(ZUKÜNFTIGES) ZUSAMMENWIRKEN ZWISCHEN DATENSCHUTZ-BEHÖRDEN UND NATIONALEN MENSCHENRECHTSINSTITUTIONEN[*]

von Peter J. Hustinx[**]

1. EINFÜHRUNG

In Übereinstimmung mit der Richtlinie 95/46/EG verfügen alle EU-Mitgliedstaaten über nationale Behörden, die die Einhaltung der Datenschutzgesetze überwachen. Allerdings wurde die Richtlinie sehr unterschiedlich in nationales Recht umgesetzt, was zu Diskrepanzen und Mängeln geführt hat, auf die von der Agentur der Europäischen Union für Grundrechte und auch in der jüngeren Rechtsprechung des Europäischen Gerichtshofs hingewiesen wurde. Im Januar 2012 legte die Europäische Kommission ein Paket mit Vorschlägen zur Aktualisierung und Stärkung des gegenwärtigen Rechtsrahmens für den Datenschutz vor. Diese Überarbeitung wird sich auch auf den Umfang eines sinnvollen Zusammenwirkens zwischen Datenschutzbehörden und nationalen Menschenrechtsinstitutionen auswirken.

Das Aufkommen des Rechts auf den Schutz personenbezogener Daten („Datenschutz“) als eigenständiges Grundrecht – eng verbunden mit dem Recht auf die Achtung des Privatlebens, aber mit seinen eigenen speziellen Eigenschaften – ist ein typisches Merkmal der Menschenrechtslandschaft in Europa. Während sich ähnliche Gesetzgebungen in anderen Regionen der Welt auf der Grundlage von Theorien zu Privatsphäre, angemessener Informationsverarbeitung und Verbraucherschutz oder einfach auf der Grundlage der Notwendigkeit der Schaffung adäquater Bedingungen für wirtschaftliches Wachstum entwickelt haben, wurden die Entwicklungen in Europa durch die frühe Überzeugung geprägt, dass sich das Wachstum der Informationsgesellschaft auf die Ausübung bestehender Grundrechte und Grundfreiheiten der Bürger in einer Größenordnung auswirken würde, die einen proaktiveren und systematischeren Ansatz erforderlich machte.

Die ersten Schritte wurden im Europarat ergriffen und führten 1981 zur Verabschiedung eines Übereinkommens zum Datenschutz mit Grundsätzen für die Verarbeitung personenbezogener Daten in automatisierter Form oder anderweitig strukturierten Datendateien, auch bekannt als Übereinkommen 108[1]. Der Begriff „Datenschutz“ wurde definiert als der Schutz der Rechte und Grundfreiheiten natürlicher Personen, *insbesondere* ihres Rechts auf einen Persönlichkeitsbereich, bei der Verarbeitung personenbezogener Daten.[2] Das Übereinkommen geht somit über den Anwendungsbereich von Artikel 8 der Europäischen Menschenrechtskonvention (EMRK)[3] hinaus und gilt im Prinzip unabhängig davon, ob das Recht auf

---

[*] Veröffentlicht in: „National Human Rights Institutions in Europe - Comparative, European and International Pesrpectives“, Jan Wouters und Katrien Meuwissen (Hrsg.), Cambridge 2013, S. 157-172.

[**] Peter Hustinx ist Europäischer Datenschutzbeauftragter (EDSB). Kontakt: edps@edps.europa.eu Website: www.edps.europa.eu.

[1] Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, 28.1.1981 (im weiteren Text: Übereinkommen 108).

[2] Übereinkommen 108, Artikel 1.

[3] Artikel 8 „Recht auf Achtung des Privat- und Familienlebens“:

1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

Persönlichkeitsbereich auf dem Spiel steht, für alle personenbezogenen Daten. Die Grundsätze des Überkommens 108 sehen wesentliche Anforderungen an den für die Verarbeitung Verantwortlichen, einige spezifische Rechte für betroffene Personen und Vorkehrungen für die institutionelle Aufsicht, die Durchsetzung und die internationale Zusammenarbeit vor. Das Übereinkommen wurde von mehr als 40 Mitgliedstaaten, darunter alle Mitgliedstaaten der EU, ratifiziert.

Bei der Umsetzung des Übereinkommens 108 in nationales Recht wurde rasch klar, dass der allgemeine Wortlaut seiner Bestimmungen sehr unterschiedliche nationale Datenschutzgesetze ermöglichte. Gleichzeitig erforderte die Entwicklung der Informationsgesellschaft mehr Harmonisierung und Kohärenz unter den nationalen Regelwerken, als dies durch das Übereinkommen möglich war. Dies veranlasste die EU zum Eingreifen und führte schließlich zur Verabschiedung der Datenschutzrichtlinie 95/46/EG, die zwar das Übereinkommen als Ausgangsbasis nahm, es aber auch in verschiedener Weise spezifizierte, u. a. durch die Forderung nach Kontrolle und Durchsetzung durch eine oder mehrere vollkommen unabhängig handelnde Datenschutzbehörden.[4]

Der nächste Entwicklungsschritt war die Verabschiedung der EU-Charta der Grundrechte im Jahr 2000[5], ursprünglich als politisches Dokument. Obwohl sie weitgehend auf der EMRK gründete, enthielt sie auch einige Neuerungen, darunter zusätzlich zum Recht auf Achtung des Privat- und Familienlebens (Artikel 7) die Anerkennung eines Rechts auf den Schutz personenbezogener Daten (Artikel 8). Artikel 8 erwähnt ausdrücklich einige der Hauptelemente des Rechts auf den Schutz personenbezogener Daten, die in der Richtlinie 95/46/EG weiter ausgearbeitet wurden:

> **Schutz personenbezogener Daten**
> 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 und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten 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.

Letzter Schritt war das Inkrafttreten des Vertrags von Lissabon Ende 2009,[6] durch den die Charta zu einem rechtsverbindlichen Dokument wurde,[7] und der auch eine horizontale Rechtsgrundlage für die Datenschutzgesetzgebung einführte, die nun nicht mehr von den Notwendigkeiten des Binnenmarkts abhängt, sondern die Natur des

---

2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31. Vgl. insbesondere Artikel 28.

