ARTIKEL-29-DATENSCHUTZGRUPPE

00062/10/DE
WP 173

Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht

Angenommen am 13. Juli 2010

ZUSAMMENFASSUNG

Die Grundsätze des europäischen Datenschutzes und die damit verbundenen Verpflichtungen spiegeln sich häufig nur unzureichend in konkreten internen Maßnahmen und Praktiken wider. Wenn der Datenschutz nicht Teil der gemeinsamen Werte und Praktiken von Organisationen wird und die entsprechenden Zuständigkeiten ausdrücklich zugewiesen werden, kann eine effektive Einhaltung der Datenschutzvorschriften kaum noch gewährleistet werden und Datenschutzpannen sind weiterhin vorprogrammiert.

Zur Stärkung des Datenschutzes in der Praxis braucht der europäische Rechtsrahmen zusätzliche Instrumente. Zweck dieser Stellungnahme ist es, die Kommission im Hinblick auf mögliche diesbezügliche Änderungen der Datenschutzrichtlinie zu beraten. Die Stellungnahme enthält insbesondere einen konkreten Vorschlag für einen Grundsatz der Rechenschaftspflicht, der die für die Verarbeitung Verantwortlichen verpflichten würde, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Richtlinie umzusetzen, und dies gegenüber den Kontrollstellen auf Verlangen nachzuweisen. Dies soll dazu beitragen, dass der Datenschutz von der Theorie zur Praxis übergeht, und die Datenschutzbehörden bei der Wahrnehmung ihrer Überwachungsaufgaben und der Durchsetzung der Rechtsvorschriften unterstützt werden.

Die Stellungnahme enthält Vorschläge, wie gewährleistet werden kann, dass der Grundsatz der Rechenschaftspflicht Rechtssicherheit bietet und gleichzeitig anpassbar ist (d. h. die Festlegung der konkreten Maßnahmen je nach dem mit der Datenverarbeitung verbundenen Risiko und den Arten der verarbeiteten Daten ermöglicht). Anschließend wird erörtert, wie sich dieser Grundsatz auf andere Bereiche, etwa Datenübertragungen in Drittländer, Meldepflichten, Sanktionen und letztlich auch die Entwicklung von Zertifizierungsprogrammen oder Gütesiegeln auswirken könnte.

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung,

hat folgende Stellungnahme angenommen:

1. EINLEITUNG

1. Der Datenschutz muss von der Theorie zur Praxis übergehen. Rechtliche Vorgaben müssen in echten Datenschutzmaßnahmen umgesetzt werden. Zur Stärkung des Datenschutzes in der Praxis braucht der europäische Rechtsrahmen zum Datenschutz zusätzliche Mechanismen. In den Diskussionen zur Zukunft des europäischen und globalen Rechtsrahmens zum Datenschutz wurden auf Rechenschaftspflicht beruhende Mechanismen vorgeschlagen, um die für die Verarbeitung Verantwortlichen dazu anzuhalten, praktische Instrumente für einen effektiven Datenschutz anzuwenden.

2. In ihrem Dokument „Die Zukunft des Datenschutzes“ (WP 168) vertritt die Artikel-29-Datenschutzgruppe die Ansicht, dass die Vorgaben zum Datenschutz mit dem gegenwärtigen Rechtsrahmen nicht vollständig in wirksame Mechanismen, die einen echten Schutz gewährleisten, umgesetzt werden konnten. Zur Verbesserung dieser Situation schlug die Artikel-29-Datenschutzgruppe der Kommission vor, auf Rechenschaftspflicht beruhende Mechanismen und insbesondere die Aufnahme eines Grundsatzes der Rechenschaftspflicht in die überarbeitete Datenschutzrichtlinie in Erwägung zu ziehen.[1] Dieser Grundsatz würde die Rolle des für die Verarbeitung Verantwortlichen stärken und ihm mehr Verantwortung übertragen.

---

[1] „Zur Bekämpfung dieses Problems wäre es angebracht, in den umfassenden Rechtsrahmen den Grundsatz der Rechenschaftspflicht aufzunehmen. Dieser Grundsatz würde die für die Verarbeitung Verantwortlichen dazu verpflichten, die notwendigen Maßnahmen zu ergreifen, um sicherzustellen, dass die wesentlichen Grundsätze und Verpflichtungen der geltenden Richtlinie bei der Verarbeitung personenbezogener Daten eingehalten werden. Eine solche Bestimmung würde die Forderung unterstreichen, dass Strategien und Mechanismen eingeführt werden müssen, mit denen die wesentlichen Grundsätze und Verpflichtungen der geltenden Richtlinie wirkungsvoll werden. Sie würde den Bedarf an wirkungsvollen Schritten unterstreichen, die zu einer wirkungsvollen internen Durchführung der wesentlichen Verpflichtungen und Grundsätze führen, die in der aktuellen Richtlinie verankert sind. Darüber hinaus würde der Grundsatz der Rechenschaftspflicht von den für die Verarbeitung Verantwortlichen verlangen, dass sie für die notwendigen internen Mechanismen sorgen, damit sie gegenüber externen interessierten Parteien, einschließlich der nationalen Datenschutzbehörden, die Einhaltung beweisen können. Die daraus resultierende Forderung nach Beweisen für die für Einhaltungszwecke durchgeführten angemessenen Maßnahmen wird die Durchsetzung von anzuwendenden Vorschriften sehr vereinfachen.“ (WP 168 Absatz 79, weitere Informationen sind auch in den Absätzen 74–78 zu finden.)

3. Ein rechtlich verankerter Grundsatz der Rechenschaftspflicht würde also, kurz gesagt, die für die Verarbeitung Verantwortlichen ausdrücklich verpflichten, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Richtlinie umzusetzen, und dies auf Verlangen nachzuweisen. In der Praxis dürfte dies zu anpassbaren Programmen führen, die der Umsetzung der bestehenden Datenschutzgrundsätze dienen (bisweilen auch als Compliance-Programme bezeichnet). Ergänzend könnten konkrete zusätzliche Vorgaben festgelegt werden, um Datenschutzgarantien umzusetzen oder ihre Wirksamkeit zu gewährleisten. Denkbar wäre beispielsweise eine Bestimmung, die bei mit höheren Risiken behafteten Datenverarbeitungsvorgängen eine Datenschutzverträglichkeitsprüfung vorschreibt.

4. Diese Stellungnahme stützt sich auf den Beitrag der Artikel-29-Datenschutzgruppe zu diesem Thema in der Stellungnahme zur Zukunft des Datenschutzes und soll die Kommission bei der laufenden Überarbeitung der Richtlinie 95/46/EG unterstützen. Zu diesem Zweck ist die Stellungnahme in vier Abschnitte untergliedert: Im ersten Abschnitt wird erörtert, warum die für die Verarbeitung Verantwortlichen ihre internen praktischen Regelungen (Grundsätze und Verfahrensweisen) stärken müssen, um zu gewährleisten, dass alle Datenverarbeitungsvorgänge den anwendbaren Vorschriften entsprechen, und wie auf Rechenschaftspflicht beruhende Systeme dazu beitragen können, dieses Ziel zu erreichen. Anschließend geht es um den möglichen rechtlichen Aufbau eines auf Rechenschaftspflicht beruhenden Systems und Beispiele aus dem Bereich des Datenschutzes und anderen Bereichen. Der zweite Abschnitt enthält einen konkreten Vorschlag für einen Grundsatz der Rechenschaftspflicht und erläutert die Beweggründe für die verschiedenen Aspekte des Vorschlags. Im dritten Abschnitt werden verschiedene Bestandteile eines Rechtssystems, das ein allgemeines System der Rechenschaftspflicht umfasst, diskutiert. Ferner wird erörtert, warum ein solcher Vorschlag Rechtssicherheit bieten und gleichzeitig ausreichend allgemein gefasst sein muss, um anpassbar zu sein (und je nach dem mit der Datenverarbeitung verbundenen Risiko und den Arten der verarbeiteten Daten die Festlegung der konkreten Maßnahmen und Überprüfungsmethoden zu ermöglichen). Danach geht es um damit zusammenhängende Aspekte, etwa bei Auslandsüberweisungen. Es wird beschrieben, welche Vorteile ein auf Rechenschaftspflicht beruhender Mechanismus für die Datenschutzbehörden hätte, und die Funktion einer möglichen Zertifizierung dargelegt.

