht der öffentlichen und privaten Akteure, die Datenverarbeitungen vornehmen, werden verschiedene Defizite deutlich. Wenngleich die Beurteilung der tatsächlichen Einhaltung der Datenschutzbestimmungen in einer Reihe von Mitgliedstaaten (z. B. Bulgarien, Dänemark, Lettland, Niederlande, Portugal, Rumänien und Slowakei) infolge des Fehlens zuverlässiger oder präziser Informationen schwierig ist, scheint doch in jedem Fall eine Kluft zwischen dem gesetzlich verankerten Schutz des Rechts auf Achtung der Privatsphäre (der möglicherweise formell den Anforderungen des EU-Rechts und des internationalen Rechts entspricht) und dem tatsächlichen Schutz dieser Rechte in der Praxis zu geben. So ist zum Beispiel die Einhaltung der Datenschutzbestimmungen bei öffentlichen Einrichtungen in Estland und Rumänien als erstaunlich schlecht zu bewerten. Andererseits führt in den meisten Ländern das Fehlen eindeutiger Konzepte für die relevanten Begriffe (bzw. das Fehlen gemeinsamer Auslegungen dieser Begriffe) – z. B. „personenbezogene Daten", „Datei", „Verarbeitung" – zu Unsicherheiten in Bezug auf die Frage, welche Tätigkeiten unter die einschlägigen Gesetze zum Schutz personenbezogener Daten fallen. Die „Artikel-29-Datenschutzgruppe" spielt eine entscheidende Rolle

bei der Entwicklung einer gemeinsamen Auslegung dieser ungenauen Bestimmungen; dieser Prozess ist jedoch auch von der Akzeptanz und Umsetzung dieser Auslegungen in den Mitgliedstaaten abhängig. Komplexe Zusammenhänge und Ungereimtheiten können zudem durch die Zersplitterung der den Datenschutz betreffenden Rechtsvorschriften in verschiedene, sektorspezifische Gesetze verursacht werden (etwa in Finnland und in Griechenland). Unter diesem Gesichtspunkt könnte somit eine bessere Durchsetzung der Datenschutznormen durch die Beteiligten in der Praxis ausreichen, um das erste Problem zu lösen; in Bezug auf das zweite Problem wären dagegen zusätzliche Rechtsvorschriften zur Konkretisierung ungenauer Bestimmungen und zur Vereinfachung des Rechtsrahmens sinnvoll. Die meisten Unzulänglichkeiten im Zusammenhang mit den komplexen Zusammenhängen und der Ungenauigkeit der Datenschutzbestimmungen sind zu einem guten Teil auf den Wortlaut der Datenschutzrichtlinie zurückzuführen. Diesbezügliche Lösungen sind daher vorzugsweise auf EU-Ebene zu entwickeln.

Ein wichtiges Problem ist die in verschiedenen Mitgliedstaaten (insbesondere im Vereinigten Königreich) dokumentierte weit verbreitete Missachtung der grundlegenden Verpflichtung zur Registrierung bei der Datenschutzbehörde, vor Beginn der Datenverarbeitung. Probleme treten beispielsweise immer wieder im Zusammenhang mit der Videoüberwachung auf: In der Praxis sind die meisten Überwachungskameras in Bulgarien, Frankreich, Litauen, Österreich, Schweden und der Tschechischen Republik überhaupt nicht registriert; entsprechend unterliegt die Nutzung dieser Kameras auch nicht der Aufsicht und der Kontrolle durch die einzelstaatlichen Kontrollstellen. Ein weiterer Bereich, der Anlass zu großer Besorgnis bietet, ist das Internet (z. B. in Slowenien und in Spanien). Dass Auftragsverarbeiter/für die Verarbeitung Verantwortliche ihren Registrierungspflichten nicht nachkommen, ist häufig eher auf das Fehlen entsprechender Kenntnisse der Rechtsvorschriften als auf eine bewusste Missachtung zurückzuführen. Diese Unzulänglichkeit stellt eine besondere Herausforderung für die Wirksamkeit der Datenschutzbestimmungen dar. Ungeachtet der Schwierigkeiten beim Bemühen, die rechtlichen Bestimmungen neuen technologischen Entwicklungen anzupassen, scheinen daher zusätzliche Rechtsvorschriften zur Einführung oder Verbesserung der gesetzlichen Bestimmungen im Zusammenhang mit Technologien, die für das Recht auf Schutz personenbezogener Daten (wie Kameraüberwachung, Abhören von Telefongesprächen, Zellproben oder Vorratsspeicherung von DNA-Codes usw.) maßgeblich sind, dringend erforderlich zu sein (u. a. um eine – etwa in der Tschechischen Republik in besorgniserregender Weise erfolgte – Diskriminierung hinsichtlich des Schutzes der Datenrechte aufgrund des wirtschaftlichen Status zu vermeiden).[102]

5.1.3. Sanktionen, Schadensersatz und Rechtsfolgen

Manche Probleme resultieren aus den einzelstaatlichen Systemen für Rechtsbehelfe bzw. aus den Regelungen zur Verhängung von Sanktionen und zur Verpflichtung zu Schadensersatzleistungen sowie aus der Anwendung der Datenschutzbestimmungen im Beschäftigungsbereich. Defizite hinsichtlich der von der Datenschutzbehörde zu verhängenden Sanktionen traten in verschiedenen Ländern auf – entweder weil die Geldbußen bzw. Geldstrafen nur begrenzte abschreckende Wirkung haben und/oder zu selten verhängt werden, oder weil die Kontrollstellen einfach keine Praxis zur Verhängung der betreffenden Sanktionen entwickelt haben (Belgien, Dänemark, Finnland, Litauen, Österreich, Polen, Ungarn und Vereinigtes Königreich). Die in manchen Mitgliedstaaten (beispielsweise in Irland) fehlende rechtliche Verpflichtung für Auftragsverarbeiter/für die Verarbeitung Verantwortliche, Verstöße gegen die Datenschutzbestimmungen zu melden, kann dann die Schwäche des Vollzugssystems nochmals verschärfen. In einigen Mitgliedstaaten (z. B. in Deutschland, Frankreich, Lettland, den Niederlanden, Österreich, Polen, Ungarn und im Vereinigten Königreich) sind die Strafverfolgung und die Sanktionen im Falle von Verstößen gegen das Datenschutzgesetz äußerst begrenzt. In verschiedenen Mitgliedstaaten (z. B. in Finnland, Irland, den Niederlanden und im Vereinigten Königreich sowie in Estland, Lettland, Malta, Polen, Schweden und Zypern in Bezug auf Schadensersatzleistungen von privaten Stellen) schließt das einzelstaatliche Rechtssystem aufgrund des Zusammenwirkens mehrerer Faktoren – beispielsweise der Handhabung der Beweislast, Schwierigkeiten hinsichtlich der Quantifizierung des Schadens sowie der kaum vorhandenen Unterstützung seitens der meist im Bereich der Öffentlichkeitsarbeit tätigen Kontrollstellen – die Möglichkeit der Erwirkung von Schadensersatz wegen der Verletzung von Datenschutzrechten praktisch aus. Der Einsatz „weicher" Methoden *ex ante* ist zwar als positive Praxis zur Gewährleistung der Einhaltung der Datenschutzbestimmungen zu bewerten, die Mitgliedstaaten müssen jedoch unbedingt auch „harte Rechtsinstrumente" vorsehen, mit deren Hilfe Urheber von Verletzungen des Rechts auf Schutz der Privatsphäre bestraft und zu Schadensersatzleistungen für Opfer verpflichtet werden können. Gesetzesreformen (die auf einzelstaatlicher Ebene als unverzichtbar zu betrachten sind) können hier eine maßgebliche Rolle spielen, indem sie für wirksamere und umfassendere Rechtsbehelfe unter Einführung von Wiedergutmachungen für Rechtsverletzungen sorgen. Gleichzeitig kann auch die Sensibilisierung von betroffenen Personen sowie von Richtern und Staatsanwälten für die Bedeutung des Rechts auf Datenschutz eine bessere Durchsetzung der bereits vorhandenen Bestimmungen für die Bestrafung von Verstößen gegen das Datenschutzrecht ermöglichen.