[5] Charta der Grundrechte der Europäischen Union (2000/C 364/01), ABl. L 364 vom 18.12.2000, S. 1 (im Folgenden „die Charta“).

[6] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft (2007/C 306/01), ABl. L 306 vom 17.12.2007, S. 1.

[7] Konsolidierte Fassung des Vertrags über die Europäische Union, ABl. C 115 vom 9. Mai 2008, S. 19 (im Folgenden „EUV“). Vgl. Artikel 6.

Datenschutzes als Grundrecht unter den allgemeinen Grundsätzen der Union widerspiegelt.[8] Damit wurde eine Entwicklung des Rechts über mehrere Jahrzehnte hinweg bestätigt.

2. UNABHÄNGIGE KONTROLLE

Die Existenz von Datenschutzbehörden war von Beginn an ein Standardmerkmal des Europäischen Datenschutzrechts, aber es dauerte eine gewisse Zeit, bis sich der Grundsatz der *unabhängigen* Kontrolle zu einem Verfassungsgrundsatz entwickelte. Artikel 8 der Charta sieht diese nun vor, und auch Artikel 16 AEUV tut dies, wie wir gerade gesehen haben, in sehr ähnlichen Worten. Artikel 28 der Richtlinie 95/46/EG geht, wie wir sehen werden,[9] detaillierter auf das Thema ein.

Rückblickend stellt man überrascht fest, dass trotz der Erfahrungen in Deutschland, Schweden und Frankreich das Konzept einer „Datenschutzbehörde" im Übereinkommen 108 bei dessen Abschluss im Jahr 1981 nur eine sehr begrenzte Rolle spielte. Oberste Pflicht jeder Vertragspartei war es gemäß Artikel 4 des Übereinkommens, „in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen zu treffen, um die Grundsätze für den Datenschutz zu verwirklichen", die in diesem Übereinkommen aufgestellt sind. Artikel 10 bestimmt, dass jede Vertragspartei „geeignete Sanktionen und Rechtsmittel" für Verletzungen dieser Grundsätze festzulegen hat. Im erläuternden Bericht wurde deutlich die Notwendigkeit unterstrichen, einen „*wirksamen Schutz"* zu gewährleisten, doch wurde die Entscheidung über die Art der praktischen Umsetzung den Vertragsparteien überlassen.[10] Die Existenz von Kontrollstellen wird nur in Zusammenhang mit nationalen Rechtsvorschriften erwähnt. Die Verfasser des Übereinkommens zögerten offensichtlich, hieraus für alle Vertragsparteien ein grundlegendes rechtliches Erfordernis zu machen.

Diese Situation änderte sich mit der Verabschiedung der EU-Datenschutzrichtlinie 95/46/EG. Artikel 28 der Richtlinie führte die Verpflichtung für alle Mitgliedstaaten ein, eine oder mehrere Kontrollstellen einzurichten, die die Anwendung der Vorschriften überwachen und ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen. Gemäß Erwägungsgrund 62 ist „die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen, ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten". Die Formulierung „*nimmt ihre Aufgaben* in völliger Unabhängigkeit *wahr*" war ein Kompromiss, mit dem ein gewisser Spielraum geschaffen werden sollte, doch kann man sich „völlige Unabhängigkeit" kaum ohne ausreichende institutionelle Garantien vorstellen. Dieses Element war in einem Verfahren gegen Deutschland vor dem EuGH, auf das wir später noch zurückkommen, von allergrößter Bedeutung.[11]

Artikel 28 der Richtlinie bestimmt ferner, dass die Kontrollstellen bestimmte Befugnisse haben müssen, wie Beratungsbefugnisse, Untersuchungsbefugnisse,

[8] Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union, ABl. C 115 vom 9.5.2008, S. 47 (im folgenden „AEUV"). Vgl. Artikel 16.
[9] Siehe nachstehenden Punkt 2.
[10] Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, Erläuternder Bericht, Punkt 60.
[11] Siehe nachstehenden Punkt 4.

wirksame Einwirkungsbefugnisse, das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die Vorschriften, die Befugnis, Eingaben entgegenzunehmen usw. Damit scheint ihnen eine zentrale Stellung zuzukommen. Allerdings treffen sie nicht die letzte Entscheidung, und gegen ihre Entscheidungen steht der Rechtsweg offen.

Nach Verabschiedung der Richtlinie wurde ein Zusatzprotokoll zum Übereinkommen 108 abgefasst, das im Wesentlichen alle Elemente von Artikel 28 der Richtlinie enthält.[12] In der Präambel dieses Zusatzprotokolls heißt es eindeutig, dass „Kontrollstellen, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen, zu einem wirksamen Schutz des Menschen bei der Verarbeitung personenbezogener Daten beitragen". Im erläuternden Bericht heißt es sogar, dass Datenschutzkontrollstellen „ein wesentlicher Bestandteil des Datenschutzkontrollsystems in einer demokratischen Gesellschaft geworden sind".[13] Dieser Bericht misst dem Begriff des „wirksamen Schutzes" und der Rolle der Kontrollstellen bei seiner Gewährleistung großes Gewicht bei.[14]

All das bedeutet gemäß Artikel 8 der Charta und Artikel 16 AEUV, dass sich der Grundsatz der „unabhängigen Kontrolle" und die Existenz „unabhängiger Kontrollstellen" zumindest auf europäischer Ebene zu festen Bestandteilen des Rechts auf Datenschutz in einer demokratischen Gesellschaft entwickelt haben. Dies gründet auf ihrer Aufgabe der „Überwachung der Einhaltung der Vorschriften" und ist eng mit dem Begriff des „wirksamen Schutzes" verknüpft.

3. VIELFALT UND MÄNGEL

Im Einklang mit der Richtlinie 95/46/EG verfügen alle EU-Mitgliedstaaten über nationale Behörden, die die Einhaltung der Datenschutzgesetze überwachen. Doch die Umsetzung der Richtlinie in nationales Recht fällt sehr unterschiedlich aus. Dies hat zu Diskrepanzen und Mängeln geführt, die in einem im Mai 2010 veröffentlichten Bericht der Agentur der Europäischen Union für Grundrechte (FRA) hervorgehoben wurden.[15]

Als erstes sollte beachtet werden, dass eine gewisse Vielfalt unvermeidbar ist und einfach aus unterschiedlichen Rechtstraditionen in den Mitgliedstaaten resultiert. Die Richtlinie lässt den Mitgliedstaaten einen großen Spielraum für die Entscheidung über Art und Struktur der für sie am besten geeigneten Kontrollstelle. Daher gibt es unterschiedliche Formen und Arten von Datenschutzbehörden: große oder kleine Ausschüsse, einzelne Beauftragte, entweder von nationalen Regierungen oder Parlamenten oder anderen gewählt oder ernannt, usw.