II. RECHENSCHAFTSPFLICHT: ZIELE, RECHTLICHER AUFBAU, BEISPIELE UND TERMINOLOGIE

II.1 Rechenschaftspflicht als Triebfeder für die effektive Umsetzung der Grundsätze des Datenschutzes

5. Heutzutage besteht zunehmend Bedarf und Interesse daran, dass die für die Verarbeitung Verantwortlichen wirksame Maßnahmen treffen, die einen echten Datenschutz gewährleisten. Dafür gibt es verschiedene Gründe, die nachstehend dargelegt werden.

6. Erstens haben wir es mit einer Datenflut zu tun, wobei die Menge der personenbezogenen Daten, die bestehen, verarbeitet und weitergeleitet werden, stetig steigt. Dazu tragen sowohl der technische Fortschritt, d. h. immer mehr Informations- und Kommunikationssysteme, als auch die wachsende Fähigkeit Einzelner, Technologien interaktiv zu nutzen, bei. Je mehr Daten verfügbar sind und übermittelt werden, umso höher ist die Gefahr von Datenschutzverletzungen. Auch dies zeigt, wie dringend notwendig es ist, dass die für die Verarbeitung Verantwortlichen im öffentlichen wie im privaten Sektor wirksame interne Mechanismen umsetzen, die den Schutz personenbezogener Daten garantieren.

7. Zweitens geht die wachsende Menge personenbezogener Informationen mit einem Anstieg ihres gesellschaftlichen, politischen und wirtschaftlichen Wertes einher. In einigen Bereichen, vor allem aber im Internet, sind personenbezogene Daten faktisch die Währung, für die man Online-Inhalte erhält. Gleichzeitig findet der soziale Nutzen des Datenschutzes immer mehr Anerkennung in der Gesellschaft. Während also der Wert der personenbezogenen Daten, mit denen die für die Verarbeitung Verantwortlichen in allen Bereichen zu tun haben, steigt, werden sich Bürger, Verbraucher und die Gesellschaft zunehmend der Bedeutung dieser Daten bewusst. Dies unterstreicht wiederum die Notwendigkeit, strikte Maßnahmen zu ihrem Schutz umzusetzen.

8. Aus den vorstehenden Ausführungen geht außerdem hervor, dass Datenschutzverletzungen erhebliche negative Folgen für die für die Verarbeitung Verantwortlichen im öffentlichen wie im privaten Sektor haben können. Mögliche Pannen bei eGovernment- oder eHealth-Anwendungen hätten verheerende wirtschaftliche, vor allem aber rufschädigende Folgen. Die für die Verarbeitung Verantwortlichen in allen Bereichen sind also darauf angewiesen, Risiken zu minimieren, einen guten Ruf aufzubauen und zu pflegen und das Vertrauen von Bürgern und Verbrauchern zu gewinnen.

9. Zusammengefasst zeigt sich, wie dringend es notwendig ist, dass die für die Verarbeitung Verantwortlichen echte und wirksame Datenschutzmaßnahmen anwenden, die auf ein verantwortungsvolles Datenschutzmanagement gerichtet sind und zudem die sich aus eine schlechten Datenschutzpraxis ergebenden rechtlichen und wirtschaftlichen Risiken sowie die Gefahr der Rufschädigung minimieren. Wie nachfolgend weiter ausgeführt wird, verfolgen auf Rechenschaftspflicht beruhende Mechanismen genau diese Ziele.

II.2 Möglicher allgemeiner rechtlicher Aufbau von auf Rechenschaftspflicht beruhenden Mechanismen

10. In diesem Zusammenhang stellt sich die Frage, auf welche Weise der Rechtsrahmen die für die Verarbeitung Verantwortlichen dazu anhalten könnte, Maßnahmen zu treffen, die einen echten Schutz in der Praxis bieten, oder – anders ausgedrückt – wie auf Rechenschaftspflicht beruhende Systeme rechtlich aufgebaut sein sollten.

11. Vor der Erörterung dieses Aufbaus sei betont, dass solche Systeme die wesentlichen Grundsätze des Datenschutzes in keiner Weise ändern oder beeinträchtigen, sondern vielmehr bewirken sollen, dass sie besser funktionieren.

12. Eine Möglichkeit, die für die Verarbeitung Verantwortlichen zu derartigen Maßnahmen zu veranlassen, wäre die Einführung eines Grundsatzes der Rechenschaftspflicht in der überarbeiteten Fassung der Richtlinie. In der Folge wäre zu erwarten, dass interne Maßnahmen und Verfahren zur effektiven Umsetzung bestehender Datenschutzgrundsätze festgelegt werden, ihre Wirksamkeit sichergestellt wird und eine Pflicht zum Nachweis auf Verlangen der Datenschutzbehörden eingeführt wird. Wie nachstehend weiter ausgeführt wird, würde sich die Art dieser Verfahren und Mechanismen nach den durch die Verarbeitung und die Art der Daten erwachsenden Risiken richten.

13. Darüber hinaus könnten besondere Anforderungen, etwa eine Pflicht zur Durchführung von Datenschutzverträglichkeitsprüfungen in bestimmten Fällen oder zur Bestellung von Datenschutzbeauftragten, in Erwägung gezogen werden. Diese besonderen Anforderungen könnten den allgemeinen Grundsatz der Rechenschaftspflicht ergänzen.

14. Die Artikel-29-Datenschutzgruppe erkennt an, dass die für die Verarbeitung Verantwortlichen unter Umständen Maßnahmen und Verfahren einführen möchten, die in den Rechtsvorschriften zum Datenschutz nicht direkt vorgesehen sind. So könnte sich etwa ein für die Verarbeitung Verantwortlicher verpflichten, sehr kurzfristig auf Zugangsanträge zu reagieren, obwohl die Rechtsvorschriften eine gewisse Flexibilität vorsehen. Er könnte sich auch verpflichten, Zugangsanträge gleichzeitig online und offline zu beantworten, um den prompten und effektiven Erhalt der Informationen zu gewährleisten. Ferner wäre denkbar, dass der für die Verarbeitung Verantwortliche die im allgemeinen Rechtsrahmen verankerten Mindestanforderungen ausweiten möchte, indem er etwa beschließt, einen Datenschutzbeauftragten zu bestellen, obwohl die geltenden Rechtsvorschriften dies nicht zwingend vorschreiben. Ein für die Verarbeitung Verantwortlicher könnte auch einen Dritten mit einer Prüfung *aller* in seine Zuständigkeit fallenden Datenverarbeitungsvorgänge beauftragen, um festzustellen, ob sie dem Rechtsrahmen zum Datenschutz entsprechen. Die Artikel-29-Datenschutzgruppe begrüßt derartige Initiativen und regt an, dass der neue Rechtsrahmen zum Datenschutz entsprechende Anreize für die für die Verarbeitung Verantwortlichen enthalten sollte.

15. Dementsprechend würden auf Rechenschaftspflicht beruhende Mechanismen rechtlich gesehen aus zwei Ebenen bestehen: Die erste Ebene würde eine grundlegende und für *alle* für die Verarbeitung Verantwortlichen verbindliche Vorgabe enthalten, die zwei Elemente umfasst: die Einführung von Maßnahmen bzw. Verfahren und das Führen entsprechender Nachweise. Spezifische Anforderungen könnten diese erste Ebene ergänzen. Die zweite Ebene würde freiwillige auf Rechenschaftspflicht beruhende Systeme enthalten, die im Rahmen der zugrunde liegenden Grundsätze des Datenschutzes über die Mindestanforderungen hinausgehen, indem sie mehr Sicherheit bieten, als in den anwendbaren Rechtsvorschriften vorgesehen, und/oder über das vorgeschriebene Mindestmaß hinaus Maßnahmen beinhalten bzw. ihre Wirksamkeit gewährleisten. Diese Stellungnahme befasst sich, ohne die Bedeutung und Vorteile solcher Systeme zu verkennen, hauptsächlich mit der Vorgabe in der ersten Ebene und insbesondere mit dem allgemeinen Grundsatz der Rechenschaftspflicht.

II.3 Der Grundsatz der Rechenschaftspflicht im Datenschutz´und anderen Bereichen und Terminologie

Beispiele

16. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass der Grundsatz der Rechenschaftspflicht an sich nicht neu ist. Er wird in den 1980 angenommenen Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zum Datenschutz ausdrücklich anerkannt. Der darin verankerte Grundsatz der Rechenschaftspflicht lautet: „Der Datenhauptverantwortliche muss bezüglich der Einhaltung der Maßnahmen, die den oben genannten [wesentlichen] Grundsätzen Gültigkeit verleihen, zur Rechenschaft gezogen werden können."