In vielen Mitgliedstaaten (Belgien, Bulgarien, Dänemark, Estland, Frankreich, Litauen, Malta, Österreich, Rumänien, Schweden, Vereinigtes Königreich und Zypern) bestehen noch keine Gesetze zur Anpassung der Datenschutzbestimmungen im Beschäftigungsbereich; offensichtlich wird also die Notwendigkeit der Einführung besonderer Datenschutzbestimmungen zur Regelung der Nutzung von personenbezogenen Daten im Beschäftigungsbereich nicht anerkannt. Entsprechend waren in manchen Ländern (z. B. in Deutschland, Schweden und Zypern in der Privatwirtschaft) Verletzungen der Persönlichkeitsrechte von natürlichen Personen durch geheime (Video-) Überwachung von Arbeitnehmern am Arbeitsplatz zu verzeichnen. In anderen Mitgliedstaaten (z. B. Finnland) dagegen war der Rechtsrahmen bisher zufriedenstellend; durch kürzlich erfolgte Gesetzesänderungen wurde der Schutz im Beschäftigungsbereich jedoch beeinträchtigt.[103] Die EU – die auf den Grundsätzen der sozialen Marktwirtschaft basiert – misst der Arbeit große Bedeutung bei, und die Freizügigkeit der Arbeitnehmer ist in den EU-Verträgen als eine der Grundfreiheiten verankert. Da die Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten nachteilige Auswirkungen auf das Funktionieren des Binnenmarkts haben können, wäre ein diesbezügliches Einschreiten der EU zur Festlegung

102 Weitere Informationen über die so genannte „OpenCard"-Sache siehe: http://opencard.praha.eu/jnp/en/home/index.html (auf Englisch).

103 www.hs.fi/english/article/Lex+Nokia+passes+in+Parliament+-+government+party+ranks+split/1135244038215.

eines Mindeststandards für den Schutz personenbezogener Daten im Beschäftigungsbereich von großem Nutzen. Ein solches Einschreiten entspricht zum einen dem Subsidiaritätsprinzip und ist zum anderen unverzichtbare Voraussetzung, wenn sichergestellt werden soll, dass die in den gemeinsamen Verfassungstraditionen der Mitgliedstaaten und im einschlägigen EU-Recht anerkannten Grundrechte von Arbeitnehmern umfassend geschützt werden.

5.1.4. Rechtsbewusstsein

In Abschnitt 4.4 wurde ein vergleichender Überblick zum Thema Rechtsbewusstsein vermittelt, und in Abschnitt 6.3 werden vielversprechende Praktiken im Zusammenhang mit dem Rechtsbewusstsein beschrieben. Die Mitwirkung von Datenschutzbehörden an der Stärkung des Rechtsbewusstseins der verschiedenen Akteure war generell positiv.

Es sind jedoch einige wenige negative Beispiele erkennbar, bei denen sich die Datenschutzbehörden im Bereich der Sensibilisierung nicht engagiert haben (z. B. in Estland und in Rumänien). So haben in einer Reihe von Mitgliedstaaten (z. B. Bulgarien, Litauen und der Slowakei) die Kontrollstellen noch keine nutzerfreundlichen und/oder umfassend aktualisierten Websites eingerichtet, auf denen alle Informationen zum Datenschutz für die breite Öffentlichkeit zugänglich und Gutachten und Vorschriften der Datenschutzbehörde problemlos zugänglich wären. Ferner wurden in manchen Ländern (z. B. in Bulgarien und in Malta) Bedenken hinsichtlich des Ausmaßes der Öffentlichkeit und der Transparenz der Tätigkeiten der Datenschutzbehörde geäußert, insbesondere wenn die Kontrollstelle einvernehmliche Lösungen für Rechtsstreitigkeiten mit Urhebern von Verstößen gegen das Datenschutzrecht aushandelt, ohne diese öffentlich bekannt zu geben (z. B. im Vereinigten Königreich). Und schließlich ist in mehreren Mitgliedstaaten (z. B. in Griechenland und Österreich) die Leistung der Kontrollstelle zwar generell zufriedenstellend; es kann jedoch unverhältnismäßig lange dauern, bis betroffene Personen Informationen erhalten. Dies liegt häufig daran, dass es den Datenschutzbehörden an ausreichenden Ressourcen fehlt, um alle Anfragen von betroffenen Personen zügig beantworten zu können. Insoweit ist zu bezweifeln, dass neue Rechtsvorschriften auf EU-Ebene oder auf einzelstaatlicher Ebene die derzeitige Situation verbessern könnten. Vielmehr müssen die nationalen Datenschutzbehörden ihre Arbeit möglicherweise besser organisieren, um betroffenen Personen umgehend Unterstützung gewähren zu können. Zudem ist eine Haltungsänderung erforderlich, um die Öffentlichkeit besser über die Arbeit der Datenschutzbehörden zu informieren und die beteiligten Akteure für Datenschutzrechte zu sensibilisieren. Datenschutzbehörden sollten die Bedeutung ihrer praktischen Rolle im Bereich der Sensibilisierung anerkennen und können sich problemlos auf Beispiele vielversprechender Praktiken von anderen europäischen Kontrollstellen stützen, um diesen Mängeln zu begegnen.

Noch problematischer ist allerdings, dass die Datenschutzbehörden in einigen Mitgliedstaaten (z. B. im Vereinigten Königreich) deutlich gemacht haben, dass sie sich nicht als zuständig dafür betrachten, dass das einzelstaatliche Datenschutzrecht in einer den EU-Standards und den internationalen Standards zum Schutz personenbezogener Daten entsprechenden Weise ausgelegt wird (auch wenn die einzelstaatlichen Rechtsvorschriften weitgehend die maßgeblichen EU-Bestimmungen und internationalen Regelungen in einzelstaatliches Recht umsetzen). Die Arbeit der nationalen Datenschutzbehörden ist jedoch maßgeblich für die Entwicklung eines gemeinsamen Verständnisses der Grundsätze des Datenschutzrechts. Ihre (spontane) Konvergenz sollte daher als gute Praxis hervorgehoben werden – nicht nur, um die Übereinstimmung zwischen den verschiedenen Rechtssystemen sicherzustellen, sondern auch, um einen angemessenen Standard für den Schutz des Rechts auf Privatsphäre zu definieren. Die Gesetzgebung kann hier nur begrenzt einwirken: Änderungen der Konzepte einzelstaatlicher Kontrollstellen müssen auf kultureller und nicht auf politischer/legislativer Ebene erfolgen.