Doch wie die FRA in ihrem Bericht klar betont, geht die derzeitige Vielfalt zwischen den Mitgliedstaaten weit über das Unvermeidliche hinaus und führt auch zu

[12] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (ETS Nr. 181), Straßburg, 8. November 2001 (Inkrafttreten: 1. Juli 2004).
[13] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, ETS Nr. 181, Erläuternder Bericht, Präambel, Absatz 5.
[14] a.a.O., Präambel, Absatz 8, Absatz 13, Absatz 16, Absatz 17, Absatz 24.
[15] Vgl.: FRA, Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden – Stärkung der Grundrechte-Architektur in der EU Teil II, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, 2012.

schwerwiegenden Mängeln.[16] Die wichtigsten Ergebnisse des Berichts wurden von der FRA wie folgt zusammengefasst.[17]

> **Bewusstsein für die eigenen Rechte**
> Sieben von zehn Befragten in einer vor kurzem durchgeführten Eurobarometer-Umfrage wussten nicht, dass es in ihrem Land eine Datenschutzbehörde gibt.
> **Begrenzte Befugnisse**
> Datenschutzbehörden sind häufig nicht mit umfassenden Untersuchungs- oder Interventionsbefugnissen oder der Befugnis zur Rechtsberatung oder zur Teilnahme an Rechtsstreitigkeiten ausgestattet.
> **Mangelnde Einhaltung**
> In vielen Mitgliedstaaten besteht eine weit verbreitete Missachtung der grundlegenden Pflicht, vor der Verarbeitung von Daten eine Registrierung bei der Datenschutzbehörde vornehmen zu lassen.
> **Mangelnde Unabhängigkeit**
> Bei einigen Datenschutzbehörden in der EU stellt die mangelnde Unabhängigkeit von der Regierung ein großes Problem für ihre Glaubwürdigkeit dar. Eine Reform des Berufungs-/Ernennungsverfahrens (…) könnte das Problem der mangelnden Unabhängigkeit lösen.
> **Mangel an Finanzmitteln und Mitarbeitern**
> Datenschutzbehörden in [einer Reihe von Mitgliedstaaten] sind nicht in der Lage, alle ihre Aufgaben zu erfüllen, da ihnen nur begrenzte Finanzmittel und Humanressourcen zur Verfügung stehen.
> **Mangel an Sanktionen und Schadenersatz**
> Es ist eine Gesetzesreform notwendig, damit die Datenschutzbehörden eine aktive Rolle in Verfahren spielen können, die zu Sanktionen und Wiedergutmachung führen. Wenn Datenschutzbehörden über die einschlägigen Befugnisse verfügen, benötigen sie die Ressourcen, um diese effizient zu nutzen. (...)

Der FRA-Bericht erwähnt auch einige Beispiele vielversprechender Praktiken,[18] aber die im Bericht aufgezeigten Unterschiede und Mängel bleiben eher besorgniserregend.

4. ERFORDERNIS DER „VÖLLIGEN UNABHÄNGIGKEIT“

Auch der Europäische Gerichtshof hat sich in der Zwischenzeit zum Erfordernis der „völligen Unabhängigkeit“ in Artikel 28 der Richtlinie 95/46/EG geäußert.

Im Urteil des EuGH in der Rechtssache C-518/07 *(Europäische Kommission gegen Bundesrepublik Deutschland)* ging es um Behörden in Deutschland, die die Verarbeitung personenbezogener Daten durch *nicht-öffentliche Stellen* auf regionaler Ebene in den Bundesländern überwachen. In allen Bundesländern waren diese Behörden staatlicher Aufsicht unterworfen. Die Europäische Kommission mit dem Europäischen Datenschutzbeauftragten (EDSB) als Streithelfer vertrat vor Gericht die Auffassung, „völlige Unabhängigkeit“ in Artikel 28 der Richtlinie 95/46/EG bedeute, dass eine Kontrollstelle frei von *jeglicher* äußerer Einflussnahme sein muss, gleichgültig von welcher Seite.[19] Die Bundesrepublik Deutschland war der Ansicht, es

[16] a.a.O., S. 42-45.
[17] Siehe Website der FRA: http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities.
[18] FRA, a.a.O., Fußnote 15, S. 47-48.
[19] Europäischer Gerichtshof, Urteil, Rechtssache C-518/07 *Europäische Kommission gegen Bundesrepublik Deutschland*, 9. März 2010, Randnr. 15.

sei lediglich eine *funktionale* Unabhängigkeit (der Kontrollierten) gefordert, schloss jedoch staatliche Aufsicht nicht aus.[20]

Der EuGH entschied zu Gunsten der Kommission, im Wesentlichen mit dem Hinweis, „völlige Unabhängigkeit" sei eben „völlige Unabhängigkeit". Seine Würdigung enthält jedoch einige interessante Botschaften. Der Gerichtshof geht davon aus, dass sich die Bedeutung des Erfordernisses aus dem Wortlaut von Artikel 28 sowie den Zielen und der Systematik der Richtlinie ergeben muss.