17. Erst kürzlich wurde er in die von der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre erarbeiteten Madrider Internationalen Standards ausdrücklich aufgenommen.[2] Er ist außerdem im jüngsten ISO-Normentwurf 29100 zur Festlegung eines Datenschutzrahmens verankert und eines der Hauptkonzepte des Datenschutzrahmens der APEC und ihrer Regeln für den grenzüberschreitenden Schutz der Privatsphäre.[3]

18. Was gesetzliche Vorgaben anbelangt, so weist die Artikel-29-Datenschutzgruppe darauf hin, dass die im kanadischen Personal Information Protection and Electronics Documents Act enthaltenen Fair Information Principles auf die Rechenschaftspflicht Bezug nehmen. So sieht der erste dieser Grundsätze die Erarbeitung und Durchführung von Maßnahmen und Verfahren zur Umsetzung der 10 Fair Information Principles (unter anderem die Einführung von Verfahren zum Schutz personenbezogener Informationen und die Festlegung von Verfahren zur Entgegennahme und Beantwortung von Beschwerden und Anfragen) vor.

19. Ferner stellt die Artikel-29-Datenschutzgruppe fest, dass der Grundsatz der Rechenschaftspflicht auch in verbindlichen unternehmensinternen Datenschutzregelungen („BCR"), die bei internationalen Datenübertragungen angewandt werden, verankert ist. BCR sind in der Tat von multinationalen Unternehmen erarbeitete und befolgte Verhaltenskodizes, die interne Maßnahmen zur wirksamen Umsetzung von Datenschutzgrundsätzen (etwa Audits, Schulungsprogramme, Netzwerke von Datenschutzbeauftragten oder ein Beschwerdebearbeitungssystem) enthalten. Nach ihrer Überprüfung durch die einzelstaatlichen Datenschutzbehörden ist davon auszugehen, dass BCR für die Übermittlung oder bestimmte Kategorien von Übermittlungen personenbezogener Daten zwischen Unternehmen eines Konzerns, die an diese BCR gebunden sind, ausreichende Garantien im Sinne von Artikel 25 und Artikel 26 Absatz 2 der Richtlinie 95/46/EG bieten.

---

2 Die verantwortliche Person muss: „a) Die notwendigen Maßnahmen zur Erfüllung der in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung aufgeführten Grundsätze und Verpflichtungen ergreifen; und b) die erforderlichen Nachweise über die Erfüllung der o. g. Vorgaben erbringen, und zwar sowohl gegenüber dem Betroffenen als auch gemäß Artikel 23 gegenüber den zuständigen Aufsichtsbehörden."

3 Darüber hinaus untersucht das Centre for Information Policy Leadership die Auswirkungen des Grundsatzes der Rechenschaftspflicht auf den Datenschutz und den Schutz der Privatsphäre. Siehe: www.informationpolicycentre.com

20. Außerhalb der Welt des Datenschutzes gibt es einige Beispiele für Rechenschaftspflicht. Dabei handelt es sich zumeist um Programme mit Maßnahmen und Verfahren des für die Verarbeitung Verantwortlichen zur Gewährleistung der Einhaltung von Gesetzen und Vorschriften. So sind etwa im Finanzdienstleistungssektor Compliance-Programme zwingend vorgeschrieben. In anderen Bereichen wie dem Wettbewerbsrecht sind Compliance-Programme zwar nicht vorgeschrieben aber durchaus erwünscht. Beispielsweise hat der kanadische Wettbewerbsbeauftragte umsichtige Regelungen zu Compliance-Programmen ausgearbeitet. Die Entscheidung, ein solches Programm anzuwenden, liegt beim jeweiligen Unternehmen. Der kanadische Wettbewerbsbeauftragte betont jedoch die Bedeutung von Compliance als Instrument zur Risikominderung und hebt die rechtlichen und wirtschaftlichen Vorteile sowie den Nutzen für das Ansehen des Unternehmens hervor.[4]

Terminologie

21. Der englische Begriff „Accountability“ (Rechenschaftspflicht) ist angelsächsischer Herkunft und wird im angelsächsischen Sprachraum häufig verwendet, wo auch im Wesentlichen Einvernehmen über seine Bedeutung herrscht, wenngleich es schwierig ist, seine exakte Bedeutung in der Praxis zu definieren. Allgemein gesagt drückt er hauptsächlich aus, wie Verantwortung überprüfbar wahrgenommen wird. Verantwortung und Rechenschaftspflicht sind zwei Seiten einer Medaille und wesentliche Bestandteile der Good Governance. Nur wenn Verantwortung in der Praxis nachweislich effektiv wahrgenommen wird, kann sich das notwendige Vertrauen entwickeln.

22. Der Begriff „Accountability“ lässt sich – hauptsächlich aufgrund der Unterschiede in den Rechtssystemen – nur schwer in die meisten anderen europäischen Sprachen übersetzen. Infolgedessen ist die Gefahr hoch, dass Auslegungsunterschiede eine Harmonisierung erschweren. Um die Bedeutung des Begriffs „Accountability“ zu erfassen, wurden andere Wörter und Wendungen wie beispielsweise „reinforced responsibility“ (verstärkte Verantwortung), „assurance“ (Zusicherung, Garantie), „reliability“ (Zuverlässigkeit), „trustworthiness“ (Vertrauenswürdigkeit) und die französische Wendung „obligation de rendre des comptes“ (Rechenschaftspflicht) vorgeschlagen. Mann könnte auch sagen, dass sich Rechenschaftspflicht auf die „Umsetzung der Grundsätze des Datenschutzes“ bezieht.

23. Wir konzentrieren uns daher in diesem Dokument auf die zur Gewährleistung der Einhaltung der Datenschutzvorschriften zu treffenden Maßnahmen. Wo auf Rechenschaftspflicht Bezug genommen wird, ist deshalb stets die in dieser Stellungnahme gebrauchte Bedeutung gemeint, was jedoch nicht ausschließt, dass sich diese Bedeutung durch ein anderes Wort genauer ausdrücken lässt. Aus diesem Grunde geht es hierin nicht um Terminologie. Stattdessen konzentriert sich dieses Dokument pragmatisch auf die zu treffenden Maßnahmen, anstatt auf den Begriff an sich.

---

4 www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

III. VORSCHLAG FÜR EINE ALLGEMEINE REGELUNG ZUR RECHENSCHAFTSPFLICHT

III.1 Eine allgemeine Regelung zur Bekräftigung und Stärkung der Verantwortung der für die Verarbeitung Verantwortlichen

24. Die Artikel-29-Datenschutzgruppe hat sich unter Berücksichtigung der in Abschnitt I angestellten Überlegungen weiter mit einer möglichen Einbeziehung von auf Rechenschaftspflicht beruhenden Lösungen in den neuen umfassenden Rechtsrahmen zum Datenschutz befasst.

25. Dabei hat sich ihre bereits in der Stellungnahme zur Zukunft des Datenschutzes vertretene Auffassung, dass in den neuen umfassenden Rechtsrahmen ein allgemeiner Grundsatz der Rechenschaftspflicht aufgenommen werden sollte, bestätigt. Zweck einer solchen Regelung wäre die Bekräftigung und Stärkung der Verantwortung der für die Verarbeitung Verantwortlichen. Dies schließt eine Ergänzung dieses Grundsatzes durch konkrete Maßnahmen in Bezug auf die Rechenschaftspflicht nicht aus.

26. Die neue Regelung würde mit den im derzeitigen Rechtsrahmen bereits enthaltenen spezifischen Vorschriften im Einklang stehen. Dies ergibt sich insbesondere aus Artikel 6 der Richtlinie 95/46/EG, in dessen Absatz 1 die Grundsätze in Bezug auf die Qualität der Daten aufgeführt werden, während es in Absatz 2 heißt: „Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.“ Die Regelung würde auch Artikel 17 Absatz 1 entsprechen, der vorsieht, dass die für die Verarbeitung Verantwortlichen sowohl technische als auch organisatorische Maßnahmen durchführen. Eine allgemeine Regelung zur Rechenschaftspflicht würde die für die Verarbeitung Verantwortlichen sogar noch mehr dazu anhalten, die in Artikel 17 festgelegten Sicherheitsanforderungen zusätzlich zu den in den übrigen Artikeln enthaltenen Vorgaben umzusetzen.