5.2. Problembereiche im Datenschutz

In diesem Abschnitt werden die wesentlichen Problembereiche ermittelt, die von der Anwendung der Datenschutzgesetze ausgeschlossen oder freigestellt sind beziehungsweise anderweitig von diesen nicht wirksam erfasst werden. In diesem Zusammenhang ist auf drei allgemeine Kategorien zu verweisen: Ausnahme von Tätigkeiten im Zusammenhang mit der Sicherheit des Staates (z. B. Nachrichtendienste oder militärische Tätigkeiten) aus dem Datenschutzsystem; Schutz von die Gesundheit natürlicher Personen betreffenden Daten; und Videoüberwachung.

5.2.1. Datenschutz und die Sicherheit des Staates

Artikel 13 Absatz 1 der Datenschutzrichtlinie (über Ausnahmen und Einschränkungen) besagt: „Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für: a) die Sicherheit des Staates; b) die Landesverteidigung; c) die öffentliche Sicherheit".

Die in Artikel 13 Absatz 1 Buchstaben a bis c der Datenschutzrichtlinie genannten Ausnahmen stehen miteinander im Zusammenhang. In verschiedenen Mitgliedstaaten (Dänemark, Griechenland, Irland, Luxemburg, Portugal und Rumänien) werden sie als die wichtigsten Bereiche bezeichnet, die aus dem Anwendungsbereich des Datenschutzgesetzes ausgenommen sind. Diese Regelung entspricht dem Wortlaut von Artikel 13 der Datenschutzrichtlinie. Im Zusammenhang mit der Auslegung dieser Bestimmung sind jedoch die folgenden wichtigen Aspekte zu bedenken.

Zunächst gestattet der Wortlaut eine „Beschränkung" im Zusammenhang mit Sicherheitsfragen. Dies ist nicht als gleichwertig mit einer „Ausnahme" vom Anwendungsbereich der Richtlinie aufzufassen. Eine grammatikalische Auslegung ist nicht der einzige Grund für die Argumentation, dass der Tätigkeitsumfang verschiedener Teilbereiche der Exekutive sehr wohl in den Anwendungsbereich der Richtlinie fällt.

Zweitens nennt der erste Erwägungsgrund der Richtlinie die Europäische Konvention zum Schutze der Menschenrechte als Hintergrund der Verarbeitung personenbezogener Daten. Zudem besagt der dritte Erwägungsgrund explizit, dass die Grundrechte der Personen gewahrt werden müssen. Wie bereits in anderen Teilen dieser vergleichenden Studie aufgezeigt, sind der Schutz der Menschenrechte und die Unversehrtheit des Einzelnen im Bereich des Datenschutzes grundlegende Voraussetzungen.[104]

104 Siehe Abschnitt 2.1 über die grundlegenden Datenschutzstandards auf der Ebene des Europarates.

Drittens besteht das Kernanliegen der Richtlinie nicht in der Schaffung eines überwachungsfreien Raums, in dem die Staaten außerhalb des Rechtsrahmens agieren können. Im Zusammenhang mit Fragen der Sicherheit des Staates ist vielmehr eine Verhältnismäßigkeitsprüfung vorzunehmen (d. h. die Abwägung von Grundrechten gegenüber anderen Interessen und nicht die ungeprüfte Außerkraftsetzung von Grundrechten).

Viertens muss die Richtlinie gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union ausgelegt werden, wobei die Charta der Grundrechte und die Verträge nach dem neuen Artikel 6 des Vertrags über die Europäische Union „rechtlich gleichrangig" sind. Artikel 8 kann nur unter den in Artikel 52 der Charta vorgesehenen Bedingungen eingeschränkt werden. Artikel 13 Absatz 1 der Datenschutzrichtlinie sieht umfassende Ausnahmen und Beschränkungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich vor. Hinsichtlich des Geltungsbereichs dieser Ausnahmen und Beschränkungen fehlt es an Klarheit. In verschiedenen Mitgliedstaaten sind diese Bereiche insgesamt vom Schutzumfang des Datenschutzrechts ausgenommen. Dadurch entsteht ein nicht regulierter Bereich beträchtlichen Ausmaßes mit schwerwiegenden Folgen für den Schutz der Grundrechte. Nach Artikel 52 der Charta muss jede Einschränkung der in dieser Charta anerkannten Rechte und Freiheiten „gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten".

Aus diesen Gründen steht die Entscheidung einzelstaatlicher Gesetzgeber, manche Teilbereiche der Exekutive (z. B. Nachrichtendienste oder das Verteidigungsministerium) vollständig auszunehmen, im Widerspruch zum normativen Rahmen der Datenschutzrichtlinie.

5.2.2. Datenschutz und Gesundheitsdaten

In mehreren Ländern (z. B. in Bulgarien, Schweden und Slowenien) wurden Bedenken hinsichtlich des Schutzrahmens für gesundheitsbezogene Daten geäußert. Nach Artikel 8 Absatz 2 der Datenschutzrichtlinie sind die Mitgliedstaaten verpflichtet, die Verarbeitung von Daten über die Gesundheit von Personen zu untersagen. Artikel 8 Absatz 3 sieht eine Ausnahme vor, „wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen".

Wenn allen Beschäftigten im Gesundheitswesen Zugriff auf sämtliche Patientendaten gewährt wird, können Effizienzgewinne erzielt werden; außerdem ist eine derartige allgemeine Zugriffsmöglichkeit in medizinischen Notfällen von Vorteil. In diesem Fall erlangen allerdings auch mehr Menschen Zugang zu sensiblen Daten (was eine stärkere Verletzung des Rechts auf Unversehrtheit darstellt), und die Gefahr einer Offenlegung sensibler Daten wächst. Über die Zugriffsmöglichkeiten kann beispielsweise anhand der Position, des medizinischen Fachgebiets und einer etablierten Zusammenarbeit entschieden werden. Abteilungen, die regelmäßig zusammenarbeiten, weil sie derselben Organisation angehören, sollten – soweit die erforderliche Vertraulichkeit sichergestellt ist – in der Regel Zugang zu den Informationen der jeweils anderen Abteilung erhalten können. Es muss auch effiziente Hilfsmittel für die Verlaufskontrolle und Rückverfolgbarkeit geben. Die Identifizierung der Nutzer muss den Sicherheitsauflagen entsprechen.