Zum *Wortlaut* von Artikel 28 führt der Gerichtshof aus, in Bezug auf öffentliche Stellen bezeichne der Begriff „Unabhängigkeit" in der Regel eine „Stellung, in der gewährleistet ist, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann".[21] Darüber hinaus impliziere laut dem Gericht der Zusatz „*völlige* Unabhängigkeit" eine „Entscheidungsgewalt, die jeder Einflussnahme von außerhalb der Kontrollstelle, sei sie unmittelbar oder mittelbar, entzogen ist".[22]

Im Hinblick auf die *Ziele* der Richtlinie 95/46/EG vertritt der Gerichtshof die Auffassung, sie hebe auf die Harmonisierung nationalen Rechts in einem Bereich ab, in dem der freie Verkehr personenbezogener Daten das Recht auf Privatsphäre beeinträchtigen könne und verfolge das Ziel, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten zu gewährleisten. Die in Artikel 28 vorgesehenen Kontrollstellen seien die „Hüter dieser Grundrechte und Grundfreiheiten", und ihre Einrichtung habe als ein „wesentliches Element" des Schutzes der Personen bei der Verarbeitung personenbezogener Daten zu gelten.[23] Der Gerichtshof fährt fort (Unterstreichungen von uns):

> „24. Um diesen Schutz zu gewährleisten, müssen die Kontrollstellen zum einen die Achtung des Grundrechts auf Privatsphäre und zum anderen die Interessen, die den freien Verkehr personenbezogener Daten verlangen, miteinander ins Gleichgewicht bringen. Im Übrigen sind die verschiedenen nationalen Kontrollstellen nach Artikel 28 Absatz 6 der Richtlinie 95/46 zu gegenseitiger Zusammenarbeit aufgerufen und können gegebenenfalls von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.
>
> 25. Die Gewährleistung der Unabhängigkeit der nationalen Kontrollstellen soll die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen und ist im Licht dieses Zwecks auszulegen. Sie wurde eingeführt, um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen selbst oder ihren Bevollmächtigten eine besondere Stellung zu verleihen. Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen."

[20] a.a.O., Randnr. 16.
[21] a.a.O., Randnr. 18.
[22] a.a.O., Randnr. 19.
[23] a.a.O., Randnr. 23.

Hinsichtlich der *Systematik* der Richtlinie zieht der Gerichtshof eine Parallele zwischen der Richtlinie 95/46/EG auf der einen Seite und der Verordnung (EG) Nr. 45/2001[24], die auf EU-Organe Anwendung findet und durch die der EDSB eingesetzt wurde, auf der anderen Seite. Artikel 28 der Richtlinie sei gemäß Artikel 44 der Verordnung auszulegen, der „völlige Unabhängigkeit" fordert, aber auch bestimmt, dass der EDSB „niemanden um Weisung ersucht und auch keine Weisungen entgegennimmt".[25] Nach Auffassung des Gerichtshofes ist Artikel 28 dahin auszulegen,

> „30. […] dass die für die Überwachung der Verarbeitung personenbezogener Daten […] zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen."

Der Gerichtshof geht dann der Frage nach, ob staatliche Aufsicht dem vorstehend definierten Erfordernis der Unabhängigkeit gerecht wird, und kommt zu dem Schluss, dass dem *nicht* so ist. Hierzu führt er aus,

> „36. […] dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen."

Nach weiterer Analyse kam der Gerichtshof zu dem Schluss, die Bundesrepublik Deutschland habe die für die Überwachung der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen verantwortlichen Behörden in den Bundesländern staatlicher Kontrolle unterworfen und sei damit ihren Verpflichtungen aus Artikel 28 der Richtlinie 95/46/EG nicht nachgekommen.

Somit entschied der Gerichtshof nicht nur, dass „völlige Unabhängigkeit" auch Freiheit von *jeglichem* äußeren Einfluss bedeutet, sondern sandte auch interessante Signale bezüglich der Rolle von Aufsichtsbehörden aus: Ihre Unabhängigkeit soll die *Wirksamkeit* ihrer Aufgabe sicherstellen, und sie sollten *objektiv* und *unparteiisch* handeln und ein *Gleichgewicht* zwischen der Wahrung des Grundrechts auf Privatleben und anderen Interessen schaffen können.

---

[24] 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.

[25] a.a.O., Artikel 44, „Unabhängigkeit":

1. Der Europäische Datenschutzbeauftragte übt sein Amt in völliger Unabhängigkeit aus.
2. Der Europäische Datenschutzbeauftragte ersucht in Ausübung seines Amtes niemanden um Weisung und nimmt keine Weisungen entgegen.
3. Der Europäische Datenschutzbeauftragte sieht von allen mit seinem Amt nicht zu vereinbarenden Handlungen ab und übt während seiner Amtszeit keine andere entgeltliche oder unentgeltliche Tätigkeit aus.
4. Der Europäische Datenschutzbeauftragte ist verpflichtet, nach Ablauf seiner Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen ehrenhaft und zurückhaltend zu handeln.

Wir werden auf die Frage zurückkommen, was all dies für das Zusammenwirken zwischen Datenschutzbehörden und nationalen Menschenrechtsinstitutionen bedeuten könnte.[26] Zunächst ist es jedoch sinnvoll, sich mit den Grundzügen der derzeitigen Überprüfung des EU-Datenschutzregelwerks vertraut zu machen.

5. VORSCHLÄGE FÜR EIN NEUES EU-DATENSCHUTZREGELWERK

5.1. Treibende Kräfte für die Überprüfung

Warum findet diese Überprüfung überhaupt statt? Hierfür gibt es im Wesentlichen drei Gründe. Der *erste* ist, dass das aktuelle Regelwerk – genauer gesagt sein Kernbestandteil, die Richtlinie 95/46/EG – auf den neuesten Stand gebracht werden muss. „Auf den neuesten Stand bringen" bedeutet in diesem Fall in erster Linie, dafür zu sorgen, dass sie in der Praxis weiterhin wirksam bleibt. Als die Richtlinie angenommen wurde, steckte das Internet noch in den Kinderschuhen; heutzutage leben wir in einer Welt, in der die kontinuierliche Datenverarbeitung zunehmend relevant wird. Folglich brauchen wir auch stärkere Schutzmaßnahmen, die in der Praxis gute Resultate liefern. Die Herausforderungen durch die neuen Technologien und die Globalisierung erfordern fantasievolle Innovationen, um einen wirksameren Schutz zu gewährleisten.