III.2 Konkreter Vorschlag für einen allgemeinen Grundsatz der Rechenschaftspflicht

27. Ziel der neuen Regelung wäre es, konkreten und praktischen Maßnahmen Vorschub zu leisten, um die auf der Ebene des für die Verarbeitung Verantwortlichen festgelegten allgemeinen Grundsätze des Datenschutzes unter Einhaltung der anwendbaren Gesetze und Vorschriften in konkrete Strategien und Verfahrensweisen umzusetzen. Der für die Verarbeitung Verantwortliche sollte außerdem die Wirksamkeit der getroffenen Maßnahmen gewährleisten und auf Verlangen nachweisen, dass er diese Maßnahmen auch tatsächlich ergriffen hat.

28. Prinzipiell müsste eine solche allgemeine Regelung zwei grundlegende Elemente enthalten:

    (i) die Vorgabe, dass der für die Verarbeitung Verantwortliche geeignete und wirksame Maßnahmen zur Umsetzung der Grundsätze des Datenschutzes treffen muss,

(ii) die Vorgabe, auf Verlangen nachzuweisen, dass geeignete und wirksame Maßnahmen getroffen worden sind. Der für die Verarbeitung Verantwortliche müsste also Nachweise zu Punkt (i) erbringen.

29. Die Vorschrift sollte für alle für die Verarbeitung Verantwortlichen und sämtliche Situationen gelten.

30. Das erste Element dieser Vorschrift würde die für die Verarbeitung Verantwortlichen dazu verpflichten, geeignete Maßnahmen zu treffen. Die Arten von Maßnahmen sollten im Wortlaut der allgemeinen Regelung zur Rechenschaftspflicht nicht festgelegt werden. In späteren Anleitungen der einzelstaatlichen Datenschutzbehörden, der Artikel-29-Datenschutzgruppe oder der Kommission (im Ausschussverfahren) könnte für bestimmte Fälle festgelegt werden, welche Maßnahmen mindestens zu treffen sind, damit die Maßnahmen als geeignet gelten können. Ein Beispiel für solche Mindestmaßnahmen wäre etwa in bestimmten Fällen die Festlegung der zur Umsetzung der Grundsätze des Datenschutzes notwendigen internen Strategien und Prozesse unter Berücksichtigung der anwendbaren Gesetze und Vorschriften.

31. Diese Maßnahmen und Prozesse können auch durch Aufgabenverteilung und Schulung des mit Datenverarbeitungsvorgängen befassten Personals effektiv durchgeführt werden. Die für die Verarbeitung Verantwortlichen sollten insbesondere im Hinblick auf Artikel 18 der Richtlinie dazu ermuntert werden, Datenschutzbeauftragte zu bestellen. In jedem Fall sollte jedoch die Aufgabenverteilung auf verschiedenen Ebenen der Organisation gefördert werden, um die Erfüllung der betreffenden Aufgaben zu gewährleisten.

32. Für die Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union sollten die für die Verarbeitung Verantwortlichen geeignete Maßnahmen – etwa die Annahme von BCR – treffen und durchführen, die, wie in Artikel 26 der Richtlinie vorgesehen, ausreichende Garantien bieten.

33. Die für die Verarbeitung Verantwortlichen sollten außerdem dafür sorgen, dass die zur Einhaltung der Grundsätze des Datenschutzes durchgeführten praktischen Maßnahmen wirksam sind. Bei umfangreichen, komplexen oder mit hohen Risiken behafteten Datenverarbeitungsvorgängen sollte die Wirksamkeit der getroffenen Maßnahmen regelmäßig überprüft werden. Dafür gibt es verschiedene Möglichkeiten wie beispielsweise Monitoring, interne oder externe Audits.

34. Die Artikel-29-Datenschutzgruppe schlägt entsprechend den vorstehenden Ausführungen folgenden Wortlaut für eine konkrete Vorschrift, die in einen umfassenden Rechtsrahmen aufgenommen werden könnte, vor:

„Artikel X – Umsetzung der Grundsätze des Datenschutzes

(1) Der für die Verarbeitung Verantwortliche trifft geeignete und wirksame Maßnahmen, die die Einhaltung der in der Richtlinie festgelegten Grundsätze und Verpflichtungen gewährleisten.
(2) Der für die Verarbeitung Verantwortliche weist gegenüber der Kontrollstelle auf deren Verlangen die Einhaltung des Absatzes 1 nach.

IV. ERÖRTERUNG VERSCHIEDENER BESTANDTEILE DES ALLGEMEINEN GRUNDSATZES DER RECHENSCHAFTSPFLICHT

IV.1 Bekräftigung bestehender Verpflichtungen

35. Der Artikel-29-Datenschutzgruppe ist bewusst, dass die für die Verarbeitung Verantwortlichen den allgemeinen Grundsatz der Rechenschaftspflicht – insbesondere angesichts der gegenwärtigen schwierigen Wirtschaftslage in der EU – möglicherweise als belastende neue Rechtsvorschrift empfinden. Dies wäre jedoch ein Irrtum.

36. Die Artikel-29-Datenschutzgruppe betont, dass die in dieser neuen Vorschrift enthaltenen Vorgaben größtenteils in den geltenden Rechtsvorschriften bereits existieren, wenn auch weniger explizit. Die für die Verarbeitung Verantwortlichen sind nach dem derzeitigen Rechtsrahmen sehr wohl verpflichtet, die in der Richtlinie dargelegten Grundsätze und Verpflichtungen einzuhalten. Dazu ist es eigentlich notwendig, Datenschutzverfahren festzulegen und gegebenenfalls zu überprüfen. So gesehen stellt eine Regelung zur Rechenschaftspflicht nichts wesentlich Neues dar und enthält im Grunde keine Vorgaben, die nicht bereits in den bestehenden Rechtsvorschriften implizit enthalten sind. Die neue Vorschrift verfolgt also, kurz gesagt, nicht das Ziel, die für die Verarbeitung Verantwortlichen neuen Grundsätzen zu unterwerfen, sondern soll vielmehr faktisch dafür sorgen, dass bestehende Grundsätze effektiv befolgt werden.

37. Zu einer in gewisser Hinsicht ähnlichen legislativen Entwicklung kam es im Zuge der Änderung der Richtlinie 2002/58/EG im Jahr 2009.[5] In diesem Fall wurde mit der neuen Richtlinie eine Verpflichtung zur Umsetzung eines Sicherheitskonzepts („*Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten*“) eingeführt. Nach Ansicht des Gemeinschaftsgesetzgebers war es also im Hinblick auf die Sicherheitsbestimmungen der Richtlinie notwendig, eine ausdrückliche Verpflichtung zur Umsetzung eines Sicherheitskonzepts einzuführen. Zudem sind in Artikel 18 der Richtlinie 95/46/EG (Bestellung von Datenschutzbeauftragten) und mit dem oben erwähnten System verbindlicher unternehmensinterner Datenschutzregelungen bereits Beispiele für praktische Maßnahmen angeführt, die der für die Verarbeitung Verantwortliche treffen kann.

38. Mit den vorstehenden Ausführungen im Zusammenhang steht die Frage nach den Folgen der Einhaltung (oder Nichteinhaltung) des Grundsatzes der Rechenschaftspflicht. Die Artikel-29-Datenschutzgruppe betont, dass die Einhaltung des Grundsatzes der Rechenschaftspflicht nicht notwendigerweise bedeutet, dass der für die Verarbeitung Verantwortliche auch die in der Richtlinie dargelegten wesentlichen Grundsätze einhält; weder lässt sich also aus ihr eine Rechtsvermutung in Bezug auf die Einhaltung ableiten, noch kann sie einen der

---

5 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

wesentlichen Grundsätze ersetzen. Ein für die Verarbeitung Verantwortlicher kann die von ihm getroffenen Maßnahmen durchgeführt und überprüft haben und dennoch gegen die Datenschutzvorschriften verstoßen. Das Treffen von Maßnahmen zur Einhaltung der Grundsätze darf also in keinem Fall ausschließen, dass für die Verarbeitung Verantwortliche von Datenschutzbehörden belangt werden können. In der Praxis ist es wahrscheinlicher, dass für die Verarbeitung Verantwortliche im öffentlichen wie im privaten Sektor, die robuste Compliance-Programme aufgestellt haben, die Rechtsvorschriften einhalten. Weil sie nämlich wirksame Maßnahmen zur Einhaltung der wesentlichen Grundsätze des Datenschutzes praktisch anwenden, ist die Wahrscheinlichkeit, dass sie gegen Rechtsvorschriften verstoßen, geringer. Die Datenschutzbehörden könnten daher bei der Festlegung von Sanktionen für Datenschutzverletzungen die Durchführung (oder Nichtdurchführung) von Maßnahmen und ihre Überprüfung berücksichtigen.