Die Einführung eines rechtsverbindlichen Instruments auf EU-Ebene kann schwere Auswirkungen im Gesundheitswesen der Mitgliedstaaten nach sich ziehen. Ein sinnvollerer Ansatz dürfte darin bestehen, sicherzustellen, dass die Vorschriften für im Gesundheitswesen Beschäftigte in Bezug auf Vertraulichkeit und Privatsphäre den Zielen der Richtlinie entsprechen, und somit die betroffene Person wirksam zu schützen, ohne das Recht der Person auf den Schutz ihrer Gesundheit zu beeinträchtigen.[105]

In manchen Mitgliedstaaten haben die Gesetzgeber in letzter Zeit einschlägige Rechtsvorschriften ausgearbeitet. In Belgien beispielsweise wurde eine Gesetzesvorlage zur Einrichtung des Portals *„e-health"*[106] eingebracht; über dieses Portal sollen u. a. medizinische Daten zwischen Beschäftigten und Einrichtungen im Gesundheitswesen ausgetauscht werden, um das Gesundheitssystem zu vereinfachen und zu verbessern. Das System ermöglicht außerdem die Übermittlung elektronischer Verordnungen für pharmazeutische Produkte. Da jedoch Ärzte, Krankenhäuser, Krankenkassen und einige Sozialversicherungseinrichtungen Zugang zu dem System haben werden, bestehen Bedenken dahingehend, dass die Privatsphäre der Patienten möglicherweise nicht ausreichend geschützt wird. Bei der Ausarbeitung einzelstaatlicher Rechtsvorschriften in Bezug auf den sensiblen Bereich der Gesundheit sollten die Rechte der Bürger sorgsam gegen andere Interessen abgewogen werden.

5.2.3. Datenschutz und Videoüberwachung

Wie weiter oben erläutert, wurde die Videoüberwachung als potenziell bedenklicher Bereich dargestellt. In Österreich ist die große Mehrzahl der Überwachungskameras überhaupt nicht registriert und unterliegt somit nicht der Aufsicht und Kontrolle der einzelstaatlichen Datenschutzbehörde. In Deutschland sind verschiedene Fälle geheimer Videoüberwachung von Arbeitnehmern am Arbeitsplatz aktenkundig geworden. Vielfach wird auch das Recht auf Selbstbestimmung verletzt, wenn betroffene Personen nur unzureichend über die Nutzung und/oder Verarbeitung ihrer Daten informiert werden. Ein bekanntes Beispiel für die Videoüberwachung am Arbeitsplatz ist die Überwachung der Verwaltungsmitarbeiter der einzelstaatlichen Wettbewerbsbehörde Zyperns durch den Behördenleiter, die letztendlich zu dessen Rücktritt führte. Es ist daran zu erinnern, dass der griechischen einzelstaatlichen Datenschutzbehörde der Zugang zu den Räumlichkeiten der Polizei verweigert wurde, in denen Daten verarbeitet wurden. Im Vereinigten Königreich gibt es wenige Beschränkungen für den Einsatz von CCTV-Kameras im öffentlichen Raum,[107] und bereits jetzt gibt es im Vereinigten Königreich mehr CCTV-Kameras als irgendwo anders auf der Welt.

105 Siehe auch Arbeitsdokument WP131 der Artikel-29-Arbeitsgruppe vom 15. Februar 2007: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

106 Belgien/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2008, siehe: www.privacycommission.be/nl/docs/Commission/2008/advies_33_2008.pdf; Commission de la protection de la vie privée, Avis no. 33/2008 (24.9.2008), siehe: www.privacycommission.be/fr/docs/Commission/2008/avis_33_2008.pdf (Französisch).

107 www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm#a41, Randnummer 213.

Die Datenschutzrichtlinie enthält keine ausführlichen Leitlinien zur Videoüberwachung. Erwägungsgrund 14 besagt: „In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muss diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden." Dies ist so aufzufassen, dass derartige Daten weitgehend unter die Definition des Begriffs „personenbezogene Daten" nach Artikel 2 der Datenschutzrichtlinie fallen können, damit sich eine natürliche Person auf den durch das EU-Recht vorgesehenen Schutz berufen kann.

Artikel 33 der Datenschutzrichtlinie besagt jedoch: „Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten." Dies macht deutlich, dass die EU der Videoüberwachung besondere Bedeutung beimisst. Es ist zu beachten, dass die Artikel-29-Arbeitsgruppe diesbezüglich einige Leitlinien bereitgestellt hat.[108] In Anbetracht der inhärenten technischen Besonderheiten von Ton- und Bilddaten sowie der weitreichenden potenziellen Auswirkungen auf die Rechte natürlicher Personen sollte für die Zukunft eine gesonderte EU-Legislativmaßnahme in Erwägung gezogen werden.

Die Gesetzgeber einiger Länder haben sich jüngst mit diesem Bereich befasst, es ist jedoch zu bezweifeln, ob der eingeschlagene Weg angemessen ist. In Dänemark wurden im Juni 2007 zwei Gesetze in Bezug auf die Videoüberwachung verabschiedet. Das erste Gesetz überträgt Privatunternehmen erweiterte Befugnisse in Bezug auf die Videoüberwachung in mit ihrem Besitz verbundenen Bereichen. Es besteht nicht mehr die Verpflichtung, vor der Installation von Überwachungsanlagen die Datenschutzbehörde zu unterrichten. Durch das zweite Gesetz werden die Befugnisse des polizeilichen Nachrichtendiensts so ausgeweitet, dass dieser Informationen mit dem Nachrichtendienst des Militärs austauschen und ohne richterliche Anordnung Informationen bei anderen öffentlichen Stellen, beispielsweise Krankenhäusern, Schulen, Bibliotheken, Sozialdiensten usw. erheben kann. Das Gesetz überträgt der Polizei zudem erweiterte Befugnisse dahingehend, dass sie von öffentlichen Stellen und privaten Parteien die Installation von Videoüberwachungsanlagen und die Durchführung einer Videoüberwachung verlangen kann.

Das Problem des Datenschutzes im Zusammenhang mit der Videoüberwachung ist Teil einer umfassenderen Debatte: der Notwendigkeit einer Aktualisierung des Datenschutzrechts, um mit den technologischen Entwicklungen Schritt zu halten. Die jüngsten und ständigen technologischen Entwicklungen (einschließlich *„Cloud Computing"*, *„Autonomic Computing"*, IKT-Implantate im menschlichen Körper, Nanotechnologien, Gehirn-Computer-Schnittstellen usw.) bergen neue Herausforderungen, die dringend bewältigt werden müssen. Auch die Auswirkungen des Internets und neuer Technologien für soziale Netzwerke wie Facebook und Twitter auf den Schutz grundlegender Datenschutzrechte müssen in geeigneter Weise berücksichtigt werden. Die Bedeutung der „digitalen Identität" natürlicher Personen kann kaum überbewertet werden.[109] Sie stellt heutzutage eine maßgebliche Komponente der allgemeinen Identität und Persönlichkeit dar. Als solche verdient sie ein gleichwertiges Schutzniveau wie andere „herkömmliche" Facetten der Persönlichkeit. Die digitale Identität ist untrennbar mit der „digitalen Existenz" einer Person verknüpft. In der Weite des Cyberspace kann eine Person ein Dasein begründen und Tätigkeiten ausführen, die früher nur im „realen" öffentlichen Bereich denkbar waren. Besondere Aufmerksamkeit haben in dieser Hinsicht die Arbeit des Forums für Internet-Verwaltung (*Internet Governance Forum,* IGF) sowie die neue „Internet-Grundrechte-Charta" verdient, auf die in einer Entschließung des Europäischen Parlaments zur Stärkung der Sicherheit und der Grundfreiheiten im Internet Bezug genommen wird.[110]

108 Siehe Arbeitsdokument WP 67 vom 25. November 2002: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf; Gutachten 4/2004, WP 89 vom 11. Februar 2004: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf .

109 Bericht mit einem Vorschlag für eine Empfehlung des Europäischen Parlaments an den Rat zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (2008/2160(INI)), Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, siehe: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2009-0103+0+DOC+XML+V0//DE.

110 T6-0194/2009 vom 26. März 2009.

6 Vielversprechende Praktiken

In diesem Abschnitt des Berichts werden kurz die wichtigsten vielversprechenden Praktiken im Zusammenhang mit dem Datenschutz in den EU-Mitgliedstaaten vorgestellt, wobei positive einzelstaatliche Beispiele im Zusammenhang mit den Datenschutzbehörden sowie mit der Einhaltung von Bestimmungen, der Inanspruchnahme von Rechtsbehelfen und der Ausprägung eines Rechtsbewusstseins hervorgehoben werden. Mit der Ermittlung von vielversprechenden Praktiken wird die Bedeutung der jeweiligen Verfahren anerkannt und ein Betrag zur Förderung einer Kultur der ständigen Weiterentwicklung geleistet. Aus der Bewertung als „vielversprechende Praktik" ist jedoch nicht zu folgern, dass die betreffenden Verfahren tatsächlich einer unmittelbaren eingehenden Prüfung durch die FRA unterzogen worden wären.

6.1. Datenschutzbehörden

Die vielversprechenden Praktiken in Bezug auf nationale Datenschutzbehörden haben entweder mit der Struktur der Kontrollstellen oder mit ihrer Arbeit zu tun. Einerseits haben nämlich mehrere Mitgliedstaaten ihre nationalen Datenschutzbehörden mit spezifischen Befugnissen ausgestattet und ihnen ein hohes Maß an Unabhängigkeit zugesichert. Andererseits haben Datenschutzbehörden eine Zusammenarbeit mit beteiligten Akteuren in drei Kategorien aufgebaut: staatlichen Einrichtungen, einschlägig tätigen NRO sowie Datenschutzbehörden anderer Mitgliedstaaten.

Die Unabhängigkeit der Datenschutzbehörden ist ein unverzichtbarer Faktor für die Gewährleistung eines hohen Maßes an Datenschutz. Unter diesem Gesichtspunkt stellen strukturelle Maßnahmen wie die Verleihung einer eigenen Rechtspersönlichkeit für die Kontrollstelle (wie in Malta und in Spanien) oder die Kodifizierung ihrer Befugnisse und ihres Aufgabenbereichs in der Verfassung (etwa in Griechenland und in Portugal) positive Beispiele für die Verbesserung der Unabhängigkeit von Kontrollstellen dar. Auch wenn ihre Wahl durch die Legislative nicht notwendigerweise die Unabhängigkeit der Mitarbeiter der Kontrollstelle gewährleistet, sollten Verfahren, die (wie in Griechenland vorgesehen) einen Konsens zwischen Mehrheit und Opposition erfordern, als vielversprechende Praktik betrachtet werden. Ein weiteres bewährtes Verfahren, das eine weit gehende Unabhängigkeit der Datenschutzbehörde gewährleistet, ist in Slowenien vorgesehen, wo die nationale Datenschutzbehörde eine Klagebefugnis besitzt, um die Verfassungsmäßigkeit von Rechtsvorschriften durch das Verfassungsgericht prüfen lassen zu können.

Die Befugnis der Datenschutzbehörden, sich aktiv an der Ausarbeitung und Vorlage von Verhaltenskodizes zu beteiligen, ist als positives Verfahren zu bewerten. Die Unterstützung bei der Ausarbeitung von Verhaltenskodizes in Datenschutzfragen bzw. deren alleinige Ausarbeitung kommt nämlich nicht nur dem allgemeinen Schutz der Bürger zugute, sondern trägt auch zur Steigerung der Sichtbarkeit der nationalen Datenschutzbehörden in der Gesellschaft bei und sollte von diesen weiter proaktiv verfolgt werden. Insbesondere in Irland übertragen einzelstaatliche Rechtsvorschriften der nationalen Datenschutzbehörde die Befugnis zur Empfehlung und Ausarbeitung von Verhaltenskodizes, die nach ihrer Genehmigung durch die Legislative Rechtsverbindlichkeit erlangen.[111]

Die Zusammenarbeit und die regelmäßige Kommunikation nationaler Datenschutzbehörden mit anderen staatlichen Stellen könnten dazu beitragen, ein reibungsloseres Funktionieren des Datenschutzsystems insgesamt sicherstellen. In Deutschland werden beispielsweise umfangreiche Schulungsprogramme in Form einer Datenschutzakademie angeboten, die umfassende und systematische Schulungsprogramme für alle Bereiche der Verwaltung entwickelt hat.

Eine enge Zusammenarbeit und Kommunikation mit im Datenschutzbereich tätigen NRO bietet verschiedene Vorteile: Erstens können NRO die nationalen Datenschutzbehörden und die Zivilgesellschaft auf systematische und/oder eklatante Verstöße gegen Datenschutzgesetze aufmerksam machen. Somit stellen sie zusätzliche, informelle Kontrollstellen dar. Unter bestimmten Umständen tragen sie wirksam zu einer umfassenden Überwachung des Datenschutzes bei. Zweitens bieten NRO einen „Bottom-up"-Kommunikationskanal, der proaktiven Bürgern die Möglichkeit bietet, Änderungen des bestehenden Rechtsrahmens vorzuschlagen. Unter diesem Gesichtspunkt steht die nationale Datenschutzbehörde in Ungarn Berichten zufolge einer Unterstützung von NRO sowie der Zusammenarbeit mit diesen offen gegenüber. Beispielsweise prüfte sie im Jahr 2000 den Datenschutzplan des vom ungarischen Helsinki-Komitee durchgeführten Forschungsvorhabens zu den Rechten der Roma, und im Jahr 2004 prüften die Mitarbeiter der Datenschutzbehörde zusammen mit der ungarischen Bürgerrechtsunion (*Hungarian Civil Liberties Union*, HCLU) in mehreren öffentlichen Gesundheitseinrichtungen, ob die angekündigten anonymen und kostenlosen HIV-Tests tatsächlich angeboten wurden. Aufgrund der gewonnenen Erkenntnisse wurde eine Empfehlung formuliert.[112]

Schließlich sind auch die Zusammenarbeit und die kontinuierliche Kommunikation mit Datenschutzbehörden anderer Staaten (EU-Mitgliedstaaten und Drittstaaten) sinnvoll. Auf EU-Ebene wird dies vor allem durch die Datenschutzgruppe erreicht, die gemäß Artikel 29 der Datenschutzrichtlinie eingesetzt wurde. Dieses Forum bietet das nötige institutionelle Umfeld, in dem die Datenschutzbehörden die Anwendung ihrer jeweiligen Gesetze harmonisieren können. Auch die bilaterale oder multilaterale Zusammenarbeit auf der Basis regionaler oder sprachlicher Verbundenheit sollte gefördert werden – sowohl innerhalb der EU als auch mit Drittstaaten. Ein gutes Beispiel in diesem Zusammenhang ist Portugal, wo jährlich ein informelles Treffen mit der spanischen Datenschutzbehörde stattfindet, um die wichtigsten Entwicklungen im Bereich des Datenschutzes zu erörtern.