Der *zweite* Grund ist, dass das aktuelle Regelwerk zu einer wachsenden Vielfalt und Komplexität geführt hat, und zwar auch in weiterem Sinn, allein aufgrund der Tatsache, dass es sich um eine Richtlinie handelt, die in nationales Recht umgesetzt werden muss – so ist es nun einmal bei Richtlinien – und wir nun 27 Fassungen der gleichen Grundprinzipien haben. Das ist schlicht und einfach zu viel und führt zu zusätzlichen Kosten, aber auch zu einem Verlust an Wirksamkeit. Mit anderen Worten: Wir brauchen mehr Harmonisierung und müssen das System nicht nur stärken und in der Praxis wirksamer machen, sondern auch kohärenter. Dies wird zu einem Abbau *nicht hilfreicher* Vielfalt und Komplexität führen.

Der *dritte* Grund hat mit dem neuen Rechtsrahmen der EU zu tun. Im Vertrag von Lissabon haben die Grundrechte großes Gewicht. Wie wir gesehen haben, gibt es jetzt unter anderem eine spezielle Datenschutzbestimmung in Artikel 8 der Charta der Grundrechte und eine neue horizontale Rechtsgrundlage in Artikel 16 AEUV für einen umfassenden Schutz in allen Politikbereichen der EU, unabhängig davon, ob es um den Binnenmarkt, um Strafverfolgung oder irgendeinen anderen Bereich im öffentlichen Sektor geht.

Bei der Überarbeitung des Regelwerks geht es also um einen stärkeren, wirksameren, kohärenteren und umfassenderen Schutz personenbezogener Daten.

Wenn wir uns nun anschauen, was auf dem Tisch liegt, sehen wir ein Paket aus mindestens zwei Hauptvorschlägen: einer Richtlinie für – kurz gesagt – den Strafverfolgungsbereich[27] und einer unmittelbar anwendbaren Verordnung als Ersatz für die derzeitige Richtlinie 95/46/EG, die für die Privatwirtschaft und den öffentlichen

[26] Vgl. nachstehenden Punkt 6.

[27] Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, COM(2012) 10 final, Brüssel, 25. Januar 2012.

Sektor mit Ausnahme der Strafverfolgung gilt.[28] Die vorgeschlagene Richtlinie wird im Allgemeinen als nicht zufriedenstellend angesehen, da ihr Schutzniveau deutlich unter dem der vorgeschlagenen Verordnung liegt. Allerdings ist sie im vorliegenden Kontext auch weniger relevant.

5.2. Kontinuität und Wandel

Wenn wir uns nun näher mit der vorgeschlagenen Verordnung[29] befassen, sind ein paar wichtige Faktoren zu beachten.

Erstens: Trotz aller Neuerungen herrscht weitgehend Kontinuität. Alle Grundkonzepte und Grundsätze, die wir derzeit haben, werden auch weiterhin Bestand haben, wenn auch teilweise klargestellt und weiterentwickelt.[30] Bei den tatsächlichen Neuerungen geht es in der Hauptsache darum, „den Datenschutz in der Praxis wirksamer zu gestalten". Wie wir noch sehen werden, beinhaltet dies eine starke Betonung der Umsetzung von Grundsätzen und der Durchsetzung von Rechten und Pflichten, um sicherzustellen, dass es den Schutz in der Praxis auch gibt.

Die Verordnung strebt aber auch Vereinfachung und Kostensenkung an. Die Vorabmeldung von Datenverarbeitungen bei der Datenschutzbehörde wurde abgeschafft. Sie wird nur noch in Situationen verlangt, die besondere Risiken beinhalten.[31] Ferner sieht die Verordnung eine zentrale Anlaufstelle für Unternehmen mit Niederlassungen in verschiedenen Mitgliedstaaten vor.[32] Dies bringt die Einführung einer „federführenden Datenschutzbehörde" mit sich, bei der es sich um die Datenschutzbehörde im Land der Hauptniederlassung handelt, die in enger Zusammenarbeit mit anderen zuständigen Datenschutzbehörden zunächst zuständig ist.[33]

Eine unmittelbar verbindliche Verordnung bedeutet natürlich auch viel stärkere Harmonisierung – im Prinzip ein einziger, in allen Mitgliedstaaten geltender Rechtsakt – und mehr Kohärenz. Auch dies hat für in mehreren Mitgliedstaaten tätige Unternehmen erhebliche Vereinfachungen und Kostensenkungen zur Folge.

Schließlich hat die vorgeschlagene Verordnung einen allgemeinen Anwendungsbereich, denn sie findet sowohl auf den privaten als auch auf den öffentlichen Sektor Anwendung. Dies entspricht voll und ganz der Situation nach der derzeitigen Richtlinie 95/46/EG. Die Möglichkeit einer systematischen Unterscheidung in dieser Richtlinie zwischen öffentlichem und privatem Sektor wurde in den 1990er Jahren ausdrücklich erörtert, dann aber verworfen.

---

[28] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung), COM(2012) 11 final, Brüssel, 25. Januar 2012 (im weiteren Text: Vorschlag für eine Allgemeine Datenschutzverordnung).

[29] Die weiteren Verweise beziehen sich auf diese Verordnung (siehe Fußnote 28).

[30] Ein Beispiel für Neuerung wäre, dass heute mehr Gewicht auf Datenminimierung gelegt wird, d. h., es werden nicht mehr Daten als unbedingt erforderlich verarbeitet (Artikel 5 Buchstabe c). Ein weiteres Beispiel ist die Anerkennung des „eingebauten Datenschutzes" als allgemeiner Grundsatz (Artikel 23).

[31] Siehe Artikel 24 zur vorherigen Zurateziehung, beispielsweise in Fällen, in denen aus einer Folgenabschätzung hervorgeht, dass hohe konkrete Risiken bestehen können.

[32] Vgl. Begründung, S. 12., Punkt 3.4.6.2.

[33] Siehe Artikel 51 Absatz 2.

Dieser Ansatz wird durch die Tatsache verstärkt, dass Artikel 8 der EU-Charta das Recht auf den Schutz personenbezogener Daten explizit anerkennt und dass Artikel 16 AEUV eine ausdrückliche horizontale Rechtsgrundlage für die Annahme von Vorschriften für den Schutz personenbezogener Daten sowohl auf EU-Ebene als auch in den Mitgliedstaaten im Rahmen von Tätigkeiten vorsieht, die in den Anwendungsbereich des EU-Rechts fallen.