IV.2 Geeignete Maßnahmen zur Umsetzung der Richtlinie

39. Eine Regelung zur Rechenschaftspflicht würde die für die Verarbeitung Verantwortlichen dazu verpflichten, die notwendigen Maßnahmen festzulegen und umzusetzen, um sicherzustellen, dass die Grundsätze und Verpflichtungen der Richtlinie eingehalten werden, und ihre Wirksamkeit regelmäßig überprüfen zu lassen.

40. Bei dem vorgeschlagenen allgemeinen Grundsatz der Rechenschaftspflicht wird eine detaillierte Festlegung der Art der durchzuführenden Maßnahmen bewusst vermieden. Daraus ergeben sich zwei miteinander verbundene, grundlegende Fragen: (i) Welche gängigen Maßnahmen würden dem Grundsatz der Rechenschaftspflicht entsprechen? (ii) Wie lassen sich die Maßnahmen skalieren und an konkrete Umstände anpassen?

Beispielhafte Maßnahmen

41. Die Artikel-29-Datenschutzgruppe schlägt folgende nicht erschöpfende Liste gängiger Maßnahmen, die dem Grundsatz der Rechenschaftspflicht entsprechen würden, vor:

    - Festlegung interner Verfahren *vor* Beginn neuer Verarbeitungen personenbezogener Daten (interne Prüfung, Beurteilung usw.);[6]
    - Aufstellung schriftlicher und verbindlicher Datenschutzstrategien, die bei neuen Datenverarbeitungsvorgängen zu berücksichtigen und anzuwenden sind (z. B. Einhaltung der Grundsätze zur Datenqualität, Unterrichtung, Sicherheit, Zugänglichkeit usw.) und den betroffenen Personen zur Verfügung zu stellen sind;
    - Zuordnung der Verfahren, um eine genaue Identifizierung aller Datenverarbeitungsvorgänge zu ermöglichen, und Führen eines Verzeichnisses von Datenverarbeitungsvorgängen;

---

[6] Für laufende Datenverarbeitungsvorgänge müsste eine Übergangsfrist festgelegt werden, innerhalb derer sie in Einklang mit den geänderten Rechtsvorschriften zu bringen sind.

- Bestellung eines Datenschutzbeauftragten und anderer für den Datenschutz zuständiger Personen;
- angemessene Mitarbeiterschulungs- und -fortbildungsangebote im Bereich Datenschutz, die sich unter anderem an diejenigen richten, die personenbezogene Daten verarbeiten (oder dafür verantwortlich sind), aber auch an IT-Manager, Entwickler und Leiter von Geschäftsbereichen, wobei genügend Ressourcen für Privacy-Management usw. bereitzustellen sind;
- Festlegung von für die betroffenen Personen transparenten Verfahren für die Bearbeitung von Anträgen auf Zugang, Berichtigung und Löschung;
- Einrichtung eines internen Beschwerdebearbeitungssystems;
- Festlegung interner Verfahren zur effektiven Handhabung und Meldung von Sicherheitsverstößen;
- Durchführung von Datenschutzverträglichkeitsprüfungen unter bestimmten Umständen;
- Einführung und Überwachung von Kontrollverfahren, die gewährleisten, dass die Maßnahmen nicht nur auf dem Papier bestehen, sondern in der Praxis angewandt werden und funktionieren (interne oder externe Audits usw.).

42. Vorstellbar wäre auch ein ergänzender Ansatz zum allgemeinen Grundsatz der Rechenschaftspflicht. Dabei würde der Rechtsrahmen nicht nur einen allgemeinen Grundsatz der Rechenschaftspflicht, sondern auch eine beispielhafte Liste von Maßnahmen, die auf Ebene der Mitgliedstaaten gefördert werden können, enthalten.[7] Eine solche beispielhafte und nicht erschöpfende Liste könnte den für

---

[7] So enthalten etwa die in Madrid von den Datenschutzbehörden angenommenen Internationalen Standards in Artikel 22 Bestimmungen über proaktive Maßnahmen mit folgendem Wortlaut: *„Die Staaten müssen über ihr innerstaatliches Recht Anreize für Maßnahmen schaffen, die eine bessere Einhaltung der Gesetzgebung zum Datenschutz durch diejenigen fördern, die an den unterschiedlichen Verarbeitungsschritten beteiligt sind. Zu diesen Maßnahmen können unter anderem Folgende zählen:*

a) Die Einführung von Verfahren zur Vorbeugung und Feststellung von Verstößen, die auf standardisierten Modellen zur Steuerung und/oder für das Management der Informationssicherheit beruhen.

b) Die Ernennung eines oder mehrerer Beauftragter für den Schutz der Privatsphäre oder des Datenschutzes, die für die Wahrnehmung ihrer Aufsichtsfunktionen über ausreichende Qualifikationen, Ressourcen und Kompetenzen verfügen müssen.

c) Die regelmäßige Durchführung von Programmen zur Bewusstseinsbildung, Aus- und Weiterbildung der Mitglieder der Organisation zur Verbesserung ihrer Kenntnisse der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren.

d) Die regelmäßige Durchführung von transparenten Audits durch qualifizierte und vorzugsweise unabhängige Personen, bei denen die Einhaltung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren geprüft wird.

e) Die Anpassung der Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, an die auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung, insbesondere wenn es darum geht, Entscheidungen über technische Merkmale, die technische Entwicklung und Implementierung zu treffen.

f) Die Praxisumsetzung von Datenschutz-Folgenabschätzungen vor der Implementierung neuer Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, sowie die Praxisumsetzung neuer Arten der Verarbeitung personenbezogener Daten vor der Einführung wesentlicher Veränderungen der Verarbeitungspraxis.

g) Die Annahme von Verhaltensregeln, deren Einhaltung verpflichtend ist und die es ermöglichen, ihre Wirksamkeit in Bezug auf die Befolgung und den Grad des Schutzes der personenbezogenen Daten zu messen und die wirkungsvolle Maßnahmen im Fall der Nichterfüllung festlegen.

die Verarbeitung Verantwortlichen als „Instrumentarium“ dienen, das ihnen dabei hilft, im jeweiligen Einzelfall zu entscheiden, welche Maßnahmen als geeignet gelten können. Diese beispielhafte Liste würde die grundsätzliche rechtliche Verpflichtung, geeignete Maßnahmen zu treffen, natürlich nur begleiten.

Anpassung der Maßnahmen

43. Die für die Verarbeitung Verantwortlichen können die vorstehenden beispielhaften Maßnahmen ergreifen, um den ersten Teil des Grundsatzes der Rechenschaftspflicht *(der für die Verarbeitung Verantwortliche trifft geeignete und wirksame Maßnahmen, die die Einhaltung der in der Richtlinie festgelegten Grundsätze und Verpflichtungen gewährleisten)* zu erfüllen.

44. Einige davon sind grundlegende Maßnahmen, die bei den meisten Datenverarbeitungsvorgängen durchzuführen sind. Bei manchen Verarbeitungen können interne Strategien und Verfahren zur Umsetzung der Grundsätze (etwa Verfahren zur Bearbeitung von Zugangsanträgen oder Beschwerden) geeignete Maßnahmen darstellen. Inwieweit bestimmte Maßnahmen geeignet sind, ist von Fall zu Fall zu entscheiden. Diese Entscheidungen obliegen den für die Verarbeitung Verantwortlichen, wobei Anleitungen der einzelstaatlichen Datenschutzbehörden und der Artikel-29-Datenschutzgruppe (siehe unten), soweit verfügbar, zu beachten sind.