6.2. Einhaltung der Standards

Im Hinblick auf die Einhaltung der Standards resultieren vielversprechende Praktiken aus den erweiterten Kapazitäten der Datenschutzbehörden in Bezug auf die Aufdeckung von Verstößen und die Verfolgung derjenigen,

111 Irisches Datenschutzgesetz (1988-2003), Abschnitt 13.
112 http://beszelo.c3.hu/03/11/04zadori.htm; http://abiweb.obh.hu/dpc/index.php?menu=reports/2004/III/2&dok=reports/2004/27.

die die Verstöße begangen haben. Ein interessantes Merkmal der vielversprechenden Praktiken in Italien ist die Zusammenarbeit zwischen der nationalen Datenschutzbehörde und Polizeistellen im Rahmen einer gemeinsamen *Ad-hoc*-Absichtserklärung mit der Finanzwacht. Entsprechendes gilt für Rumänien, wo die nationale Datenschutzbehörde Kooperationsvereinbarungen mit öffentlichen Einrichtungen unterzeichnet hat (mit der einzelstaatlichen Behörde für Verbraucherschutz, der Generalinspektion der rumänischen Polizei, der Finanzwacht, dem Ministerium für Kommunikation und Informationstechnologie und dem nationalen Handelsregisteramt).

Eine interessante Facette des niederländischen Systems ist die Verpflichtung der Regierung, innerhalb von fünf Jahren nach Inkrafttreten des einzelstaatlichen Gesetzes dem niederländischen Parlament einen Bericht über die Wirksamkeit und die Auswirkungen des Gesetzes in der Praxis vorzulegen. Diese Evaluierung des niederländischen Gesetzes zum Schutz personenbezogener Daten wurde in zwei Phasen durchgeführt. Die erste Phase, eine Literaturstudie, wurde im Jahr 2007 abgeschlossen und in dem Bericht „Erste Phase der Evaluierung des Gesetzes zum Schutz personenbezogener Daten" („*Eerste fase evaluatie Wet bescherming persoonsgegevens*") vorgestellt.[113] Die zweite Phase der Evaluierung besteht aus Fallstudien und Befragungen zur Wirksamkeit des Gesetzes zum Schutz personenbezogener Daten in der Praxis. Der Bericht wurde im Februar 2009 veröffentlicht.[114]

6.3. Rechtsbewusstsein

Im vorstehenden Abschnitt 4.4 wurde der Aspekt des Rechtsbewusstseins in einem vergleichenden Überblick behandelt, und in Abschnitt 5.1.4 wurden Defizite hinsichtlich des Rechtsbewusstseins erörtert. Im Bereich der von nationalen Datenschutzbehörden durchgeführten Tätigkeiten zur Sensibilisierung für Datenschutzrechte hat sich ein breites Spektrum an vielversprechenden Praktiken herauskristallisiert. Zunächst haben viele einzelstaatliche Stellen nutzerfreundliche Websites aufgebaut, auf denen relevante Informationen zum Datenschutz zu finden sind. Häufig bieten diese Websites die Informationen in mehr als einer Sprache an. Eine zweite Gruppe vielversprechender Praktiken betrifft die von den Stellen durchgeführten Bildungsmaßnahmen zur Förderung der Kultur der Privatsphäre, die sich besonders – jedoch nicht ausschließlich – auf jüngere Generationen konzentrieren. Außerdem werden spezielle Kurse, Seminare und Vorträge veranstaltet, um die an Datenverarbeitungen beteiligten Akteure anzusprechen. Die Herausgabe von Leitlinien für diese Akteure stellt eine weitere wichtige, vielversprechende Praktik von Datenschutzbehörden dar. Und schließlich werden Preise zur Förderung der Einhaltung der Datenschutzbestimmungen verliehen.

Um ein möglichst wirksames Funktionieren der Gesetzgebung sicherzustellen und den Zugang zu wirksamen Rechtsbehelfen zu erleichtern, haben viele nationale Datenschutzbehörden umfassende Internetsites und Websites aufgebaut. Über diese können die in den Rechtsvorschriften vorgesehenen amtlichen Unterlagen eingereicht, Registrierungen vorgenommen, die Verarbeitung personenbezogener Daten gemeldet, Beratungsleistungen und/oder Informationen beantragt und empfangen und Beschwerden erhoben werden. In Deutschland betreibt beispielsweise das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein mit Unterstützung fast aller deutschsprachigen Datenschutzbehörden eine Website, auf der umfassende Informationen über die jüngsten Entwicklungen, Gerichtsverfahren, Berichte und Pressemitteilungen sowie eine Datenbank mit den wichtigsten Begriffen zu finden sind.[115] Insbesondere für Lehrkräfte und sonstige „Multiplikatoren" wurde ferner eine umfassende Homepage mit Informationen über Möglichkeiten des Selbstschutzes gegen datenschutzrechtliche Verstöße eingerichtet.[116] In Italien und in Spanien[117] ermöglicht ein Datenübermittlungssystem für Meldungen an die Datenschutzbehörde die Meldung von Dateien ebenfalls über das Internet.

In vielen Fällen ist die amtliche Website mehrsprachig, entweder wegen der Sprachenregelung des betreffenden Mitgliedstaats, die die Verwendung von mehr als einer Sprache vorsieht, oder weil eine englische Fassung eingerichtet wurde, um einem größeren Nutzerkreis den Zugang zu der Website zu erleichtern. Diese Möglichkeit sollte angesichts der Freizügigkeit der EU-Bürger in allen 27 Mitgliedstaaten unbedingt von den Datenschutzbehörden berücksichtigt werden. In Luxemburg beispielsweise ist das Material auf der mehrsprachigen Website der einzelstaatlichen Datenschutzbehörde sehr umfangreich und bietet eine Fülle von Informationen für betroffene Personen, für die Verarbeitung Verantwortliche, Auftragsverarbeiter und Gesetzgeber.[118] Auch in Finnland ist die Website der Datenschutzbehörde ein wichtiger Kanal für die Bereitstellung von Informationen in mehreren Sprachen.[119]