5.3. Inhalt der vorgeschlagenen Verordnung

Wenn wir uns nun den Inhalt der Verordnung ansehen, so stärkt dieser die Rollen der wichtigsten Akteure, also der betroffenen Person, des für die Verarbeitung Verantwortlichen und der Aufsichtsbehörden. Ein kurzer Blick auf die ersten beiden ist wichtig, um die Rolle der Datenschutzbehörde besser zu verstehen.

5.3.1. Betroffene Person

Als erstes könnte man von einer Stärkung der „Nutzerkontrolle“ sprechen, also von der Möglichkeit für die betroffene Person, darauf Einfluss zu nehmen, was mit ihren personenbezogenen Daten geschieht. Die bestehenden Rechte der betroffenen Person wurden insgesamt bestätigt und sogar noch gestärkt und ausgeweitet. Es wird auch einfacher sein, diese Rechte in der Praxis auszuüben.[34]

Das Erfordernis der Einwilligung wurde geklärt: *wenn* sie erforderlich ist, muss sie echt und kräftig sein.[35] Auch das Recht auf Einspruch wurde gestärkt.[36] Es stehen bessere Mittel zur Verfügung, mit denen sich die Wahrung der Rechte der betroffenen Person in der Praxis gewährleisten lässt. Der Transparenz wird größeres Gewicht beigemessen.[37] Es gibt eine Bestimmung, die kollektive Rechtsbehelfe einführt, nicht im Sinne einer Sammelklage nach US-Art, aber doch für Organisationen, die im Namen ihrer Mitglieder oder ihrer Klientel tätig werden.[38]

Es wird viel über das „Recht auf Vergessenwerden“ gesprochen, doch wird bei näherer Betrachtung klar, dass hier nur betont wird, dass Daten zu löschen sind, sobald kein hinreichender Grund mehr für ihre Aufbewahrung besteht.[39] Das Recht auf Datenübertragbarkeit[40] ist eigentlich auch nur eine Spezifizierung des bestehenden Rechts, eine Kopie der über eine Person gespeicherten Daten verlangen zu können, und zwar in einem bestimmten Format.

5.3.2. Für die Verarbeitung Verantwortlicher

Die größte Änderung ist eine wesentlich stärkere Betonung der tatsächlichen Verantwortung der verantwortlichen Organisationen. Verantwortung ist kein Konzept, das erst greift, wenn etwas schiefgelaufen ist. Stattdessen ist sie eine Verpflichtung, in der Praxis ein gutes Datenmanagement zu entwickeln. Dies zeigt sich an Formulierungen wie die, dass *durch geeignete Maßnahmen sichergestellt wird, dass die*

[34] Artikel 15 bis 17.
[35] Artikel 4 Absatz 8 und Artikel 7.
[36] Artikel 19.
[37] Artikel 5 Buchstabe a sowie Artikel 11 und 14.
[38] Artikel 73 Absatz 2 und Artikel 76 Absatz 1.
[39] Artikel 17.
[40] Artikel 18.

Bestimmungen der Verordnung eingehalten werden und *dass die Wirksamkeit dieser Maßnahmen zu überprüfen und der Nachweis dafür zu erbringen ist.*[41]

Hier haben sich die Akzente deutlich verschoben. Daran wird auch deutlich, dass die Beweislast in vielen Fällen bei der verantwortlichen Organisation liegt, die nachweisen können muss, dass es eine angemessene Rechtsgrundlage gibt, dass Einwilligungen tatsächlich erteilt wurden, und dass ergriffene Maßnahmen weiterhin wirksam sind. Das bedeutet, dass Datenschutzbehörden *ex post* stärker involviert und in der Lage sein werden, von den für die Verarbeitung Verantwortlichen angemessene Nachweise für den Stand ihrer Einhaltung der Vorschriften zu verlangen.

Die Verordnung beinhaltet auch einige spezifische Anforderungen, etwa für Datenschutz-Folgenabschätzungen[42], die Dokumentation der Datenverarbeitung[43] und die Ernennung eines behördlichen oder betrieblichen Datenschutzbeauftragten[44]. Diese sind wichtige Elemente eines guten Datenmanagements in Organisationen. Datenschutzbeauftragte können Organisationen bei der Einhaltung der Bestimmungen helfen und auch als Kontaktstellen für Datenschutzbehörden fungieren.

Einige dieser Bestimmungen, insbesondere zur Dokumentation, sind zu detailliert und müssten geändert werden, um sie angemessener zu gestalten. Einige der in den Bestimmungen aufgeführten Ausnahmen sind möglicherweise nicht ganz gerechtfertigt. Mehr Ausgewogenheit in diesem Teil des Vorschlags könnte beide Probleme tatsächlich lösen.

Darüber hinaus wurde eine allgemeine Bestimmung zur Meldung von Sicherheitsverletzungen eingeführt.[45] Im Moment sieht das EU-Recht eine solche Meldung nur für Telekommunikationsanbieter vor.

5.3.3. Aufsicht und Durchsetzung

Ein dritter Schwerpunkt der Verordnung ist eine wirksamere Aufsicht und Durchsetzung durch die Datenschutzbehörden. Die Garantien für die völlige Unabhängigkeit von Datenschutzbehörden wurden in voller Übereinstimmung mit dem Urteil des EuGH in der Rechtssache *Europäische Kommission gegen Bundesrepublik* Deutschland gestärkt.[46]

Die Verordnung sieht auch in allen Mitgliedstaaten Aufsichtsbehörden mit starken Durchsetzungsbefugnissen vor, wobei es sowohl um Untersuchungsbefugnisse als auch um Anordnungsbefugnisse und die Verhängung verwaltungsrechtlicher Sanktionen geht.[47] Derzeit verfügen die Mitgliedstaaten im Rahmen der Richtlinie 95/46/EG über einen sehr großen Ermessensspielraum, wodurch etliche Datenschutzbehörden im Moment nur geringe Befugnisse haben, und keine verfügt über die komplette Palette von Befugnissen, wie sie die vorgeschlagene Verordnung vorsieht.

[41] Artikel 22.
[42] Artikel 33.
[43] Artikel 28.
[44] Artikel 35 bis 37.
[45] Artikel 30 bis 32.
[46] Artikel 47.
[47] Artikel 53 und 79.