45. Aus den vorstehenden Ausführungen ist ersichtlich, dass es, wenn es darum geht, die Arten der zu ergreifenden Maßnahmen festzulegen, keine Wahlmöglichkeiten, sondern nur maßgeschneiderte Lösungen gibt. Welche konkreten Maßnahmen durchzuführen sind, ist in jedem einzelnen Fall nach den jeweiligen Gegebenheiten und Umständen unter besonderer Berücksichtigung der mit der Verarbeitung verbundenen Risiken und der Art der Daten zu bestimmen. Eine Einheitslösung würde die für die Verarbeitung Verantwortlichen nur in unpassende und letztendlich zum Scheitern verurteilte Strukturen zwängen.

46. Die für die Verarbeitung Verantwortlichen müssen in der Lage sein, die Maßnahmen an ihre eigenen Gegebenheiten und die Besonderheiten der jeweiligen Datenverarbeitungsvorgänge anzupassen. In diesem Zusammenhang erinnert die Artikel-29-Datenschutzgruppe an die zur Bestimmung der Art der durchzuführenden Sicherheitsmaßnahmen in Artikel 17 der geltenden Richtlinie festgelegten Kriterien[8], nämlich die von der Verarbeitung ausgehenden Risiken und die Art der Daten. Diese beiden Kriterien könnten ebenfalls verwendet werden, um die grundlegenden Arten der anzuwendenden Maßnahmen zu bestimmen. Wie hoch das Risiko ist, lässt sich etwas konkreter anhand des Umfangs der Datenverarbeitungsvorgänge, des Zwecks der Verarbeitung und der Zahl der vorgesehenen Datenübertragungen bestimmen. Berücksichtigt werden

---

h) Die Einführung von Eventualfallplänen, die Handlungsanweisungen für den Fall festlegen, dass eine Nichtbefolgung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung festgestellt wird, und die zumindest die Verpflichtung enthalten, die Ursache und Reichweite der eingetretenen Vorschriftsverletzung zu bestimmen, ihre negativen Auswirkungen zu beschreiben und die erforderlichen Maßnahmen zu ergreifen, damit das zukünftig nicht noch einmal geschieht.“

8 *„Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“*

sollte auch die Art der Daten, und ob es sich um sensible Daten handelt oder nicht. Im Zusammenhang mit dem Grundsatz der Rechenschaftspflicht wäre möglicherweise auch darüber nachzudenken, ob dem Auftragsverarbeiter oder den Entwicklern und/oder Herstellern von IKT (Informations- und Kommunikationstechnologien) bestimmte Verpflichtungen auferlegt werden sollten.

47. Große für die Verarbeitung Verantwortliche sollten grundsätzlich strenge Maßnahmen treffen, die diesen Kriterien entsprechen. In manchen Fällen kann es auch erforderlich sein, dass kleine oder mittlere für die Verarbeitung Verantwortliche, etwa wenn sie mit hohen Risiken verbundene Datenverarbeitungsvorgänge durchführen (z. B. bei bestimmten Verarbeitungen im Bereich der elektronischen Gesundheitsdienste), rigorose Sicherheitsmaßnahmen einführen. So brauchen etwa eine Kommunalverwaltung (Rathaus), ein multinationaler Konzern, ein Kleinunternehmen (Internet), eine Organisation, deren Kernaktivität die Datenverarbeitung ist, oder ein Unternehmen, das bereits früher gegen Rechtsvorschriften verstoßen hat, jeweils ganz spezifische Maßnahmen, um ein glaubwürdiges und effektives Datenmanagement zu gewährleisten. Der im zweiten Teil des Grundsatzes der Rechenschaftspflicht enthaltenen Nachweispflicht ließe sich daher in einfachen Fällen wie z. B. der Verarbeitung personenbezogener Daten der Belegschaft zur Erstellung eines Personalverzeichnisses leicht nachkommen (beispielsweise durch die verwendeten Bekanntmachungen, die Beschreibung der grundlegenden Sicherheitsmaßnahmen usw.). In komplexeren Fällen wie etwa der Verwendung innovativer biometrischer Geräte, können zur Erfüllung der Nachweispflicht weitere Schritte notwendig sein. Der für die Verarbeitung Verantwortliche könnte z. B. nachweisen, dass er eine Datenschutzverträglichkeitsprüfung durchgeführt hat, dass die beteiligten Mitarbeiter regelmäßig geschult und unterrichtet werden usw.

48. Transparenz ist ein wesentlicher Bestandteil vieler Maßnahmen im Zusammenhang mit der Rechenschaftspflicht. Transparenz gegenüber den betroffenen Personen und der Öffentlichkeit dazu bei, dass die für die Verarbeitung Verantwortlichen ihrer Rechenschaftspflicht besser nachkommen können. So kann etwa durch die Veröffentlichung von Datenschutzerklärungen im Internet, Transparenz in Bezug auf interne Beschwerdeverfahren und die Veröffentlichung in Jahresberichten der Rechenschaftspflicht in größerem Maße Rechnung getragen werden.

Anleitung und Rechtssicherheit

49. Während die Notwendigkeit der Anpassbarkeit und somit Flexibilität eher für die Verwendung eines allgemein gefassten Wortlauts spricht, ist sich die Artikel-29-Datenschutzgruppe darüber im Klaren, dass eine derart allgemein gehaltene Regelung mit Raum für Flexibilität und Anpassung auch zu Unsicherheit führen kann. Die für die Verarbeitung Verantwortlichen werden möglicherweise einwenden, dass die Regelung nicht detailliert genug ist und daher keine Rechtssicherheit bietet. So könnte etwa Unsicherheit darüber bestehen, wie detailliert Datenschutzerklärungen oder -verfahren sein sollen, wann und wie ein Datenschutzbeauftragter zu bestellen ist, wann Schulungen durchzuführen sind

usw. Weiterhin könnte die Art der gegebenenfalls erforderlichen Überprüfung (extern oder intern) unklar sein. Zudem könnten die für die Verarbeitung Verantwortlichen befürchten, unterschiedlichen und willkürlichen Auslegungen der Mitgliedstaaten in Bezug auf Umfang und Art ihrer Pflichten ausgesetzt zu sein.

50. Die Artikel-29-Datenschutzgruppe kann diese Besorgnisse nachvollziehen. Jedoch lässt sich aus den oben genannten Gründen (notwendige Flexibilität und Anpassbarkeit) Rechtssicherheit nicht durch die Richtlinie selbst erreichen. Die Artikel-29-Datenschutzgruppe hält eine von der Kommission (z. B. in Form praktischer Durchführungsbestimmungen) und/oder der Artikel-29-Datenschutzgruppe herausgegebene und der Harmonisierung dienende Anleitung für ein geeignetes Instrument, um mehr Sicherheit zu schaffen und mögliche Unterschiede bei der Umsetzung auszuräumen.[9] Die Artikel-29-Datenschutzgruppe könnte auch eine allgemeine Anleitung erarbeiten, welche die von den für die Verarbeitung Verantwortlichen in der Regel benötigten grundlegenden Elemente enthält und sich im Einzelfall an die spezifischen Erfordernisse des für die Verarbeitung Verantwortlichen anpassen lässt.

51. Sinnvoll wäre möglicherweise auch, wie bereits bei der von der Artikel-29-Datenschutzgruppe erstellten Anleitung für BCR[10] geschehen, die Erarbeitung eines *Musterprogramms für Datenschutz-Compliance*, das mittlere und große für die Verarbeitung Verantwortliche als Grundlage für ihre jeweiligen Programme verwenden könnten. Diese Muster sollten nach sorgfältiger Überprüfung der derzeit gängigen Praxis und verfügbarer Muster sowie Konsultation mit allen einschlägigen Beteiligten erarbeitet werden. Dies ist ein Bereich, dem sich alle Beteiligten ernsthaft zuwenden sollten.

Wirksamkeit der Maßnahmen

52. Die bereits in Bezug auf geeignete Maßnahmen erörterten Fragen treten auch auf, wenn es um die Gewährleistung der Wirksamkeit von Maßnahmen geht. Je nach Art der Datenverarbeitung kann die Wirksamkeit auf unterschiedliche Weise gewährleistet werden.

53. Die für die Verarbeitung Verantwortlichen haben viele verschiedene Möglichkeiten, die Wirksamkeit (oder Unwirksamkeit) der Maßnahmen zu beurteilen. Bei umfangreichen, komplexen oder mit hohen Risiken behafteten Datenverarbeitungsvorgängen sind interne und externe Audits gängige Überprüfungsmethoden. Auch die Art und Weise, in der die Audits durchgeführt werden, kann variieren – von vollständigen Prüfungen bis hin zu Negativprüfungen (bei denen ebenfalls unterschiedliche Formen möglich sind).