Die von manchen nationalen Datenschutzbehörden entwickelte Bildungspolitik ist ein innovatives, facettenreiches Element. Einerseits fördert das Angebot von Bildungsprogrammen auf allen Bildungsstufen, d. h. von der Grundschule bis zur Universität, die Sensibilisierung für Datenschutzfragen. Und andererseits können speziell angepasste Programme für unterschiedliche Altersgruppen der Gesellschaft hilfreiches Feedback zu den Eigenheiten und Bedürfnissen der verschiedenen gesellschaftlichen Gruppen liefern. Die Massenmedien bieten reichlich Raum für die Weiterentwicklung von Fernsehprogrammen, interaktiven Websites und anderen Initiativen zur Sensibilisierung der Öffentlichkeit. In der Tschechischen Republik führt die einzelstaatliche Datenschutzbehörde beispielsweise ein auf Kinder und Jugendliche ausgerichtetes Projekt sowie ein Bildungsprojekt mit dem Titel „Schutz personenbezogener Daten in der Bildung" durch. Die einzelstaatliche Datenschutzbehörde war 2006 auch an der Realisierung einer Fernsehserie über den Datenschutz mit dem Titel „Informationsbedarf ist kein Grund – Wir alle haben unsere Geheimnisse" beteiligt. (Laut Jahresbericht 2006 wurde jede Folge von etwa 160 000 – 310 000 Personen gesehen.)[120] Eine weitere vielversprechende Praktik im Bildungsbereich ist die Mitwirkung von Fachleuten der Datenschutzbehörde an Vorträgen und Seminaren für Mitglieder von Interessengruppen. Dies gilt beispielsweise für Finnland, wo die Datenschutzbehörde viermal jährlich ein Magazin herausgibt, das sich insbesondere an für die Verarbeitung Verantwortliche richtet. Überdies werden auch telefonische Beratungen angeboten. In Portugal und Belgien bietet die Datenschutzbehörde Praktika für Studierende und

113 G. Zwenne u. a. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, siehe: www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969, Zusammenfassung (auf Englisch) auf S. 207.

114 H.B. Winter u. a. (2008), *Wat niet weet wat niet deert*, WODC 2008, siehe: www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#.

115 www.datenschutz.de.

116 www.datenparty.de/.

117 https: //212.170.242.196/portalweb/canalresponsable/inscripcion_ficheros/Notificaciones_tele/que_es/index-ides- idphp.php.

118 www.cnpd.lu/fr.

119 www.tietosuoja.fi.

120 Siehe *Výroční zpráva za rok 2006* (Jahresbericht 2006), S. 2, unter www.uoou.cz/vz_2006.pdf.

Hochschulabsolventen in Rechtswissenschaften in diesem Bereich an, um diese mit ihrer Arbeit vertraut zu machen. In Italien wurden insbesondere auf Jugendliche ausgerichtete Kommunikationsinitiativen durchgeführt. (Unter anderem arbeitete die Datenschutzbehörde zusammen mit dem Bildungsministerium (*Ministero dell'Istruzione*) Leitlinien für die sachgerechte Nutzung von Handys und Videokameras während des Schulunterrichts aus.)

Die Bereitstellung von Orientierungshilfen und Beratung zu verschiedenen Datensystemprojekten ist ein wichtiger und ständig wachsender Aufgabenbereich. Die einzelstaatliche Datenschutzbehörde in Spanien hat Leitfäden zu zahlreichen Bereichen herausgegeben, die für Fragen des Datenschutzes von Bedeutung sind. Gegenstände der Leitfäden sind Empfehlungen zu den Rechten der Kinder und den Pflichten der Eltern;[121] Datensicherheitsmaßnahmen;[122] die Speicherung von Daten;[123] der Datenschutz als Grundrecht;[124] und die Handhabung personenbezogener Daten (Informationen für Stadträte,[125] staatliche Schulen und staatliche Universitäten, Berufsverbände, das öffentliche Gesundheitswesen und Sozialversicherungen). Entsprechendes gilt für Estland[126] und für Italien.[127] In Frankreich und im Vereinigten Königreich haben die Datenschutzbehörden Leitfäden zum Datenschutz bei Beschäftigungsverhältnissen herausgegeben.

Eine vielversprechende Praktik im Bereich der Sensibilisierung sind die von nationalen Datenschutzbehörden durchgeführten Informations- und Beratungskampagnen zur Bekämpfung von „Spam" oder unerwünschten E-Mails. In Frankreich beispielsweise hatte sich die Datenschutzbehörde zum Ziel gesetzt, die Beschwerden von Internet-Nutzern zu sammeln, zu bearbeiten und an die an der Kampagne gegen „Spam" beteiligten Akteure (an öffentliche und politische Stellen und Fachleute mit jeweils unterschiedlichen Aufträgen und Fähigkeiten) weiterzuleiten.[128] Auch in Spanien beteiligte sich die einzelstaatliche Kontrollstelle direkt an der Ausarbeitung von Informationsmaterial und Leitfäden[129] sowie an der Erarbeitung eines Katalogs mit Empfehlungen[130] zur Bekämpfung von „Spam".

Eine vielversprechende Praktik ist auch die Verleihung spezieller Preise durch die Datenschutzbehörden. In Slowenien wählt die einzelstaatliche Kontrollstelle jedes Jahr anlässlich des Europäischen Datenschutztages ein privates Unternehmen oder eine öffentliche Stelle aus, das bzw. die sich als besonders erfolgreich im Bereich des Schutzes personenbezogener Daten erwiesen hat. Diesem Unternehmen bzw. dieser Stelle wird ein „Preis für gute praktische Lösungen" verliehen, und es/sie wird als Vorbild in dem Bereich empfohlen.[131] In Frankreich hat die einzelstaatliche Kontrollstelle unter dem Motto *„Datenverarbeitung, Dateien und die Freiheiten des Einzelnen"* einen Promotionspreis mit einem Preisgeld von 7 000 EUR gestiftet. In diesem Zusammenhang wurde 2008 zudem ein Vorschlag zur Schaffung eines Nobelpreises im Bereich Datenschutz angenommen; der Preis soll 2010 zum ersten Mal verliehen werden[132] Ferner wurde in Spanien ein Preis für bewährte Datenschutzverfahren im öffentlichen Dienst in Europa eingerichtet.

121 www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf.

122 www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf .

123 https: //212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf .

124 https: //212.170.242.196/portalweb/canal_joven/common/pdfs/FOLLETO.pdf.

125 Siehe: www.madrid.org/cs/Satellite?c=CM_Publicacion_FA&cid=1114180060765&idPage=1109266885968&language=es&pagename=APDCM%2FCM_Publicacion_FA%2FfichaPublicacionAPDCM.

126 Siehe: www.aki.ee/est/?part=html&id=56.

127 Zu den wichtigsten Leitlinien gehören: die praktischen Leitlinien für KMU, zum Arbeitgeber/Arbeitnehmer-Verhältnis im privaten und öffentlichen Sektor, zu Kundenbeziehungen im Bankensektor, zur Veröffentlichung und Verbreitung von Dokumenten durch Kommunalbehörden, zur Datenverarbeitung im Rahmen klinischer Arzneimitteltests, zu Kundenkarten.

128 Siehe das am 30.10.2007 zwischen der französischen Datenschutzbehörde und der Vereinigung Signal Spam unterzeichnete Partnerschaftsabkommen.

129 www.agpd.es/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N- SPAM--ap-V.-30-mayo-cp-.pdf.

130 https: //212.170.242.196/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf.

131 www.lek.si/slo/mediji/sporocila-za-javnost/3849/ und www.ip-rs.si/novice/detajl/nagrajenca-ob-2-evropskem-dnevu-varstva-osebnih-podatkov-sta-zavod-za-zdravstveno-zavarovanje-slove/.

132 Erklärung der „International Privacy Association" (IPA) zur Schaffung eines Nobelpreises im Bereich Datenschutz und Freiheiten, der jährlich von der internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre verliehen werden soll www.privacyconference2008.org/index.php?langue=2&page_id=1.

7 Schlussfolgerungen

Sowohl auf EU-Ebene als auch auf nationaler Ebene können verschiedene Schritte unternommen werden, um einigen der größten Herausforderungen zu begegnen, denen sich das gegenwärtige Datenschutzsystem stellen muss. Wenngleich sicher auch nationale Maßnahmen eingeführt werden könnten, dürfte ein abgestimmter und harmonisierter Ansatz auf EU-Ebene doch wirksamer zur Stärkung des Schutzes personenbezogener Daten beitragen.

Den EU-Institutionen kommt in diesem Zusammenhang besondere Bedeutung zu, und das Europäische Parlament beschäftigt sich ebenfalls intensiv mit Fragen des Datenschutzes.[133] Das Europäische Parlament ist gemeinsam mit dem Rat der EU und mit der Europäischen Kommission aufgerufen, durch entsprechende Rechtsreformen die Wirksamkeit des Datenschutzsystems zu gewährleisten. In diesem Zusammenhang ist zu begrüßen, dass das für Justiz, Grundrechte und Bürgerschaft zuständige Mitglied der Kommission die Bedeutung des Datenschutzes betont und seine Absicht bekräftigt hat, aus den Datenschutzsystemen der EU ein modernes und umfassendes Rechtsinstrument zu entwickeln.[134] Der EuGH verfolgt einen proaktiven Ansatz hinsichtlich des Datenschutzes. Bislang hat der EuGH den Datenschutz als Instrument der Harmonisierung des Binnenmarkts betrachtet (Datenschutzrichtlinie); dieses Instrument sollte den Schutz eines Grundrechts innerhalb der Gemeinschaft unterstützen. In diesem Zusammenhang hat der EuGH umfassend zum Schutzumfang der Datenschutzrichtlinie Stellung genommen; die Auslegung des EuGH geht über die Beschränkung auf wirtschaftliche Aktivitäten hinaus und sieht eine restriktivere Auslegung der vom gewährten Schutz auszunehmenden Bereiche vor.

Verbesserungen der bestehenden Datenschutzvorschriften können auch in Zusammenarbeit der nationalen Datenschutzbehörden mit der Artikel-29-Datenschutzgruppe erzielt werden. Insbesondere die Gutachten und Empfehlungen der Datenschutzgruppe – soweit sie von den nationalen Datenschutzbehörden berücksichtigt werden – tragen zur Entwicklung eines gemeinsamen EU-Standards für einen weit reichenden Schutz personenbezogener Daten bei. Der Europäische Datenschutzbeauftragte ist ebenfalls beauftragt, die Einhaltung der Grundrechte und -freiheiten natürlicher Personen (insbesondere des Rechts auf den Schutz der Privatsphäre) durch die Gemeinschaftsorgane und -einrichtungen sicherzustellen. Die Konsultationsfunktion des Europäischen Datenschutzbeauftragten ist insoweit von besonderer Bedeutung, als sie wirksam zum Schutz der Grundfreiheiten der Unionsbürger bei der Verabschiedung neuer Rechtsvorschriften beiträgt.

Verbesserungen sind ferner im Hinblick auf die Unabhängigkeit, die Wirksamkeit, die Ressourcen und die Befugnisse von Datenschutzbehörden erforderlich. Sie spielen im Bewusstsein der Öffentlichkeit eine entscheidende Rolle als Hüter des Datenschutzes. Das gesamte Datenschutzsystem hängt vom Vertrauen der Öffentlichkeit in diese Behörden ab. Die Bürger werden sich schwerlich davon überzeugen lassen, dass ihre Vorbehalte hinsichtlich des Datenschutzes und der Achtung ihrer Privatsphäre ernst genommen werden, wenn anhaltende Zweifel an der Unabhängigkeit von Datenschutzbehörden bestehen oder wenn der Eindruck besteht, dass diese Behörden nicht so ausgestattet sind, dass sie ihren Pflichten in wirksamer und effizienter Weise nachkommen können.

Die Datenschutzbehörden sind ebenfalls ein wichtiges Element der EU-Grundrechte-Architektur; der EU kommt nämlich eine Vorreiterrolle bei der Behandlung des Datenschutzes als Grundrecht zu, und die EU hat in vielen Mitgliedstaaten entscheidend zur Entwicklung von Datenschutzsystemen beigetragen. Der Datenschutz ist auch eines der entscheidenden Politikfelder im Bereich der Grundrechte, in denen die EU die Zuständigkeit zur Erlassung von Rechtsvorschriften besitzt. Daher könnte ein wirksames Datenschutzsystem insgesamt positive Auswirkungen auch auf die öffentliche Wahrnehmung der EU als Hüterin der Grundrechte haben.

133 Siehe beispielsweise Vorschlag des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres für eine Empfehlung des Europäischen Parlaments an den Rat zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (2008/2160(INI)).

134 Siehe Mitteilung an die Mitglieder des Europäischen Parlaments vom 7.1.2010, Dokument PE431.139v02-00, www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_de.pdf.

In jedem dieser vier Berichte der Agentur der Europäischen Union für Grundrechte (FRA) werden eng miteinander verbundene Themen, Einrichtungen und EU-Gesetze betrachtet, die zur allumfassenden Grundrechte-Architektur in der Europäischen Union beitragen. Die Bausteine dieser Grundrechte-Architektur sind die Datenschutzbehörden und nationalen Einrichtungen zur Förderung und zum Schutz der Menschenrechte sowie die im Rahmen der „Richtlinie zur Rassengleichbehandlung“ (2000/43/EG) eingerichteten Gleichbehandlungsstellen.

Agentur der Europäischen Union für Grundrechte

Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2012

2012 – 52 S. – 21 x 29,7 cm

ISBN 978-92-9192-508-7
doi:10.2811/47194

Zahlreiche weitere Informationen zur Agentur der Europäischen Union für Grundrechte stehen auf der Webseite der FRA (fra.europa.eu) zur Verfügung.

TK-31-09-265-DE-C

doi:10.2811/47194

FRA – Agentur der Europäischen Union für Grundrechte
Schwarzenbergplatz 11
1040 Wien
Österreich
Tel.: +43 (0) 1 580 30 - 0
Fax: +43 (0) 1 580 30 - 699
E-Mail: information@fra.europa.eu
fra.europa.eu

Amt für Veröffentlichungen

ISBN 978-92-9192-508-7