Bußgelder in Millionenhöhe – von der gleichen Größenordnung wie im Wettbewerbsrecht – ziehen viel Aufmerksamkeit auf sich, aber die Botschaft, die damit vermittelt werden soll, ist folgende: Wenn das hier wichtig ist, soll entsprechend damit umgegangen werden. Dies wird dazu führen, dass dem „Datenschutz" in den Chefetagen mehr Bedeutung beigemessen wird, was zu begrüßen wäre, und wahrscheinlich führt es auch zu einem besseren Datenmanagement und einer besseren Wahrung der Rechte der betroffenen Personen.

Auch die internationale Zusammenarbeit zwischen Datenschutzbehörden einschließlich Amtshilfe und gemeinsamer Maßnahmen wird stark unterstützt und erleichtert.[48] Die Einführung einer „federführenden Behörde" für Unternehmen mit mehreren Niederlassungen[49] ist begrüßenswert, aber diese federführende Behörde wird nicht alleine handeln, sondern Teil eines eng zusammenarbeitenden Netzwerks mit anderen zuständigen Behörden sein. Diese EU-Dimension wird auch explizit bei den Aufgaben von Datenschutzbehörden erwähnt.[50]

Von großer Bedeutung ist in dieser Hinsicht die Einführung eines Kohärenzverfahrens im Rahmen eines Europäischen Datenschutzausschusses[51], der auf der derzeitigen Gruppe der EU-Datenschutzbehörden („Artikel 29-Datenschutzgruppe") aufbauen wird.[52] Dieses Verfahren, an dem alle unabhängigen Behörden beteiligt werden, soll kohärente Ergebnisse der Aufsichts- und Durchsetzungsaktivitäten in allen Mitgliedstaaten gewährleisten. Seine Sekretariatsgeschäfte werden vom EDSB wahrgenommen.[53]

5.3.4 Datenschutz weltweit

Ein letztes Element ist die internationale Dimension der Verordnung im weiteren Sinn, und das in zweierlei Hinsicht. Der Anwendungsbereich der Verordnung wurde klargestellt und ausgeweitet. Diese Bestimmungen werden nunmehr nicht nur auf alle Datenverarbeitungen einer Niederlassung in der EU anwendbar sein, sondern auch, wenn Waren oder Dienstleistungen von einem Drittland auf den europäischen Markt geliefert oder dort erbracht werden, oder wenn das Verhalten von Europäern online überwacht wird.[54]

Das ist heutzutage im Internet Realität. Gleichzeitig ist es ein realistischer Ansatz, der auf einer wachsenden Konvergenz der Ansichten über den Datenschutz weltweit aufbaut. Das bedeutet, dass europäische Datenschutzbehörden vermehrt mit Fragen mit internationaler Dimension einschließlich Drittländern außerhalb der EU befasst sein werden.[55]

---

[48] Artikel 55 und 56.
[49] Vgl. weiter oben Punkt 5.2.
[50] Siehe Artikel 46 Absatz 1.
[51] Artikel 57 bis 58 und 64 bis 72.
[52] Diese gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtete Arbeitsgruppe arbeitet seit 1996 und besteht heute aus Vertretern aller nationalen Datenschutzbehörden und dem EDSB. Sie berät die Kommission auf deren Ersuchen oder auf eigene Initiative und erarbeitet unverbindliche Orientierungshilfen zu verschiedenen Themen, die in der Praxis allerdings von großer Bedeutung sind.
[53] Artikel 71.
[54] Siehe Artikel 3.
[55] Zu Beispielen aus jüngerer Zeit gehören Untersuchungen gegen Google durch die französische Datenschutzbehörde CNIL und gegen Facebook durch den irischen Datenschutzbeauftragten, an denen

Die internationale Zusammenarbeit entwickelt sich daher auch zwischen Datenschutzbehörden – z. B. zwischen der Federal Trade Commission in den USA und Datenschutzbehörden in der EU – mit einem weltweiten Netz (GPEN) auch in einem breiteren Kontext. Damit wird es möglich sein, besser mit globalen Akteuren im Internet umzugehen[56].

6. ZUSAMMENWIRKEN ZWISCHEN DATENSCHUTZBEHÖRDEN UND NATIONALEN MENSCHENRECHTSINSTITUTIONEN

Was also bedeutet dies alles für das Zusammenwirken zwischen Datenschutzbehörden und nationalen Menschenrechtsinstitutionen?

Zunächst gibt es da einen wichtigen Zeitfaktor. Die Vorschläge der Kommission werden derzeit in Rat und Parlament erörtert. Diese Erörterungen werden nicht nur ein paar Monate dauern. Aktuelle Schätzungen besagen, dass wir im Verlauf des Jahres 2013, vermutlich unter irischem Vorsitz, erste Schlussfolgerungen sehen werden. Auf jeden Fall kann die vorgeschlagene Verordnung 2014 vorbehaltlich einiger Verbesserungen bei verschiedenen Details verabschiedet werden. Damit dürfte die Verordnung vermutlich 2016 in Kraft treten. Mit anderen Worten: Die Mitgliedstaaten und alle anderen Interessengruppen haben ausreichend Zeit, sich auf die Umstellung vorzubereiten. Bis dahin werden der derzeitige Rahmen und die nationalen Rechtsvorschriften zu seiner Umsetzung weiterhin gelten und nur in Teilen geändert werden, um beispielsweise auf die Rechtsprechung des EuGH zu reagieren.

Für den Moment bedeutet dies, dass es auch weiterhin Vielfalt unter den nationalen Datenschutzbehörden geben wird. Eine ähnliche Vielfalt besteht allerdings auch bei den nationalen Menschenrechtsinstitutionen. Die an anderer Stelle in dieser Veröffentlichung erörterten Pariser Grundsätze[57] legen bestimmte Standards bezüglich der Befugnisse, Zuständigkeiten, Zusammensetzung und Arbeitsmethoden der nationalen Institutionen fest, aber es sind keine spezifischen Strukturen, Mandate oder Formen erforderlich. Das bedeutet, dass die derzeitige Art und Weise des Zusammenwirkens zwischen Datenschutzbehörden und nationalen Menschenrechtsinstitutionen in den verschiedenen Mitgliedstaaten je nach den herrschenden Bedingungen einschließlich der politischen Kultur und anderer Traditionen ganz unterschiedlich sein kann.