---

9 Ein Beispiel für eine solche Anleitung ist das vom kanadischen Datenschutzbeauftragten veröffentlichte PIPEDA Self-Assessment Tool, das mittleren und großen für die Verarbeitung Verantwortlichen dabei helfen soll, ein sinnvolles Datenschutzmanagement zu entwickeln und umzusetzen. Dieses Tool ist abrufbar unter: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf.

10 Arbeitsdokument WP 153 der Artikel-29-Datenschutzgruppe mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) und Arbeitsdokument WP 154 „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)".

Die Artikel-29-Datenschutzgruppe regt an, für Entscheidungen darüber, wie die Wirksamkeit der Maßnahmen gewährleistet werden soll, dieselben Kriterien wie bei Entscheidungen über die Maßnahmen selbst anzuwenden. Diese Kriterien ergeben sich aus Artikel 17 der Richtlinie 95/46/EG (von der Verarbeitung ausgehende Risiken und der Art der Daten). Wie ein für die Verarbeitung Verantwortlicher die Wirksamkeit der Maßnahmen zu gewährleisten hat, richtet sich also nach der Sensibilität der Daten, der Menge der verarbeiteten Daten und den mit der Datenverarbeitung verbundenen besonderen Risiken. Die von der Artikel-29-Datenschutzgruppe gegebenenfalls zu erarbeitende Anleitung kann auch diesen Aspekt mit einschließen.

IV.3 Verbindung mit anderen Anforderungen

Vorherige Meldungen

54. Es könnte darüber nachgedacht werden, wie sich geeignete Sicherheitsmaßnahmen auf der Ebene der für die Verarbeitung Verantwortlichen möglicherweise auf die vorherigen Meldungen auswirken. Wie von der Artikel-29-Datenschutzgruppe bereits in ihrer Stellungnahme zur Zukunft des Datenschutzes angeregt, wäre vorstellbar, dass bestimmte Mechanismen im Zusammenhang mit der Rechenschaftspflicht die Verwaltungsanforderungen nach den geltenden Rechtsvorschriften zum Datenschutz ersetzen oder mindern.

Internationale Datenübertragungen

55. Verbindliche unternehmensinterne Datenschutzregelungen sind ein Beispiel dafür, wie Grundsätze des Datenschutzes nach dem Grundsatz der Rechenschaftspflicht umgesetzt werden können. Sie stellen eine von der Artikel-29-Datenschutzgruppe aufgezeigte und akzeptierte Möglichkeit dar, Datenübertragungen in Drittländer auf angemessene Weise zu schützen.

56. In diesem Bereich wären im Zusammenhang mit der Überarbeitung der Richtlinie 95/46/EG weitere Analysen sinnvoll. Dabei wäre es besonders wichtig zu überlegen, ob verbindliche unternehmensinterne Datenschutzregelungen und letztendlich andere ähnlich verbindliche Mechanismen im Zusammenhang mit der Rechenschaftspflicht nach Artikel 26 Absatz 2 der Richtlinie *(kann ein Mitgliedstaat eine Übermittlung … genehmigen …, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien … bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben)* in vollem Umfang als Instrumente, die ausreichende Garantien bieten, gelten können.

57. In diesem Zusammenhang sollten unter anderem unbedingt die Mechanismen, die die für die Verarbeitung Verantwortlichen intern zur Umsetzung der Grundsätze des Datenschutzes und Erfüllung der Verpflichtungen verwenden, sowie die Systeme zu ihrer Überprüfung, beurteilt werden. Sachdienlich wäre ferner eine Diskussion über die Mechanismen zur Rationalisierung des derzeitigen auf Genehmigungen von Datenübertragungen durch die Datenschutzbehörden der Mitgliedstaaten beruhenden Systems.

IV.4 Die Rolle der Datenschutzbehörden

58. Es stellt sich die Frage, ob sich der in dieser Stellungnahme vorgeschlagene Grundsatz der Rechenschaftspflicht auf die Befugnisse der Datenschutzbehörden, insbesondere bei der Durchsetzung der Rechtsvorschriften, auswirkt. Wie nachstehend erläutert, schränkt der Grundsatz die Befugnisse der Datenschutzbehörden in keiner Weise ein, sondern bringt den Behörden vielmehr Vorteile.

59. Was die Rechtsdurchsetzung anbelangt, so sind die Datenschutzbehörden dem vorgeschlagenen Grundsatz zufolge berechtigt, von dem für die Verarbeitung Verantwortlichen einen Nachweis der Einhaltung des Grundsatzes der Rechenschaftspflicht zu verlangen. Dies stärkt die Rechtsdurchsetzung seitens der Behörden und gewährleistet, dass die Behörden auch weiterhin jederzeit zu Durchsetzungsmaßnahmen befugt sind. Hervorzuheben ist, dass die Datenschutzbehörden in jedem Fall nicht nur für die Überwachung der von den für die Verarbeitung Verantwortlichen getroffenen Maßnahmen, sondern vor allen Dingen für die Überwachung der Einhaltung der Grundprinzipien und Verpflichtungen zuständig bleiben.

60. Außerdem erhalten die Datenschutzbehörden durch die Verwirklichung des Grundsatzes der Rechenschaftspflicht wertvolle Informationen für die Überwachung der Einhaltung. Da ja die für die Verarbeitung Verantwortlichen in der Lage sein müssen, gegenüber den Behörden nachzuweisen, ob und wie sie die Maßnahmen durchgeführt haben, würden den Behörden sehr wichtige Informationen zur Einhaltung der Vorschriften zur Verfügung stehen, die sie im Rahmen ihrer Durchsetzungsmaßnahmen nutzen können. Zudem haben die Datenschutzbehörden, sofern die verlangten Informationen nicht zur Verfügung gestellt werden, einen unmittelbaren Grund, unabhängig von der mutmaßlichen Verletzung der betreffenden Grundsätze des Datenschutzes gegen die für die Verarbeitung Verantwortlichen vorzugehen.

61. Der Grundsatz ermöglicht den Datenschutzbehörden auch ein stärker selektives und strategisches Vorgehen, weil sie ihre Ressourcen so einsetzen können, dass das größtmögliche Maß an Einhaltung erreicht wird.

62. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass der Grundsatz der Rechenschaftspflicht zur Entwicklung des juristischen und technischen Fachwissens im Bereich der Umsetzung von Datenschutzvorschriften beitragen kann. Hier werden Experten mit fundierten technischen und juristischen Kenntnissen auf dem Gebiet des Datenschutzes, mit Kommunikationsfähigkeiten und Kompetenzen in der Mitarbeiterschulung, der Aufstellung und Umsetzung von Strategien und auf dem Gebiet der Audits unentbehrlich sein. Dieses Fachwissen wird sowohl unternehmensintern als auch in Form externer entgeltlicher Unternehmensdienstleistungen erforderlich sein. Mit dieser unerlässlichen Entwicklung wird gewährleistet, dass die für die Verarbeitung Verantwortlichen ihren Pflichten nachkommen und gegebenenfalls interne und externe Audits durchführen lassen können. Gleichzeitig kommt die Entwicklung auch den Datenschutzbehörden zugute, weil das System zur Einhaltung der Vorschriften insgesamt beiträgt, den Behörden mehr fundierte Informationen über

die internen Abläufe von Unternehmen zur Verfügung stehen und die Herausbildung eines Pools von Datenschutzexperten mit fundierten Fachkenntnissen und Fähigkeiten zweifelsohne die Zusammenarbeit mit den für die Verarbeitung Verantwortlichen erleichtert.

63. Daraus lässt sich ableiten, dass die Datenschutzbehörden eher im Nachhinein als vorab tätig werden. Weil im Rahmen der Rechenschaftspflicht Wert auf bestimmte zu erreichende Resultate (etwa ein gutes Datenschutzmanagement) gelegt wird, ist sie eher ergebnisorientiert und schwerpunktmäßig auf nachträgliche Maßnahmen (nach Beginn der Datenverarbeitung) ausgerichtet.