So ist es sehr gut möglich, dass die Datenschutzbehörden in einigen Mitgliedstaaten ähnlich wie Gleichstellungsstellen und nationale Ombudsleute zu den wichtigsten Akteuren in den nationalen Menschenrechtsinstitutionen zählen und auch aktiv zu deren Programmen beitragen, während dies in anderen Mitgliedstaaten nicht der Fall ist. In den Fällen, in denen ein reges Zusammenwirken zwischen Datenschutzbehörden und nationalen Institutionen besteht, ist es wahrscheinlich, dass die Zusammenarbeit auf dem allgemeinen Gebiet der Sensibilisierung und Bildung am engsten ist, denn diese Tätigkeiten hängen weniger von formalen Befugnissen und Verfahren ab. Bei der Bearbeitung von Beschwerden und bei Inspektionen dürfte ein

---

die meisten anderen europäischen Datenschutzbehörden sowie zuständige Behörden in Kanada und den USA beteiligt waren.

[56] Dies basiert auf einer zunehmenden Annäherung der Datenschutzgrundsätze und –praktiken weltweit, wobei nicht nur formale, von OECD, Europarat, EU, APEC, ISO und anderen Organisationen entwickelte Standards, sondern auch andere Instrumente wie Verhaltenskodizes, verbindliche unternehmensinterne Vorschriften usw. betroffen sind.

[57] Vgl. insbesondere G. De Beco, „Assessment of the Paris Principles and the ICC Sub-Committee on Accreditation“, Kapitel 11 in diesem Band.

reges Zusammenwirken etwas weniger wahrscheinlich sein. Es ist allerdings gut möglich, dass nationale Institutionen bei der Aufdeckung struktureller Probleme oder bestimmter Fragen, die Gegenstand einer Beschwerde oder Inspektion sein könnten, gute Arbeit geleistet haben oder dass sie sogar – im allgemeinen Interesse oder nicht - als einer der Beschwerdeführer auftreten.

In Zukunft kann all dies weiterhin der Fall sein, aber der wichtigste Unterschied wird darin bestehen, dass die derzeitige große Vielfalt bei den nationalen Datenschutzbehörden verschwunden oder wesentlich geringer sein wird. Dies wird das Ergebnis *unmittelbar* verbindlicher Anforderungen in der Verordnung sein, und zwar nicht nur an die unabhängige Stellung, sondern auch an die Aufgaben und Befugnisse der Aufsichtsbehörden. Es mag wohl nationale Regeln zu weiteren Details geben, vor allem hinsichtlich der Zusammensetzung und der internen Struktur der Aufsichtsbehörden, aber die wichtigsten Elemente werden in der Verordnung sichtbar und EU-weit unmittelbar anwendbar sein.

Viel mehr als jetzt wird es so sein, dass die nationalen Datenschutzbehörden nicht nur befugt sind, ihre Rolle im Bereich ihrer eigenen Rechtsordnung wahrzunehmen, sondern sie werden auch integraler Bestandteil der EU-weiten Zusammenarbeit bei grenzüberschreitenden und anderen gemeinsamen Fragen sein, und darüber hinaus werden sie zu einem EU-weiten Kohärenzverfahren gehören, das kohärente Ergebnisse sicherstellen soll. Es ist zweifellos ein Paradoxon, dass die institutionellen Garantien für Unabhängigkeit stärker sein werden und gleichzeitig Vorkehrungen getroffen werden, um eine nicht hilfreiche Vielfalt unter unabhängigen Behörden zu vermeiden. Das richtige Gleichgewicht in diesem Bereich zu finden wird natürlich ein Hauptanliegen sein. Selbst wenn in der Verordnung die geeigneten rechtlichen Vorkehrungen getroffen wurden, wird nach ihrer Verabschiedung noch immer die Notwendigkeit bestehen, wirksame Verfahren in der Praxis zu entwickeln. Die bestehende Artikel 29-Datenschutzgruppe als derzeitige Plattform der Datenschutzbehörden in der EU könnte viel bei der Vorbereitung des Wegs in diese Richtung tun.

Im Zusammenwirken mit nationalen Menschenrechtsinstitutionen wird dies wahrscheinlich nicht zu größeren Veränderungen, aber ganz bestimmt zu einer kohärenteren und berechenbareren Landschaft führen. Auf jeden Fall scheint es, als ob das Erfordernis der völligen Unabhängigkeit und die Notwendigkeit der Vermeidung jeglichen äußeren Einflusses die nationalen Datenschutzbehörden nicht daran hindern werde, entsprechende Beziehungen mit den nationalen Menschenrechtsinstitutionen einzugehen, und zwar vor allem im allgemeinen Bereich der Sensibilisierung und Bildung, um beiden mehr Wirkung zu verleihen. Gemäß den Pariser Grundsätzen werden nämlich ähnliche Standards für die nationalen Institutionen gelten. Somit wird es Sache beider Seiten sein, gegenseitige Beziehungen zum bestmöglichen gemeinsamen Nutzen zu entwickeln und zu strukturieren.

Ein weiteres Element mag noch zu betrachten sein. Wenn die Verordnung in ihrer vorliegenden Form verabschiedet wird, wird sie auch „Einrichtungen, Organisationen oder Verbänden, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben“ und die gemäß nationalem Recht korrekt gebildet wurden, das „Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben“ gewähren, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte

infolge der Verarbeitung personenbezogener Daten verletzt wurden.[58] Ein ähnliches Recht wird im Zusammenhang mit Gerichtsverfahren gelten.[59] Dies gibt mehr Raum für Sammelklagen, auch in Mitgliedstaaten, in denen diese Möglichkeit noch nicht besteht, und wird somit zu einer aktiveren Durchsetzung von Datenschutzvorschriften beitragen. Es bleibt abzuwarten, in welchem Ausmaß dies den nationalen Menschenrechtsinstitutionen oder ihren Anhängern erlauben würde, sich unmittelbarer als bisher in Datenschutzfragen einzubringen.

[58] Vorschlag für eine allgemeine Datenschutzverordnung, Fußnote 28, Artikel 73.
[59] Vorschlag für eine allgemeine Datenschutzverordnung, Fußnote 28, Artikel 76.