IV.5 Sanktionen

64. Das vorgeschlagene System kann nur dann funktionieren, wenn die Datenschutzbehörden befugt sind, wirkungsvolle Sanktionen zu verhängen. Solche Sanktionen sind insbesondere dann notwendig, wenn für die Verarbeitung Verantwortliche den Grundsatz der Rechenschaftspflicht verletzen. Beispielsweise sollten Verstöße von für die Verarbeitung Verantwortlichen gegen Verpflichtungen in verbindlichen internen Strategien geahndet werden. Dies erweitert offensichtlich den Tatbestand der Zuwiderhandlung gegen wesentliche Grundsätze des Datenschutzes.

65. Darüber hinaus sollten die Datenschutzbehörden der Mitgliedstaaten nach Ansicht der Artikel-29-Datenschutzgruppe befugt sein, den für die Verarbeitung Verantwortlichen genaue Weisungen in Bezug auf ihre Compliance-Systeme zu erteilen.

IV.6 Die Entwicklung von Zertifizierungssystemen

66. Langfristig kann die Regelung zur Rechenschaftspflicht die Entwicklung von Zertifizierungsprogrammen oder Gütesiegeln unterstützen. Solche Programme würden den Nachweis erleichtern, dass der für die Verarbeitung Verantwortliche den Grundsatz erfüllt, also geeignete Maßnahmen getroffen und durchgeführt hat, die regelmäßig überprüft werden. Zu dieser Entwicklung können mehrere Faktoren beitragen:

67. Grundsätzlich ist zu erwarten, dass Dienstleister in den Bereichen Datenschutz, Audits oder Datenschutzverträglichkeitsprüfungen, in zunehmendem Maße Zertifikate und Gütesiegel anbieten werden, um sich im Markt abzuheben und Wettbewerbsvorteile zu verschaffen. Die für die Verarbeitung Verantwortlichen können sich dann nach eigenem Ermessen von vertrauenswürdigen Dienstleistern zertifizieren lassen. Wenn bekannt wird, dass bestimmte Gütesiegel mit strengen Prüfungen verbunden sind, werden die für die Verarbeitung Verantwortlichen diese wahrscheinlich bevorzugen, weil sie neben Wettbewerbsvorteilen auch mehr Compliance-Sicherheit bieten.

68. Wenn für die Verarbeitung Verantwortliche BCR als Rechtsgrundlage für Datenübertragungen in Drittländer verwenden wollen, müssen sie nachweisen, dass sie ausreichende Sicherheitsmaßnahmen getroffen haben. In diesem Fall können die Datenschutzbehörden die Übertragungen genehmigen. Dies ist ein

Bereich, in dem Zertifizierungsdienste hilfreich sein könnten. Die Dienstleister würden die Sicherheitsmaßnahmen des für die Verarbeitung Verantwortlichen analysieren und, falls sie ausreichen, das entsprechende Gütesiegel erteilen. Wenn die Datenschutzbehörde prüft, ob der für die Verarbeitung Verantwortliche in den BCR ausreichende Garantien für die Sicherheit von Datenübertragungen in Drittländer bietet, könnte sie sich an die im Rahmen eines bestimmten Zertifizierungsprogramms erteilte Zertifizierung halten, was wiederum zu einer Rationalisierung des Genehmigungsverfahrens für solche Datenübertragungen beitragen würde.

IV.6 Die Regulierung von Zertifizierungssystemen

69. Aus denselben Gründen, die für die Entwicklung von Zertifizierungsdiensten sprechen, sollten diese Dienste auch reglementiert werden, denn wenn sie die Einhaltung von Datenschutzvorschriften (gegenüber Datenschutzbehörden, den für die Verarbeitung Verantwortlichen und dem Verbraucher) zuverlässig nachweisen und im Binnenmarkt reibungslos funktionieren sollen, werden Vorschriften für die Erbringung dieser Dienstleistungen wohl unumgänglich sein. Die Datenschutzbehörden sollten bei der Erarbeitung dieser Vorschriften eine Schlüsselrolle übernehmen (Verweise, Muster usw.) und in der Lage sein, ihre Anwendung durchzusetzen. Dazu müssen sie auch mit ausreichenden Mitteln ausgestattet sein. Außerdem sollten die Datenschutzbehörden in die Akkreditierung der Zertifizierungsstellen einbezogen werden. Dies kann im Bereich der grenzüberschreitenden Datenübertragungen von besonderer Bedeutung sein. Da die Qualität der Dienstleistungen und ihr Funktionieren im Binnenmarkt Schlüsselkriterien sind, muss der Gesetzgeber die Voraussetzungen schaffen, um diese Qualität erreichen zu können. Dies dem Markt zu überlassen scheint nicht möglich zu sein. Erfahrungen in anderen Bereichen wie der Zertifizierung von Gütern waren tendenziell negativ. Wettbewerb zwischen Dienstleistern kann zu sinkenden Preisen und auch zu einer gewissen Flexibilität oder Lockerung der Verfahren führen. Unabhängig davon, ob es um grenzüberschreitende Datenübertragungen geht oder nicht, scheinen also Vorschriften notwendig, um eine hohe Dienstleistungsqualität und gleiche Bedingungen für alle zu gewährleisten.

70. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass bestehende Akkreditierungsvorschriften[11] unter Umständen auch auf Zertifizierungsdienste im Bereich des Datenschutzes angewandt werden können. Diese Rechtsvorschriften enthalten bereits die zur Regelung der Organisation und der Arbeit von Akkreditierungsstellen erforderliche Struktur und gelten für freiwillige sowie in bestimmten Fällen auch für obligatorische Akkreditierungen.

[11] Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates.

71. Derartige Dienstleistungen würden sicherlich auch die Harmonisierung der Standards, an denen Unternehmen zu messen wären, voranbringen. Die erwähnte Anleitung (seitens der Artikel-29-Datenschutzgruppe oder der Kommission) mit Musterprogrammen für die Datenschutz-Compliance wäre hier von großer Bedeutung.

V. FAZIT

72. Die Entwicklung neuer Technologien und die anhaltende Globalisierung von Wirtschaft und Gesellschaft haben dazu geführt, dass die Menge der gesammelten, ausgewerteten, übertragenen oder anderweitig aufbewahrten personenbezogenen Daten stark zugenommen hat. Damit vervielfältigen sich die Gefahren, denen diese Daten ausgesetzt sind.

73. Die Artikel-29-Datenschutzgruppe ist davon überzeugt, dass der steigende Wert personenbezogener Daten und die Zunahme der damit verbundenen Gefahren an sich schon Grund genug sind, die Rolle und die Verantwortung der für die Verarbeitung Verantwortlichen zu stärken. Ein Rechtsrahmen, der diesen neuen Gegebenheiten Rechnung trägt, muss die für die Verarbeitung Verantwortlichen mit den entsprechenden Instrumenten dazu ermuntern, geeignete und wirksame Maßnahmen zur Umsetzung der Grundsätze des Datenschutzes in der Praxis anzuwenden. Beispiele für solche Maßnahmen sind die Gewährleistung der Erkennung sämtlicher Datenverarbeitungsvorgänge, die Beantwortung von Zugangsanträgen, die Zuteilung von Ressourcen einschließlich der Benennung der für die Organisation der Einhaltung der Datenschutzvorschriften zuständigen Personen.

74. Zur Stärkung des Datenschutzes in der Praxis schlägt die Artikel-29-Datenschutzgruppe vor, in die Vorschläge zur Änderung der Datenschutzrichtlinie zunächst eine neue Vorschrift aufzunehmen, die die für die Verarbeitung Verantwortlichen verpflichtet, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Richtlinie umzusetzen, und dies auf Verlangen nachzuweisen. Diese Maßnahmen sollten die Einhaltung der Grundsätze des Datenschutzes und der damit verbundenen Verpflichtungen fördern und gleichzeitig die Gefahr des unbefugten Zugriffs, Missbrauchs, Verlustes usw. auf ein Minimum reduzieren. Die Pflicht, das Ergreifen der notwendigen Maßnahmen auf Verlangen nachzuweisen, dürfte den Datenschutzbehörden ein nützliches Instrument für die Durchsetzung der Rechtsvorschriften an die Hand geben.

75. Zur Durchführung dieser Maßnahmen sollten die für die Verarbeitung Verantwortlichen in allen Bereichen des öffentlichen und privaten Sektors verpflichtet werden. Außerdem müssen die Maßnahmen so anpassbar sein, dass sie den von der Verarbeitung ausgehenden Risiken und der Art der Daten entsprechen können.

Brüssel, den 13. Juli 2010

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM