Dokumente
zu Datenschutz
und Informationsfreiheit
2006

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
An der Urania 4 – 10
10787 Berlin
Telefon: 0 30/1 38 89-0
Telefax: 0 30/2 15 50 50
E-Mail:mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Stand: Januar 2007

Inhaltsverzeichnis

Vorwort

Seit 1998 haben die Datenschutzbeauftragten Berlins und Brandenburgs gemeinsam diese Schriftenreihe „Dokumente zu Datenschutz und Informationsfreiheit“ herausgegeben, um die wichtigsten Ergebnisse der Zusammenarbeit auf nationaler, europäischer und globaler Ebene auch unabhängig von den Jahres- und Tätigkeitsberichten in gedruckter Form verfügbar zu machen. Es gibt in der Bundesrepublik keine vergleichbare Textsammlung mit den Stellungnahmen zu den wichtigsten aktuellen Problemen des Datenschutzes und der Informationsfreiheit.

Dieser Dokumentenband ist stets gemeinsam mit dem jeweiligen Jahres- und Tätigkeitsbericht veröffentlicht worden. Nachdem das Land Brandenburg zu einem zweijährlichen Berichtsrhythmus bei den Tätigkeitsberichten der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht übergegangen ist, ergab sich die Schwierigkeit der Synchronisation zwischen Brandenburg und Berlin, wo der Berliner Beauftragte für Datenschutz und Informationsfreiheit nach wie vor einen „Jahresbericht“ vorlegt. Wir haben uns daher entschlossen, die „Dokumente zu Datenschutz und Informationsfreiheit“ künftig als alleinige Herausgeber weiter zu veröffentlichen.

Der vorliegende Band enthält neben den Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstmals auch Beschlüsse des sog. Düsseldorfer Kreises, des Koordinationsgremiums der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Dieses Gremium geht erst neuerdings dazu über, seine Stellungnahmen zum Datenschutz in der Wirtschaft stärker öffentlich zu machen, was aus Gründen der Transparenz ebenso wie unter datenschutzpolitischen Gesichtspunkten zu begrüßen ist. Es ist zu hoffen, dass in nicht allzu ferner Zukunft die bereits 1998 von den Herausgebern dieser Dokumente beklagte Zersplitterung in der Zuständigkeit der Datenschutzaufsicht dadurch beseitigt wird, dass diese in allen Bundesländern bei den Landesbeauftragten für den Datenschutz konzentriert wird. Damit würde auch der länderübergreifende Koordinationsaufwand in zwei entsprechenden Gremien (Datenschutzkonferenz und Düsseldorfer Kreis) wegfallen.

Die Aufsichtsbehörden mussten sich sowohl in Deutschland als auch in Europa mit gleich gelagerten Fragestellungen wie etwa der Datenverarbeitung bei SWIFT auseinandersetzen. Auf die dort festgestellten massiven Datenschutzverstöße können die nationalen Aufsichtsbehörden nur gemeinsam reagieren. Die Artikel-29-Datenschutzgruppe der europäischen Datenschutzkontrollstellen hat darüber hinaus eine Vielzahl von Arbeitspapieren beschlossen, von denen nur die drei wichtigsten in diese Veröffentlichung aufgenommen wurden. Die Entschließungen und Stellungnahmen der übrigen Gremien (der Europäischen und Inter-

nationalen Datenschutzkonferenzen sowie der unter Berliner Vorsitz tagenden Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation) sind dagegen vollständig wiedergegeben.

Die Informationsfreiheitsbeauftragten haben im zurückliegenden Jahr erhebliche Verstärkung erhalten: Seit Anfang 2006 gibt es einen Bundesbeauftragten für die Informationsfreiheit, der in den letzten zwölf Monaten auch die länderübergreifende Zusammenarbeit koordiniert hat. Außerdem haben die Länder Bremen, Mecklenburg-Vorpommern und das Saarland – dem Beispiel der bisherigen Informationsfreiheitsgesetze des Bundes und der Länder folgend – den jeweiligen Landesdatenschutzbeauftragten auch die Funktion eines Beauftragten für die Informationsfreiheit übertragen. Die Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland – das Gremium wird künftig als „Konferenz der Informationsfreiheitsbeauftragten“ zusammentreten – sind ebenfalls in diesem Band abgedruckt.

Dr. Alexander Dix

A Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 71. Konferenz vom 16./17. März 2006 in Magdeburg

Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat*. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u. a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die

* KOM (2005) 475 vom 4. Oktober 2005

Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt – einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte – Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen

Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung wirtschaftlicher Interessen – zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkun-

gen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z. B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche

Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

2. Entschließung zwischen der 71. und 72. Konferenz vom 11. Oktober 2006

(bei Enthaltung von Schleswig-Holstein)

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispiels-

weise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

3. Entschließungen der 72. Konferenz vom 26./27. Oktober 2006 in Naumburg

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes“ kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes“ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat – sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z. B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- **Transparenz**
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

- **Kennzeichnungspflicht**
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

- **Keine heimliche Profilbildung**
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- **Vermeidung der unbefugten Kenntnisnahme**
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

- **Deaktivierung**
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben“ ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kinder-

garten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen „Bildungsregisters“ nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

– Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

– Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

– Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Beschlüsse der Sitzung am 8./9. November 2006 in Bremen

Nutzung von Daten aus dem Inkasso-Bereich für die Auskunftserteilung

Eine generelle Übermittlung von weichen Negativdaten aus dem Inkassobereich für die Auskunftserteilung auf Grund entgegenstehender überwiegender schutzwürdiger Interessen des Betroffenen ist nicht zulässig.

Kann jedoch nach sorgfältiger Einzelfallabwägung die Zahlungsunfähigkeit oder Zahlungsunwilligkeit zweifelsfrei festgestellt werden, d. h. besteht kein Grund zur Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, wird eine Übermittlung unter den folgenden Voraussetzungen als zulässig angesehen.

1. Es muss sich um eine unbestrittene Forderung handeln.

2. Sowohl Gläubiger als auch Inkassounternehmen haben die der Einmeldung zugrunde liegende Forderung gegenüber dem Schuldner nachweisbar jeweils mindestens zweimal vergeblich schriftlich gemahnt.

3. Der Schuldner wird (z. B. in den Mahnschreiben) darüber informiert, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt.[1]

4. Die Einmeldung erfolgt frühestens dann, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungs- bzw. Rückantwortfrist von zehn Tagen verstrichen sind.[2]

SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort

[1] Bei der Formulierung der Information an den Schuldner hat das Inkassobüro im eigenen Interesse darauf zu achten, dass dabei die strafrechtlichen Grenzen einer Nötigung [§ 240 StGB] nicht überschritten werden. Vielmehr sollte dem Betroffenen vermittelt werden, dass ihm mit dieser Information die Möglichkeit gegeben wird, vor einer Einmeldung Stellung zu nehmen.

[2] Damit hätte der Schuldner über dem gesamten Zeitraum von zehn Tagen die Gelegenheit zur Zahlung bzw. Äußerung sowie der Gläubiger die gesicherte Kenntnis über den erfolgten bzw. nicht erfolgten Zahlungseingang

gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich:

Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – zum Beispiel mit Hilfe von Hintergrundsystemen – später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird – insbesondere wegen der geringen Größe der RFID-Chips – künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz / Benachrichtigungspflicht
Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht
Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken“ der Betroffenen darf es nicht geben.

Deaktivierung
Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit
Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Ver-

schlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung
Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

Benachrichtigung Dritter bei der Einmeldung in die Warn- und Hinweissysteme der Versicherungen (HIS)

Nach § 33 Abs. 1 Bundesdatenschutzgesetz (BDSG) besteht eine Benachrichtigungspflicht gegenüber Betroffenen. Soweit Versicherungen Daten von Zeugen, Sachverständigen, Gutachtern und sonstigen Dritten speichern, gilt diese gesetzlich geregelte Benachrichtigungspflicht. Die Ausnahmen gemäß § 33 Abs. 2 BDSG sind restriktiv auszulegen und lediglich in besonders gelagerten Einzelfällen gegeben.

Die Übermittlung personenbezogener Daten von Dritten an andere Versicherungen oder ihre Einmeldung in zentrale Warn- und Hinweissysteme setzt auf der Grundlage der §§ 28 und 29 BDSG eine Abwägung der berechtigten Interessen der Versicherung mit den schutzwürdigen Interessen der Betroffenen voraus. Eine Beeinträchtigung schutzwürdiger Belange ist jedenfalls dann anzunehmen, wenn die Übermittlung von Daten der Dritten an eine Vielzahl von angeschlossenen Versicherungen erfolgt, ohne dass diese Dritten zuvor informiert worden sind.

Selektion von Kundendaten für Werbezwecke oder Markt- und Meinungsforschung; listenmäßige Übermittlung nach § 28 Abs. 3 S. 1 Nr. 3 Bundesdatenschutzgesetz

Im Rahmen der Auslegung des § 28 Abs. 3 S. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG) stellt sich bei der Erstellung von Adresslisten für Werbezwecke oder Markt- und Meinungsforschung mit Gruppenmerkmalen oft die Frage, welchen Inhalt das aufgeführte Listendatum „eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe“ nach dieser Vorschrift haben darf.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

1. Nach § 28 Abs. 3 S. 1 Nr. 3a BDSG darf nur eine Angabe über die Zugehörigkeit der betroffenen Person zu dieser Personengruppe für Zwecke der Werbung oder der Markt- und Meinungsforschung übermittelt oder genutzt werden.

2. Die Konkretisierung eines ausgewählten Gruppenmerkmals darf nur so weit erfolgen, dass das Merkmal zwar die zu Zwecken der Werbung und der Markt- und Meinungsforschung geeignete Aussagekraft besitzt, aber kein Gruppenprofil darstellt. In jedem Fall dürfen über die eine Angabe hinaus keine anderen Merkmale gleichzeitig versteckt mitverwertet werden.

Soweit zur Selektion von Adressdaten mehr als ein Gruppenmerkmal im Sinne des § 28 Abs. 3 S. 1 Nr. 3a BDSG für Werbezwecke oder Markt- und Meinungsforschung genutzt oder übermittelt wird, bedarf es der Einwilligung der Betroffenen. Dies gilt auch bei der Kombination verschiedener Merkmale zur Bildung eines neuen und weiter reichenden Gruppenmerkmals.

III. Europäische Konferenz der Datenschutzbeauftragten

1. Budapest, 24./25. April 2006

Erklärung von Budapest

Die Ausweitung des grenzüberschreitenden Informationsaustausches und die – dem Prinzip der Verfügbarkeit unterliegende – gemeinsame Nutzung von in nationalen Dateien gespeicherten Daten als Teil der Zusammenarbeit von Polizei- und Justizbehörden auf der Ebene der Europäischen Union bilden mittlerweile den Brennpunkt der Diskussionen in Europa.

In diesem Zusammenhang erinnert die Konferenz der Europäischen Datenschutzbeauftragten die Mitgliedstaaten daran, dass die gemeinsame Nutzung personenbezogener Informationen durch ihre Strafverfolgungsbehörden nur auf der Grundlage von datenschutzrechtlichen Vorschriften zulässig ist, die ein hohes und harmonisiertes Datenschutzniveau auf europäischer Ebene und in allen Teilnehmerstaaten gewährleisten. Ansonsten könnten Situationen entstehen, in denen aufgrund der unterschiedlichen Schutzstandards und des Mangels an gemeinsamen Vorschriften für Zugangsbeschränkungen die Mindeststandards für den Datenschutz nicht eingehalten werden. In ihrer Erklärung von Krakau hatte die Konferenz betont, dass die bestehenden, in der EU angewandten Rechtsinstrumente des Datenschutzes zu allgemein gehalten sind, um einen wirksamen Datenschutz im Bereich der Strafverfolgung zu gewährleisten. Daher begrüßt die Konferenz den Vorschlag der Europäischen Kommission, den Datenschutz bei Polizei- und Justizbehörden durch die Schaffung von datenschutzrechtlichen Sicherungen in der Dritten Säule zu harmonisieren und zu stärken, die beim Informationsaustausch unter dem Prinzip der Verfügbarkeit angewandt werden müssen.

Es gibt keine Alternative zur Schaffung eines hohen und harmonisierten Datenschutzstandards in der Dritten Säule der EU. Dies ist eine logische Konsequenz des Haager Programms, dem zufolge die Wahrung der Freiheit, der Sicherheit und des Rechts unteilbare Bestandteile der Aufgabe der EU als Ganzes sind, ebenso wie die kürzlich auf EU-Ebene unternommenen Schritte auf Gebieten wie etwa des VISA Informationssystems (VIS), des Schengener Informationssystems II (SIS II), oder der Interoperabilität zwischen europäischen Datenbanken im Bereich der justiziellen und inneren Angelegenheiten. Allein mittels eines derartigen Standards wird es möglich sein, den rechten Ausgleich zwischen den bestehenden und künftigen Formen des Informationsaustausches zwischen den europäischen Strafverfolgungsbehörden zu finden und den Grundsatz der Verhältnismäßigkeit zu beachten, in dem auf der einen Seite die Sicherheit der EU-Bürgerinnen und Bürger geschützt wird und auf der anderen Seite ihre Freiheits-

rechte in einem Raum der Freiheit, der Sicherheit und des Rechts gewährleistet werden. Die Konferenz ruft die Parlamente – sowohl das Europäische Parlament als auch die nationalen Vertretungsorgane – dazu auf, ihren Einfluss auf die Regierungen der EU-Mitgliedstaaten geltend zu machen, um dieses Ziel zu erreichen. Die Konferenz appelliert an die Regierungen der Mitgliedstaaten, beim Ausbau der Möglichkeiten des Informationsaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten die Freiheitsrechte der in der EU lebenden Bürgerinnen und Bürger zu berücksichtigen und zu stärken.

Die Konferenz erachtet es als dringend notwendig, dass entsprechende datenschutzrechtliche Regelungen auf diesem Gebiet so schnell wie möglich verabschiedet und angewandt werden. Infolge dessen empfiehlt sie bei der Verabschiedung des Vorschlags der Europäischen Kommission für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, die Berücksichtigung der Inhalte der Stellungnahme, die am 24. Januar 2006 von der Konferenz der Europäischen Datenschutzbeauftragten verabschiedet wurde.

2. London, 2. November 2006

Erklärung von London

Der Ausbau des grenzüberschreitenden Informationsaustausches und die vorbehaltlich des Grundsatzes der Verfügbarkeit erfolgende Weitergabe von in nationalen Dateien gespeicherten Daten im Rahmen der Zusammenarbeit zwischen den Polizei- und Justizbehörden auf EU-Ebene stehen im Mittelpunkt der Diskussionen in Europa. In diesem Zusammenhang haben die Europäischen Datenschutzbehörden bereits wiederholt hervorgehoben, dass angesichts der Tatsache, dass die Union verpflichtet ist, die Menschenrechte und Grundfreiheiten zu achten, Initiativen zur Verbesserung der Kriminalitätsbekämpfung in der EU, wie z. B. der Grundsatz der Verfügbarkeit, nur auf der Grundlage eines angemessenen Systems von Datenschutzmaßnahmen eingeführt werden sollten, die ein hohes und vergleichbares Datenschutzniveau gewährleisten, das den Standards der Ersten Säule entspricht.

Die Europäischen Datenschutzbehörden fordern die Mitgliedstaaten auf, die bürgerlichen Freiheiten der in der EU lebenden Bürger zu respektieren und zu stärken und ein angemessenes System von Datenschutzmaßnahmen aufzubauen, das ein hohes und vergleichbares Datenschutzniveau für die gesamte Datenverarbeitung im Bereich der Kriminalitätsbekämpfung gewährleistet.

Es gibt keine Alternative zum Aufbau eines hohen und harmonisierten Datenschutzstandards im Rahmen der Dritten Säule der EU. Dies ist eine logische Kon-

sequenz aus dem Haager Programm, dem zu folge die Wahrung der Freiheit, der Sicherheit und des Rechts unteilbarer Bestandteil der Aufgabe der EU insgesamt ist. Einschlägige Datenschutzbestimmungen im Bereich der Kriminalitätsbekämpfung sollten so bald als möglich verabschiedet und umgesetzt werden, so dass ein angemessenes und harmonisiertes System von Datenschutzmaßnahmen geschaffen wird, die sich nicht nur auf den Datenaustausch zwischen den Mitgliedstaaten, sondern auf die gesamte Verarbeitung personenbezogener Daten im Rahmen der Kriminalitätsbekämpfung beziehen. Ein hohes Schutzniveau sollte auch für die Weitergabe von Daten an Drittstaaten und internationale Stellen gelten, die vorbehaltlich der auf der Grundlage gemeinsamer Europäischer Standards zu treffenden Feststellung eines angemessenen Datenschutzniveaus erfolgt.

Jeder andere, weniger umfassende Ansatz wäre nicht praktikabel und ungeeignet, das für eine wirksame Kooperation im Bereich der Kriminalitätsbekämpfung erforderliche Vertrauen zu schaffen.

IV. Dokumente der Europäischen Union: Arbeitspapiere der Artikel-29-Datenschutzgruppe

ARTIKEL-29-DATENSCHUTZGRUPPE

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von:

Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Zivil-justiz, Grundrechte und Unionsbürgerschaft).

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm

Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (WP 117)

Angenommen am 1. Februar 2006

INHALTSVERZEICHNIS

i) Die Einrichtung eines Verfahrens zur Meldung von Missständen ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt (Artikel 7, Buchstabe c))

ii) Die Einrichtung eines Verfahrens zur Meldung von Missständen ist erforderlich zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen (Artikel 7 Buchstabe f))

2. Anwendung der Grundsätze der Datenqualität und Verhältnismäßigkeit (Artikel 6 der Datenschutzrichtlinie)

i) Mögliche Begrenzung der Zahl der Personen, die berechtigt sind, mutmaßliche Unregelmäßigkeiten oder Fehlverhalten im Rahmen von Verfahren zur Meldung von Missständen zu melden

ii) Mögliche Begrenzung der Zahl der Personen, die in einem Verfahren zur Meldung von Missständen beschuldigt werden können

iii) Förderung von mit Namen versehenen vertraulichen Meldungen im Gegensatz zu anonymen Meldungen

iv) Verhältnismäßigkeit und Genauigkeit der verarbeiteten Daten

v) Einhaltung strenger Speicherfristen

3. Bereitstellung klarer und vollständiger Informationen über das System (Artikel 10 der Datenschutzrichtlinie)

4. Rechte der Beschuldigten

i) Informationsrechte

ii) Rechte auf Zugang, Berichtigung und Löschung

5. Sicherheit der Verarbeitung (Artikel 17 der Richtlinie 95/46/EG)

i) Materielle Sicherheitsmaßnahmen

ii) Vertraulichkeit von Meldungen mit Hilfe von Systemen zur Meldung von Missständen

6. Management von Systemen zur Meldung von Missständen

i) Bestimmte interne organisatorische Einheiten für das Management von Systemen zur Meldung von Missständen

ii) Die Möglichkeit, externe Dienstleister heranzuziehen

iii) Grundsatz der Untersuchung von Meldungen über EU-Unternehmen in der EU und Ausnahmen

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

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,[1]

gestützt auf Artikel 29 und 30 Absatz 1 Buchstabe c und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

I. EINFÜHRUNG

Diese Stellungnahme enthält Leitlinien zur Umsetzung interner Verfahren zur Meldung von Missständen nach den EU-Datenschutzvorschriften, die in der Richtlinie 95/46/EG festgelegt sind.[2]

Die zahlreichen Fragen, die sich mit der Einführung von Verfahren zur Meldung von Missständen in Europa 2005 ergaben, darunter auch Datenschutzfragen, hat gezeigt, dass die Entwicklung dieser Praktiken in allen EU-Ländern erhebliche Schwierigkeiten mit sich bringen kann. Diese Schwierigkeiten beruhen hauptsächlich auf kulturellen Unterschieden, die ihrerseits auf gesellschaftliche und/oder historische Gründe zurückzuführen sind, die nicht abzustreiten oder von der Hand zu weisen sind.

Der Gruppe ist klar, dass diese Schwierigkeiten teilweise mit dem breiten Spektrum der Fragen zusammenhängen, auf die mittels interner Verfahren zur Meldung von Missständen aufmerksam gemacht werden kann. Ihr ist ferner bekannt, dass Verfahren zur Meldung von Missständen in einigen EU-Ländern arbeitsrechtlich besonders problematisch sind und dass zu diesen Themen Arbeiten im Gange sind, die weitere Bemühungen erfordern werden. Die Gruppe muss ferner

[1] ABl. L 281vom 23.11.1995, S. 31, auch verfügbar unter: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

[2] Entsprechend dem spezifischen Auftrag der Gruppe befasst sich das vorliegende Arbeitspapier nicht mit anderen rechtlichen Schwierigkeiten durch Verfahren zur Meldung von Missständen, insbesondere im Hinblick auf Arbeits- und Strafrecht.

der Tatsache Rechnung tragen, dass die Funktionsweise der Verfahren zur Meldung von Missständen in einigen EU-Ländern gesetzlich geregelt ist, während in den meisten EU-Ländern keine spezifischen Rechtsvorschriften oder Regelungen zu diesem Thema vorhanden sind.

Die Gruppe hält es folglich für verfrüht, zum jetzigen Zeitpunkt eine endgültige Stellungnahme zu Verfahren zur Meldung von Missständen im Allgemeinen abzugeben. Durch die Verabschiedung dieser Stellungnahme hat sie beschlossen, sich mit den Themen auseinanderzusetzen, für die EU-Leitlinien am dringendsten erforderlich sind. In Anbetracht dessen und aus den im Dokument erwähnten Gründen ist diese Stellungnahme formal auf die Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität beschränkt.

Die Gruppe hat diese Stellungnahme unter der klaren Voraussetzung angenommen, dass sie weiter über die mögliche Vereinbarkeit von EU-Datenschutzvorschriften mit internen Verfahren zur Meldung von Missständen in anderen Bereichen als den bereits erwähnten nachdenken muss, z. B. Humanressourcen, Gesundheit und Sicherheit am Arbeitsplatz, Umweltschäden oder -gefahren und Straftaten. Sie wird ihre Untersuchungen in den kommenden Monaten fortsetzen, um zu entscheiden, ob auch für diese Themen EU-Leitlinien erforderlich sind; in diesem Falle könnten die im vorliegenden Dokument entwickelten Grundsätze in einem Folgedokument ergänzt oder geändert werden.

II. BEGRÜNDUNG FÜR DEN BEGRENZTEN ANWENDUNGSBEREICH DER STELLUNGNAHME

Der US-Kongress verabschiedete 2002 im Anschluss an mehrere Finanzskandale den *Sarbanes-Oxley Act (SOX)*.

Nach dem SOX müssen US-Aktiengesellschaften und ihre Unternehmenseinheiten in der EU sowie Nicht-US-Unternehmen, die an einer US-Börse notiert sind, im Rahmen ihres Prüfungsausschusses Verfahren zur Entgegennahme, Speicherung und Bearbeitung von Beschwerden einführen, die der Emittent in Bezug auf die Rechnungslegung, interne Rechnungslegungskontrollen und Wirtschaftsprüfungsfragen erhält; und zur vertraulichen, anonymen Einreichung von Beschwerden durch Angestellte des Emittenten in Bezug auf fragliche Rechnungslegungs- oder Wirtschaftsprüfungsangelegenheiten.[3] Darüber hinaus enthält Abschnitt 806 des SOX Vorschriften zur Gewährleistung des Schutzes von Beschäftigten bör-

[3] Sarbanes-Oxley Act, Abschnitt 301(4).

sennotierter Unternehmen, die Beweise für Betrug vorlegen, vor Vergeltungsmaßnahmen, die wegen der Nutzung des Meldeverfahrens gegen sie ergriffen werden könnten.[4] Die Securities and Exchange Commission (SEC) ist die zuständige US-Behörde für die Überwachung der Anwendung des SOX.

Diese Vorschriften spiegeln sich in den Regeln der NASDAQ[5] und des New York Stock Exchange (NYSE)[6] wider. Unternehmen, die an der NASDAQ oder der NYSE notiert sind, müssen ihre Rechnungsabschlüsse für diese Märkte jährlich bescheinigen lassen. Dieses Prüfungsverfahren bedeutet, dass die Unternehmen die Einhaltung einer Reihe von Vorschriften nachweisen können, darunter Vorschriften zur Meldung von Missständen.

Unternehmen, die diesen Berichterstattungsanforderungen nicht entsprechen, unterliegen strengen Sanktionen und Strafen durch die Nasdaq, NYSE oder SEC. Aufgrund der Unsicherheit bezüglich der Vereinbarkeit der Verfahren zur Meldung von Missständen mit den EU-Datenschutzvorschriften laufen die betroffenen Unternehmen einerseits Gefahr, Sanktionen von EU-Datenschutzbehörden auferlegt zu bekommen, wenn sie gegen die EU-Datenschutzvorschriften verstoßen und andererseits von den US-Behörden, wenn sie die US-Vorschriften nicht einhalten.

Die Anwendbarkeit einiger SOX-Vorschriften auf europäische Tochterunternehmen von US-Unternehmen und europäische Unternehmen, die an US-Börden notiert sind, wird derzeit in den Vereinigten Staaten gerichtlich überprüft.[7] Trotz dieser relativen Unsicherheit bezüglich der Anwendbarkeit aller SOX-Bestimmungen auf in Europa ansässige Unternehmen, streben Unternehmen, die auf der Grundlage der eindeutigen extraterritorialen Vorschriften des Gesetzes dem SOX unterliegen, an, auch in der Lage zu sein, die spezifischen Vorschriften des SOX über die Meldung von Missständen einzuhalten.

Wegen des Sanktionsrisikos für EU-Unternehmen hat die Artikel 29-Gruppe es als dringlich erachtet, ihre Analyse hauptsächlich auf die Verfahren zur Meldung von Missständen zu konzentrieren, die eingerichtet wurden, um potenzielle Verstöße gegen Rechnungslegungs-, interne Rechnungslegungskontroll- und Wirtschaftsprüfungsfragen zu melden, wie sie im Sarbanes-Oxley Act auf-

4 Der Sarbanes-Oxley Act, Abschnitt 406, und insbesondere die Regelungen wichtiger US-Börsen (NASDAQ, NYSE) schreiben ferner vor, dass an diesen Börsen notierte Unternehmen „Verhaltenskodizes“ annehmen müssen, die für leitende Finanzmanager und Direktoren gelten und Rechnungslegungs-, Berichterstattungs- und Wirtschaftsprüfungsfragen betreffen und Durchsetzungsmechanismen enthalten sollten.

5 Regel 4350 (D) (3): “Audit Committee Responsibilities and Authority”

6 New York Stock Exchange (NYSE), Abschnitt 303A.06: “Audit Committee”

7 Das U.S. Court of Appeals (1st Circuit) befand am 5. Januar 2006, dass SOX-Vorschriften über den Schutz von Hinweisgebern nicht für ausländische Staatsbürger gelten, die außerhalb der USA für ausländische Niederlassungen von Unternehmen arbeiten, die die übrigen Bestimmungen des SOX erfüllen müssen.

geführt werden, und über die nachfolgend erwähnten verwandten Fragen. Die Gruppe möchte damit zur Schaffung von Rechtssicherheit für Unternehmen beitragen, die sowohl den EU-Datenschutzvorschriften als auch dem SOX unterliegen.

III. DER SCHWERPUNKT DER DATENSCHUTZVORSCHRIFTEN LIEGT AUF DEM SCHUTZ DER PERSONEN, DIE DURCH EIN VERFAHREN ZUR MELDUNG VON MISSSTÄNDEN BELASTET WERDEN

Interne Verfahren zur Meldung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige Grundsätze der Unternehmensführung in den täglichen Betrieb der Unternehmen einzuführen. Verfahren zur Meldung von Missständen sind als zusätzlicher Mechanismus für die Beschäftigten gedacht, um Missstände intern über einen bestimmten Kanal zu melden. Sie ergänzen die regulären Informations- und Meldekanäle der Einrichtung, wie beispielsweise Arbeitnehmervertretungen, Linienmanagement, Qualitätskontrollpersonal oder interne Auditoren, die eigens dafür eingestellt sind, solche Missstände zu melden. Die Meldung von Missständen ist als Ergänzung zum internen Management zu sehen und nicht als Ersatz dafür.

Die Gruppe weist darauf hin, dass Verfahren zur Meldung von Missständen in Übereinstimmung mit den EU-Datenschutzvorschriften eingerichtet werden müssen. In der Tat wird die Umsetzung von Verfahren zur Meldung von Missständen in den allermeisten Fällen auf der Verarbeitung personenbezogener Daten beruhen (d. h. auf der Sammlung, Registrierung, Speicherung, Offenlegung und Löschung von Daten im Zusammenhang mit einer festgestellten oder feststellbaren Person), was wiederum bedeutet, dass die Datenschutzvorschriften gelten.

Die Anwendung dieser Vorschriften wird unterschiedliche Folgen für die Einrichtung und Verwaltung von Verfahren zur Meldung von Missständen haben. Das umfassende Spektrum dieser Folgen wird an anderer Stelle in diesem Dokument behandelt (siehe Abschnitt IV).

Die Gruppe stellt fest, dass vorhandene Regelungen und Leitlinien über Verfahren zur Meldung von Missständen darauf ausgelegt sind, der Person („dem Hinweisgeber“), die diese Verfahren nutzt, besonderen Schutz zu gewähren, sie aber an keiner Stelle den Schutz der beschuldigten Person besonders erwähnen, insbesondere hinsichtlich der Verarbeitung seiner/ihrer personenbezogenen Daten. Eine Person hat jedoch Anspruch auf die Rechte, die ihr nach der Richtlinie 95/46/EG und den entsprechenden einzelstaatlichen Rechtsvorschriften zustehen, auch wenn sie eines Verstoßes beschuldigt wird.

Die Anwendung von EU-Datenschutzvorschriften auf Verfahren zur Meldung von Missständen bedeutet, dass der Frage des Schutzes der Person, die durch eine Meldung möglicherweise beschuldigt wurde, besondere Aufmerksamkeit gewidmet wird. Diesbezüglich weist die Gruppe darauf hin, dass Verfahren zur Meldung von Missständen eine sehr ernste Gefahr der Stigmatisierung und Viktimisierung dieser Person innerhalb der Einrichtung, der sie angehört, mit sich bringen. Die Person wird solchen Risiken sogar schon ausgesetzt sein, bevor ihr bewusst wird, dass sie beschuldigt wurde und die angeblichen Fakten auf ihren Wahrheitsgehalt untersucht wurden.

Die Gruppe ist der Ansicht, dass die korrekte Anwendung der Datenschutzvorschriften auf Verfahren zur Meldung von Missständen zur Verringerung der genannten Gefahren beitragen wird. Sie ist ferner der Auffassung, dass die Anwendung dieser Vorschriften generell zum Funktionieren von Verfahren zur Meldung von Missständen beitragen und sie nicht im geringsten daran hindern wird, den beabsichtigten Zweck zu erfüllen.

IV. BEWERTUNG DER VEREINBARKEIT VON VERFAHREN ZUR MELDUNG VON MISSSTÄNDEN MIT DATENSCHUTZVORSCHRIFTEN

Die Anwendung von Datenschutzvorschriften auf Verfahren zur Meldung von Missständen betrifft die Frage der Zulässigkeit von Verfahren zur Meldung von Missständen (1); die Anwendung der Grundsätze der Datenqualität und der Verhältnismäßigkeit (2); die Bereitstellung klarer und vollständiger Informationen über das Verfahren (3); die Rechte der beschuldigten Person (4); die Sicherheit der Verarbeitung (5); die Verwaltung interner Verfahren zur Meldung von Missständen (6); Fragen im Zusammenhang mit der internationalen Übermittlung von Daten (7); die Meldung und die Voraussetzungen für eine Vorabkontrolle (8).

1. Zulässigkeit von Verfahren zur Meldung von Missständen (Artikel 7 der Richtlinie 95/46/EG)

Damit ein Verfahren zur Meldung von Missständen rechtmäßig ist, muss die Verarbeitung personenbezogener Daten legitim sein und eine der in Artikel 7 der Datenschutzrichtlinie genannten Voraussetzungen erfüllen.

Beim derzeitigen Stand erscheinen in diesem Zusammenhang zwei Voraussetzungen relevant: die Einrichtung eines Verfahrens zur Meldung von Missständen ist entweder für die Erfüllung einer rechtlichen Verpflichtung erforderlich (Arti-

kel 7 Buchstabe c)) oder zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, dem/denen die Daten übermittelt werden (Artikel 7 Buchstabe f)).[8]

i) Die Einrichtung eines Verfahrens zur Meldung von Missständen ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt (Artikel 7, Buchstabe c))

Die Einrichtung eines Meldeverfahrens sollte der Erfüllung einer rechtlichen Verpflichtung auf Grund von Rechtsvorschriften der Gemeinschaft oder eines Mitgliedstaates dienen, und insbesondere eine rechtlichen Verpflichtung, durch die interne Kontrollverfahren in genau festgelegten Bereichen geschaffen werden sollen.

Derzeit gibt es solche Verpflichtungen in den meisten Mitgliedstaaten beispielsweise für den Banksektor; hier haben die Regierungen beschlossen, die internen Kontrollen zu verschärfen, insbesondere hinsichtlich der Tätigkeiten von Kredit- und Investmentgesellschaften.

Eine solche rechtliche Verpflichtung zur Einrichtung von verstärkten Kontrollmechanismen gibt es auch im Zusammenhang mit der Korruptionsbekämpfung, insbesondere infolge der Umsetzung des OECD-Übereinkommens zur Bekämpfung der Bestechung ausländischer Beamter im Rahmen internationaler Wirtschaftsabkommen (OECD-Übereinkommen vom 17. Dezember 1997) in einzelstaatliches Recht.

Hingegen gilt eine Verpflichtung aufgrund eines ausländischen Statuts oder einer ausländischen Verordnung, die die Einrichtung von Meldeverfahren erforderlich machen würde, möglicherweise nicht als rechtliche Verpflichtung, die die Datenverarbeitung in der EU legitimieren würde. Jede andere Interpretation würde es ausländischen Vorschriften leicht machen, die EU-Vorschriften gemäß Richtlinie 95/46/EG zu umgehen. Folglich sind die SOX-Vorschriften über die Meldung von Missständen nicht als rechtliche Grundlage für die Verarbeitung nach Artikel 7 Buchstabe c) anzusehen.

In bestimmten EU-Ländern kann es jedoch sein, dass Verfahren zur Meldung von Missständen mittels rechtlich verbindlicher Verpflichtungen des nationalen Rechts in den gleichen Bereichen eingeführt werden müssen, die das SOX

[8] Unternehmen sollten wissen, dass die Verarbeitung von Daten über mutmaßliche Straftaten in einigen Mitgliedstaaten weiteren spezifischen Anforderungen unterliegt, die mit der Zulässigkeit ihrer Verarbeitung zusammenhängen (siehe *unten*, Abschnitt IV, 8).

abdeckt.[9] In anderen EU-Ländern, wo es derartige rechtlich bindende Verpflichtungen nicht gibt, kann das gleiche Ergebnis jedoch auf der Grundlage von Artikel 7 Buchstabe f) erzielt werden.

ii) Die Einrichtung eines Verfahrens zur Meldung von Missständen ist erforderlich zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen (Artikel 7Buchstabe f))

Die Einrichtung von Verfahren zur Meldung von Missständen kann zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, für erforderlich gehalten werden (Artikel 7 Buchstabe f)). Ein solcher Grund wäre nur unter der Voraussetzung akzeptabel, dass „nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen".

Wichtige internationale Organisationen, darunter die EU[10] und die OECD[11], haben erkannt, dass es wichtig ist, auf gute Grundsätze der Unternehmensführung zu bauen, um die angemessene Funktionsweise der Organisationen sicherzustellen. Die Grundsätze oder Leitlinien, die in diesen Foren entwickelt wurde, beziehen sich auf die Verbesserung der Transparenz, die Entwicklung solider finanzieller und Rechnungslegungspraktiken, und damit die Verbesserung des Schutzes der Betroffenen und der finanziellen Stabilität der Märkte. Sie erkennen insbesondere das Interesse einer Organisation an der Einrichtung angemessener Verfahren an, die es den Beschäftigten ermöglichen, Unregelmäßigkeiten und fragwürdige Rechnungslegungs- oder Wirtschaftsprüfungspraktiken an den Verwaltungsrat oder den Prüfungsausschuss zu melden. Diese Meldeverfahren müssen sicherstellen, dass Vorkehrungen für die verhältnismäßige und unabhängige Untersuchung der gemeldeten Tatsachen getroffen wurden, wozu auch ein angemessenes Auswahlverfahren für die an der Verwaltung des Verfahrens beteiligten Personen und für angemessene Folgemaßnahmen gehört.

Darüber hinaus sollte in diesen Leitlinien und Regelungen hervorgehoben werden, dass der Schutz der Hinweisgeber gewährleistet sein sollte und dass es angemessene Garantien für den Schutz der Hinweisgeber vor Vergeltungsmaßnahmen (diskriminierende oder disziplinarische Maßnahmen) geben sollte.[12]

---

9 Niederländisches Gesetz über Corporate Governance, 9.12.2003, Abschnitt II, 1.6 Spanischer Entwurf eines Einheitlichen Gesetzes über Corporate Governance in börsennotierten Unternehmen, Kapitel IV, 67(1)d). Dieses Gesetz muss im Hinblick auf Folgen für den Datenschutz noch von der spanischen Datenschutzbehörde geprüft werden.

10 Europäische Gemeinschaft: Empfehlung der Kommission vom 15. Februar 2005 zu den Aufgaben von nicht geschäftsführenden Direktoren/Aufsichtsratsmitgliedern börsennotierter Gesellschaften sowie zu den Ausschüssen des Verwaltungs-/Aufsichtsrats (ABl. L 52 vom 25.2.2005, S. 51).

11 OECD: OECD Principles of Corporate Governance. 2004. Teil 1, Abschnitt IV.

12 Siehe beispielsweise UK Public Interest Disclosure Act 1998.

Tatsächlich scheint das Ziel der Gewährleistung der finanziellen Sicherheit auf den internationalen Finanzmärkten und insbesondere die Verhütung von Betrug und Fehlverhalten in Bezug auf die Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung sowie die Bekämpfung von Korruption, Banken- und Finanzkriminalität oder Insider-Geschäften ein berechtigtes Interesse des Arbeitgebers zu sein, das die Verarbeitung personenbezogener Daten mittels Verfahren zur Meldung von Missständen in diesen Bereichen rechtfertigt. Es ist ein wesentliches Anliegen für eine Aktiengesellschaft, insbesondere eine börsennotierte, zu gewährleisten, dass Berichte über mutmaßliche Rechnungslegungsmanipulationen oder fehlerhafte Rechnungslegung, die sich auf die Jahresabschlüsse des Unternehmens auswirken und sich auf die berechtigten Interessen der Betroffenen an der finanziellen Stabilität des Unternehmens auswirken können, den Vorstand auch erreichen, damit angemessene Folgemaßnahmen ergriffen werden können.

In diesem Zusammenhang kann der Sarbanes-Oxley Act der USA als eine der Maßnahmen gesehen werden, die getroffen wurden, um die Stabilität der Finanzmärkte und den Schutz der berechtigten Interessen der Betroffenen sicherzustellen, indem Regeln festgelegt wurden, die die angemessene Unternehmensführung der Unternehmen gewährleisten.

Aus all diesen Gründen ist die Gruppe der Auffassung, dass die für die Verarbeitung Verantwortlichen in den EU-Ländern, die keine spezifischen rechtlichen Anforderungen aufweisen, die die Einführung von Verfahren zur Meldung von Missständen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und Bekämpfung von Korruption und von Banken- und Finanzkriminalität erforderlich machen, dennoch ein berechtigtes Interesse an der Umsetzung solcher interner Verfahren auf diesen Gebieten haben können.

Nach Artikel 7 Buchstabe f) ist jedoch ein Gleichgewicht zwischen den berechtigten Interessen durch die Verarbeitung personenbezogener Daten und den Grundrechten und -freiheiten der betroffenen Personen herzustellen. Diese Prüfung des Gleichgewichts der Interessen sollte Fragen der Verhältnismäßigkeit, der Subsidiarität, der Ernsthaftigkeit der mutmaßlichen Verstöße, die gemeldet werden können sowie die Folgen für die betroffenen Personen berücksichtigen. Im Rahmen der Prüfung des Gleichgewichts der Interessen werden auch angemessene Garantien eingerichtet werden müssen. Insbesondere in Artikel 14 der Richtlinie 95/46/EG ist festgelegt, dass Personen das Recht haben, jederzeit aus überwiegenden schutzwürdigen Gründen dagegen Widerspruch einlegen können, dass sie betreffende Daten verarbeitet werden, wenn die Datenverarbeitung auf Artikel 7 Buchstabe f) basiert. Diese Punkte werden weiter unten ausgeführt.

2. Anwendung der Grundsätze der Datenqualität und Verhältnismäßigkeit (Artikel 6 der Datenschutzrichtlinie)

Gemäß Richtlinie 95/46/EG müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;[13] sie müssen für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden[14] und dürfen nicht in einer damit nicht zu vereinbarenden Weise weiterverarbeitet werden. Darüber hinaus müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen.[15] Diese Vorschriften werden manchmal als „Grundsatz der Verhältnismäßigkeit" bezeichnet. Schließlich müssen angemessene Maßnahmen getroffen werden, um sicherzustellen, dass nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden.[16] Die Anwendung dieser grundlegenden Datenschutzvorschriften hat eine Reihe von Folgen hinsichtlich der Weise, wie die Beschäftigten einer Einrichtung Meldungen machen können und wie diese von der Organisation verarbeitet werden. Diese Folgen werden weiter unten untersucht.

i) Mögliche Begrenzung der Zahl der Personen, die berechtigt sind, mutmaßliche Unregelmäßigkeiten oder Fehlverhalten im Rahmen von Verfahren zur Meldung von Missständen zu melden

In Anwendung des Grundsatzes der Verhältnismäßigkeit empfiehlt die Gruppe, dass das für das Verfahren zur Meldung von Missständen verantwortliche Unternehmen sorgfältig prüfen sollte, ob es angemessen wäre, die Zahl der Personen zu begrenzen, die für die Meldung mutmaßlichen Fehlverhaltens mit Hilfe des Verfahrens zur Meldung von Missständen infrage kommen, insbesondere in Anbetracht der Schwere der zu meldenden mutmaßlichen Verstöße. Die Gruppe erkennt jedoch an, dass die aufgeführten Personalkategorien in einigen der Bereiche, die unter diese Stellungnahme fallen, manchmal alle Beschäftigten umfassen können.

Der Gruppe ist bewusst, dass im Einzelfall die jeweiligen Umstände entscheidend sein werden. Daher will sie zu diesem Punkt keine Vorgaben machen und überlässt es den für die Verarbeitung Verantwortlichen, gegebenenfalls mit Überprüfung durch die zuständigen Behörden, zu entscheiden, ob solche Beschränkungen unter den spezifischen Umständen ihrer Tätigkeit angemessen sind.

---

[13] Artikel 6 Absatz 1 Buchstabe a) der Richtlinie 95/46/EG

[14] Artikel 6 Absatz 1 Buchstabe b) der Richtlinie 95/46/EG

[15] Artikel 6 Absatz 1 Buchstabe c) der Richtlinie 95/46/EG

[16] Artikel 6 Absatz 1) Buchstabe d) der Richtlinie 95/46/EG

ii) Mögliche Begrenzung der Zahl der Personen, die in einem Verfahren zur Meldung von Missständen beschuldigt werden können

In Anwendung des Grundsatzes der Verhältnismäßigkeit empfiehlt die Gruppe, dass das Unternehmen, das ein Verfahren zur Meldung von Missständen einführt, sorgfältig prüfen sollte, ob es angebracht wäre, die Zahl der Personen zu begrenzen, die über das Verfahren gemeldet werden können, insbesondere in Anbetracht der Schwere der gemeldeten mutmaßlichen Verstöße. Die Gruppe erkennt jedoch an, dass die aufgeführten Personalkategorien in einigen der Bereiche, die unter diese Stellungnahme fallen, manchmal alle Beschäftigten umfassen können.

Der Gruppe ist bewusst, dass im Einzelfall die Umstände entscheidend sein werden. Daher will sie zu diesem Punkt keine Vorgaben machen und überlässt es den für die Verarbeitung Verantwortlichen, gegebenenfalls mit Überprüfung durch die zuständigen Behörden, zu entscheiden, ob solche Beschränkungen unter den spezifischen Umständen ihrer Tätigkeit angemessen sind.

iii) Förderung von mit Namen versehenen vertraulichen Meldungen im Gegensatz zu anonymen Meldungen

Die Frage, ob Verfahren zur Meldung von Missständen es ermöglichen sollten, eine Meldung anonym anstatt offen zu machen (d. h. unter Angabe des Namens und auf jeden Fall unter vertraulichen Bedingungen) verdient besondere Aufmerksamkeit.

Anonymität ist möglicherweise keine gute Lösung für den Hinweisgeber oder für die Organisation, und zwar aus einer Reihe von Gründen:

– Anonymität hindert andere nicht daran, mit Erfolg zu erraten, wer die Beschwerde vorgebracht hat;

– die Beschwerde ist schwerer zu überprüfen, wenn keine Anschlussfragen gestellt werden können;

– es ist leichter, den Schutz des Hinweisgebers vor Vergeltungsmaßnahmen zu organisieren, vor allem wenn dieser Schutz gesetzlich gesichert ist,[17] wenn die Beschwerde offen vorgebracht wird;

– anonyme Meldungen können dazu führen, dass sich die Menschen auf den Hinweisgeber konzentrieren, vielleicht mit dem Verdacht, dass er oder sie die Beschwerde aus Bosheit vorgebracht hat;

[17] Z. B. nach dem UK Public Interest Disclosure Act

– eine Organisation läuft Gefahr, dass eine Kultur anonymer böswilliger Meldungen entsteht;

– das soziale Klima innerhalb der Organisation könnte schlechter werden, wenn den Beschäftigten bewusst würde, dass mit Hilfe des Verfahrens jederzeit anonyme Meldungen über sie gemacht werden könnten.

Was die Datenschutzvorschriften angeht, so stellen anonyme Meldungen ein besonderes Problem bezüglich der grundlegenden Anforderungen dar, dass personenbezogene Daten nur nach Treu und Glauben erhoben werden sollten. Generell ist die Gruppe der Auffassung, dass ausschließlich mit Namen versehene Meldungen durch Verfahren zur Meldung von Missständen übermittelt werden sollten, um dieser Anforderung zu genügen.

Der Gruppe ist jedoch bewusst, dass manche Hinweisgeber vielleicht nicht immer in der Lage sind oder nicht immer die psychische Veranlagung haben, mit Namen versehene Meldungen zu machen. Sie ist sich ferner der Tatsache bewusst, dass anonyme Beschwerden innerhalb von Unternehmen Wirklichkeit sind, auch und vor allem, wenn es keine organisierten vertraulichen Verfahren zur Meldung von Missständen gibt, und dass diese Wirklichkeit nicht übersehen werden darf. Die Gruppe ist daher der Auffassung, dass Verfahren zur Meldung von Missständen dazu führen können, dass über das System anonyme Meldungen gemacht werden und daraufhin gehandelt wird, aber als Ausnahme von der Regel und unter folgenden Bedingungen.

Die Gruppe ist der Meinung, dass Verfahren zur Meldung von Missständen so aufgebaut sein sollten, dass sie anonyme Meldungen als normale Art der Beschwerde nicht unterstützen. Insbesondere sollten die Unternehmen nicht darauf hinweisen, dass das Verfahren anonyme Meldungen ermöglicht. Da Verfahren zur Meldung von Missständen im Gegenteil sicherstellen sollten, dass die Identität des Hinweisgebers vertraulich behandelt wird, sollte eine Person, die eine Meldung mit Hilfe eines solchen Verfahrens machen möchte wissen, dass er/sie nicht wegen seiner/ihrer Maßnahme benachteiligt werden wird. Aus diesem Grund sollte der Hinweisgeber bei der ersten Kontaktaufnahme mit dem System vom System darauf hingewiesen werden, dass seine/ihre Identität während aller Schritte des Verfahrens vertraulich behandelt wird und insbesondere Dritten nicht offenbart werden wird, weder der beschuldigten Person selbst noch dem Linienmanagement des Beschäftigten. Wenn die meldende Person trotz dieser Informationen anonym bleiben möchte, so wird die Meldung in das System aufgenommen. Es ist ferner erforderlich, den Hinweisgebern klar zu machen, dass ihre Identität den Personen, die an weiteren Überprüfungen oder anschließenden Gerichtsverfahren, die als Ergebnis der Nachforschungen durch das System zur Meldung von Missständen eingeleitet wurden, beteiligt sind, enthüllt werden kann.

Die Bearbeitung anonymer Meldungen muss besonders vorsichtig erfolgen. Diese Vorsicht würde beispielsweise die Prüfung der Zulässigkeit der Meldung und der Angemessenheit ihrer Verbreitung im Rahmen des Systems durch den ersten Empfänger erfordern. Es könnte sich auch lohnen, zu überlegen, ob anonyme Meldungen wegen der Gefahr des Missbrauchs schneller geprüft und bearbeitet werden sollten als vertrauliche Beschwerden. Solche besondere Vorsicht bedeutet aber nicht, dass bei anonymen Meldungen nicht alle Tatsachen des Falles mit der erforderlichen Sorgfalt untersucht werden sollten, wie es bei offenen Meldungen der Fall wäre.

iv) Verhältnismäßigkeit und Genauigkeit der verarbeiteten Daten

Nach Artikel 6 Absatz 1 Buchstabe b) und c) der Datenschutzrichtlinie müssen personenbezogene Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen.

Da der Zweck des Meldeverfahrens darin besteht, eine richtige Corporate Governance zu gewährleisten, sollten die über ein Verfahren zur Meldung von Missständen erhobenen Daten auf die Fakten begrenzt werden, die mit diesem Zweck zusammenhängen. Unternehmen, die diese Systeme einrichten, sollten die Art der Informationen, die durch das System offen gelegt werden, klar definieren, indem sie die Art der Information auf Rechnungslegung, interne Rechnungslegungskontrollen oder Wirtschaftsprüfung oder die Bekämpfung von Banken- und Finanzkriminalität und Korruption begrenzen. Es wird anerkannt, dass das Gesetz in einigen Ländern ausdrücklich vorsehen kann, dass Verfahren zur Meldung von Missständen auch auf andere Kategorien schwerer Verstöße angewandt werden, die im öffentlichen Interesse offen gelegt werden müssen[18], aber diese liegen außerhalb des Erfassungsbereichs dieser Stellungnahme; in anderen Ländern gelten sie möglicherweise nicht. Die im Rahmen des Verfahrens verarbeiteten personenbezogenen Daten sollten auf die Daten begrenzt werden, die unbedingt und objektiv erforderlich sind, um die gemachten Anschuldigungen zu überprüfen. Darüber hinaus sollten Beschwerdemeldungen von anderen personenbezogenen Daten getrennt gehalten werden.

Wenn einem System zur Meldung von Missständen Tatsachen gemeldet werden, die sich nicht auf die Bereiche des betreffenden Systems beziehen, so könnten sie an die zuständigen Bediensteten des Unternehmens/der Organisation weitergeleitet werden, wenn die wesentlichen Interessen des Betroffenen oder die moralische Integrität von Beschäftigten auf dem Spiel stehen oder wenn nach den ein-

[18] Beispielsweise im UK Public Interest Disclosure Act 1998.

zelstaatlichen Rechtsvorschriften eine rechtliche Verpflichtung besteht, die Information an öffentliche Stellen oder Behörden zu übermitteln, die für die Verfolgung von Straftaten zuständig sind.

v) Einhaltung strenger Speicherfristen

In der Richtlinie 95/46/EG ist festgelegt, dass verarbeitete personenbezogene Daten für den Zeitraum, der für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, gespeichert werden dürfen. Dies ist wesentlich, um die Einhaltung des Grundsatzes der Verhältnismäßigkeit der Verarbeitung personenbezogener Daten sicherzustellen.

Personenbezogene Daten, die von einem System zur Meldung von Missständen verarbeitet werden, sollten gelöscht werden, unverzüglich und in der Regel innerhalb von zwei Monaten nach Abschluss der Untersuchungen der in der Meldung enthaltenen Fakten.

Diese Zeiträume wären anders, wenn rechtliche Verfahren oder Disziplinarmaßnahmen gegen die beschuldigte Person oder, im Falle von falschen oder rufschädigenden Erklärungen, gegen den Hinweisgeber eingeleitet würden. In solchen Fällen sollten personenbezogene Daten bis zum Abschluss dieser Verfahren und dem Ablauf der Rechtsbehelfsfristen aufbewahrt werden. Solche Speicherfristen werden durch die Rechtsvorschriften der Mitgliedstaaten festgelegt.

Personenbezogene Daten im Zusammenhang mit Meldungen, die von der Einheit, die für die Bearbeitung der Meldung zuständig ist, als grundlos erachtet werden, sollten unverzüglich gelöscht werden.

Darüber hinaus behalten einzelstaatliche Vorschriften bezüglich der Archivierung von Daten im Unternehmen ihre Gültigkeit. Diese Vorschriften können sich insbesondere auf den Zugang zu den Daten in solchen Archiven beziehen und die Zwecke aufführen, für die ein solcher Zugang möglich ist, die Kategorien von Personen, die Zugang zu diesen Dateien erhalten können und alle anderen relevanten Sicherheitsbestimmungen.

3. Bereitstellung klarer und vollständiger Informationen über das System (Artikel 10 der Datenschutzrichtlinie)

Die Anforderung, klare und vollständige Informationen über das System bereitzustellen, verpflichtet den für die Verarbeitung Verantwortlichen dazu, die Betroffenen von der Existenz, dem Zweck und der Funktionsweise des Systems, den Empfängern der Meldungen und den Zugangs-, Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten zu unterrichten.

Die für die Verarbeitung Verantwortlichen sollten ferner über die Tatsache informieren, dass die Identität des Hinweisgebers während des gesamten Verfahrens vertraulich behandelt wird und dass ein Missbrauch des Systems zu Maßnahmen gegen denjenigen führen kann, der das System missbraucht hat. Andererseits können die Nutzer des Systems auch darüber informiert werden, dass sie nicht mit Sanktionen rechnen müssen, wenn sie das System in gutem Glauben benutzen.

4. Rechte der Beschuldigten

Der durch die Richtlinie 95/46/EG gesteckte rechtliche Rahmen legt besonderen Wert auf dem Schutz der personenbezogenen Daten des Betroffenen. Unter Datenschutzgesichtspunkten sollte der Schwerpunkt von Systemen zur Meldung von Missständen somit auf den Rechten des Betroffenen liegen, ohne dass die Rechte des Hinweisgebers beeinträchtigt werden. Ein Gleichgewicht der Interessen sollte zwischen den Rechten der betroffenen Parteien hergestellt werden, einschließlich des legitimen Untersuchungsbedarfs des Unternehmens.

i) Informationsrechte

Nach Artikel 11 der Richtlinie 95/46/EG sind die betroffenen Personen zu unterrichten, wenn personenbezogene Daten bei Dritten erhoben werden und nicht unmittelbar bei ihnen selbst.

Die Person, die in der Meldung eines Hinweisgebers beschuldigt wird, muss sobald wie möglich von der für das System verantwortlichen Person informiert werden, wenn die sie betreffenden Daten aufgezeichnet wurden. Nach Artikel 14 hat sie ferner das Recht, Widerspruch gegen die Verarbeitung ihrer Daten einzulegen, wenn die Verarbeitung auf Artikel 7 Buchstabe f) beruht. Dieses Widerspruchsrecht kann jedoch nur aus zwingenden rechtlichen Gründen ausgeübt werden, die sich auf die besondere Situation der Person beziehen.

Insbesondere muss der/die gemeldete Beschäftigte unterrichtet werden über: [1] die für das System zur Meldung von Missständen zuständige Einheit, [2] die Beschuldigungen, die gegen ihn/sie vorgebracht werden, [3] die Abteilungen oder Dienststellen, die die Meldung innerhalb der eigenen Firma oder in anderen Einheiten oder Unternehmen der Gruppe, zu der das Unternehmen gehört, erhalten können und [4] wie er/sie die Zugangs- und Berichtigungsrechte wahrnehmen kann.

Wenn jedoch das Risiko, dass eine solche Notifizierung die Fähigkeit des Unternehmen zur wirksamen Untersuchung des Vorwurfs oder zur Sammlung der erforderlichen Beweise gefährden würde, erheblich wäre, kann die Notifizierung der beschuldigten Person so lange aufgeschoben werden wie diese Gefahr besteht. Diese Ausnahme von der in Artikel 11 festgelegten Regel soll dazu die-

nen, Beweise zu sichern, indem ihre Vernichtung oder Änderung durch die beschuldigte Person verhindert wird. Sie muss im jeweiligen Fall restriktiv angewandt werden und sollte die breiteren Interessen berücksichtigen, die auf dem Spiel stehen.

Das System zur Meldung von Missständen sollte die erforderlichen Maßnahmen treffen, um sicherzustellen, dass die offen gelegten Informationen nicht vernichtet werden.

ii) Rechte auf Zugang, Berichtigung und Löschung

Artikel 12 der Richtlinie 95/46/EG gibt dem/der Betroffenen die Möglichkeit, Zugang zu ihn/sie betreffenden Daten zu erhalten, um ihre Richtigkeit zu überprüfen und sie zu berichtigen, falls sie unrichtig, unvollständig oder überholt sind (Recht auf Zugang und Berichtigung). Folglich muss bei der Einrichtung von Meldesystemen die Wahrung der Rechte des Einzelnen auf Zugang und Berichtigung unrichtiger, unvollständiger oder überholter Daten gewährleistet werden.

Die Ausübung dieser Rechte kann jedoch beschränkt sein, um den Schutz der Rechte und Grundfreiheiten anderer am System beteiligter Personen zu gewährleisten. Diese Beschränkung sollte von Fall zu Fall angewandt werden.

In gar keinem Fall kann die durch die Meldung eines Hinweisgebers beschuldigte Person vom System auf Grund des Zugangsrechts der beschuldigten Person Informationen über die Identität des Hinweisgebers erhalten, außer wenn der Hinweisgeber in böswilliger Absicht eine falsche Angabe macht. Ansonsten ist der Schutz der Daten des Hinweisgebers immer zu gewährleisten.

Darüber hinaus haben die Betroffenen das Recht, ihre Daten zu berichtigen oder zu löschen, wenn die Verarbeitung dieser Daten gegen die Bestimmungen dieser Richtlinie verstößt, insbesondere wenn die Daten unvollständig oder unrichtig sind (Artikel 12 Buchstabe b)).

5. Sicherheit der Verarbeitung (Artikel 17 der Richtlinie 95/46/EG)

i) Materielle Sicherheitsmaßnahmen

Nach Artikel 17 der Richtlinie 95/46/EG muss das Unternehmen oder die Organisation, das/die für ein System zur Meldung von Missständen verantwortlich ist, die geeigneten technischen und organisatorischen Maßnahmen treffen, die für die Gewährleistung der Sicherheit der Daten bei ihrer Erhebung, Verbreitung oder Speicherung erforderlich sind. Ziel ist, die Daten gegen zufällige oder unrechtmäßige Zerstörung oder den zufälligen Verlust und die unberechtigte Weitergabe oder den unberechtigten Zugang zu schützen.

Die Meldungen können mit allen – elektronischen oder anderen – Mitteln zur Datenverarbeitung erhoben werden. Solche Mittel sollten auf das Verfahren zur Meldung von Missständen beschränkt sein, um jegliche Abweichung von seinem ursprünglichen Zweck zu verhindern und größere Datensicherheit zu gewährleisten.

Diese Sicherheitsmaßnahmen müssen im Verhältnis zu der Untersuchung der angesprochenen Fragen stehen, entsprechend den Sicherheitsvorschriften der einzelnen Mitgliedstaaten.

Wenn das System zur Meldung von Missständen von einem externen Dienstleister betrieben wird, so muss der für die Verarbeitung Verantwortliche einen Vertrag über die Zweckdienlichkeit abschließen und insbesondere alle geeigneten Maßnahmen treffen, um die Sicherheit der verarbeiteten Informationen während des gesamten Prozesses zu gewährleisten.

ii) Vertraulichkeit von Meldungen mit Hilfe von Systemen zur Meldung von Missständen

Die Vertraulichkeit der Meldungen ist eine grundlegende Anforderung, um den Verpflichtungen gemäß Richtlinie 95/46/EG zu entsprechen und die Sicherheit der Verarbeitung einzuhalten.

Um den Zweck zu erfüllen, für den ein System zur Meldung von Missständen eingerichtet wurde und Personen zu ermutigen, das System zu nutzen und Tatsachen zu melden, die Fehlverhalten oder illegale Aktivitäten des Unternehmens aufzeigen können, ist es wesentlich, dass die meldende Person angemessen geschützt wird, indem die Vertraulichkeit der Meldung garantiert wird und Dritte daran gehindert werden, ihre Identität in Erfahrung zu bringen.

Unternehmen, die Verfahren zur Meldung von Missständen einrichten, sollten die angemessenen Maßnahmen treffen, um sicherzustellen, dass die Identität des Hinweisgebers vertraulich bleibt und während aller Untersuchungen der beschuldigten Person nicht enthüllt wird. Wenn sich jedoch herausstellt, dass eine Meldung nicht begründet ist und der Hinweisgeber böswillig eine falsche Angabe gemacht hat, wird die beschuldigte Person möglicherweise eine Klage wegen Verleumdung oder Diffamierung erheben wollen; in diesem Fall muss die Identität des Hinweisgebers gegebenenfalls der beschuldigten Person preisgegeben werden, wenn das einzelstaatliche Recht dies zulässt. Einzelstaatliche Rechtsvorschriften und Grundsätze über die Meldung von Missständen im Bereich der Corporate Governance sehen auch vor, dass der Hinweisgeber vor Vergeltungsmaßnahmen, weil er das Verfahren genutzt hat, geschützt werden muss, beispielsweise Disziplinarmaßnahmen oder diskriminierende Maßnahmen des Unternehmens oder der Organisation.

Die Vertraulichkeit personenbezogener Daten muss bei der Erhebung, der Offenlegung und der Speicherung gewährleistet sein.

6. Management von Systemen zur Meldung von Missständen

Bei Systemen zur Meldung von Missständen muss sorgfältig erwogen werden, wie die Meldungen gesammelt und gehandhabt werden sollen. Die Gruppe bevorzugt zwar die interne Handhabung des Systems, erkennt aber an, dass Unternehmen sich möglicherweise für die Nutzung externer Dienstleister entscheiden, an die sie Teile des Systems vergeben, hauptsächlich für die Sammlung der Meldungen. Diese externen Dienstleister müssen die strenge Verpflichtung zur Vertraulichkeit einhalten und sich verpflichten, die Datenschutzgrundsätze zu befolgen. Unabhängig von dem System, das ein Unternehmen eingerichtet hat, muss es insbesondere Artikel 16 und 17 der Richtlinie einhalten.

i) Bestimmte interne organisatorische Einheiten für das Management von Systemen zur Meldung von Missständen

Innerhalb des Unternehmens oder der Gruppe muss eine bestimmte organisatorische Einheit eingerichtet werden, die für die Handhabung der Meldungen der Hinweisgeber und die Durchführung der Untersuchung zuständig ist.

Diese Organisation muss aus besonders ausgebildeten und für diesen Zweck abgestellten Personen bestehen, deren Zahl begrenzt ist und die vertraglich verpflichtet sind, besondere Verpflichtungen hinsichtlich der Vertraulichkeit einzuhalten.

Dieses System zur Meldung von Missständen sollte streng von anderen Abteilungen des Unternehmens getrennt werden, beispielsweise der Personalabteilung.

Es soll sicherstellen, dass die erhobenen und verarbeiteten Informationen, soweit erforderlich, ausschließlich an die Personen weitergeleitet werden, die innerhalb des Unternehmens oder der Gruppe, zu der das Unternehmen gehört, besonders für die Untersuchung oder die erforderlichen Folgemaßnahmen hinsichtlich der gemeldeten Tatsachen zuständig sind. Personen, die diese Informationen erhalten, sollen sicherstellen, dass die erhaltenen Informationen vertraulich behandelt werden und Sicherheitsmaßnahmen unterliegen.

ii) Die Möglichkeit, externe Dienstleister heranzuziehen

Wenn Unternehmen oder Unternehmensgruppen sich an externe Dienstleister wenden, um einen Teil der Verwaltung des Systems zur Meldung von Missständen nach außen zu vergeben, behalten sie dennoch die Verantwortung für die daraus hervorgehenden Verarbeitungen, weil diese Dienstleister lediglich als Auftragsverarbeiter im Sinne der Richtlinie 95/46/EG tätig werden.

Externe Dienstleister können Unternehmen sein, die Call Center betreiben oder spezialisierte Unternehmen oder Anwaltskanzleien, die auf die Sammlung von Meldungen spezialisiert sind und zuweilen sogar Teile der erforderlichen Untersuchungen durchführen.

Auch diese externen Dienstleister müssen die Grundsätze der Richtlinie 95/46/EG einhalten. Sie müssen durch einen Vertrag mit dem Unternehmen, für das das System betrieben wird, sicherstellen, dass sie die Informationen nach den Grundsätzen der Richtlinie 95/46/EG erheben und verarbeiten; und dass sie die Informationen nur für die spezifischen Zwecke verarbeiten, für die sie gesammelt wurden. Insbesondere halten sie sich an strenge Verpflichtungen in Bezug auf die Vertraulichkeit und leiten die verarbeiteten Informationen nur an bestimmte Personen in dem Unternehmen oder der Organisation mit, das/die für die Untersuchung oder für die erforderlichen Maßnahmen zur Weiterverfolgung der gemeldeten Tatsachen zuständig ist. Sie halten ferner die Speicherfristen ein, an die der für die Verarbeitung Verantwortliche gebunden ist. Das Unternehmen, das diese Mechanismen anwendet, muss in seiner Eigenschaft als für die Verarbeitung Verantwortlicher regelmäßig prüfen, ob die externen Dienstleister die Grundsätze der Richtlinie einhalten

iii) Grundsatz der Untersuchung von Meldungen über EU-Unternehmen in der EU und Ausnahmen

Die Art und Struktur multinationaler Gruppen bringt es mit sich, dass die Fakten und Ergebnisse aller Berichte möglicherweise innerhalb der gesamten Gruppe verbreitet werden müssen, auch außerhalb der EU.

Unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit sollten Art und Schweregrad des mutmaßlichen Verstoßes im Prinzip darüber entscheiden, auf welcher Ebene und damit in welchem Land der Bericht bewertet werden sollte. In der Regel ist die Gruppe der Auffassung, dass die Gruppen Berichte lokal handhaben sollten, d. h. in einem EU-Land, und nicht alle Informationen automatisch mit anderen Unternehmen der Gruppe teilen sollten.

Die Gruppe erkennt jedoch einige Ausnahmen von dieser Regel an.

Die über das System zur Meldung von Missständen eingegangenen Daten können innerhalb der Gruppe weitergeleitet werden, wenn eine solche Weiterleitung für die Untersuchung erforderlich ist, je nach Art oder Schweregrad des gemeldeten Verstoßes, oder wenn sie auf die Struktur der Gruppe zurückzuführen ist. Eine solche Weiterleitung wird als notwendig für die Anforderungen der Untersuchung erachtet, beispielsweise wenn der Bericht einen Partner einer anderen rechtlichen Einheit innerhalb der Gruppe beschuldigt, ein hochrangiges Mitglied oder einen Manager des betroffenen Unternehmens. In diesem Fall dürfen Daten nur unter

vertraulichen und sicheren Bedingungen an die zuständige Organisation der empfangenden rechtlichen Einheit weitergeleitet werden, die gleichwertige Garantien hinsichtlich der Verwaltung der Berichte aus dem System zur Meldung von Missständen bietet wie die Organisation, die für die Handhabung solcher Berichte in dem EU-Unternehmen zuständig ist.

7. Übermittlung in Drittländer

Artikel 25 und 26 der Richtlinie 95/46/EG gelten, wenn personenbezogene Daten in Drittländer übermittelt werden. Die Anwendung der Bestimmungen der Artikel 25 und 26 wird dann relevant, wenn das Unternehmen Teile der Verwaltung des Systems für die Meldung von Missständen an einen Dritten ausgelagert hat, der außerhalb der EU niedergelassen ist oder wenn die in Berichten gesammelten Daten innerhalb der Gruppe verbreitet werden und damit auch Unternehmen außerhalb der EU erreichen.

Diese Übermittlungen werden wahrscheinlich vor allem bei EU-Tochtergesellschaften von Unternehmen aus Drittländern auftreten.

Wenn das Drittland, in das die Daten geschickt werden sollen, kein angemessenes Schutzniveau nach Artikel 25 der Richtlinie 95/46/EG gewährleistet, können Daten übermittelt werden, wenn:

[1] der Empfänger personenbezogener Daten eine in den USA niedergelassene Einheit ist, die die Grundsätze des „sicheren Hafens“ angenommen hat;

[2] der Empfänger einen Übermittlungsvertrag mit dem EU-Unternehmen geschlossen hat, das die Daten übermittelt, in dem letzteres ausreichende Garantien bietet, beispielsweise auf der Grundlage der Standardvertragsklauseln der Europäischen Kommission nach ihren Entscheidungen vom 15. Juni 2001 oder 27. Dezember 2004;

[3] der Empfänger verbindliche Unternehmensregelungen eingeführt hat, die von den zuständigen Datenschutzstellen genehmigt wurden.

8. Einhaltung der Meldepflicht

Nach Artikel 18 bis 20 der Datenschutzrichtlinie müssen Unternehmen, die Verfahren zur Meldung von Missständen einführen, die Meldepflicht bei oder die Vorabkontrolle durch die einzelstaatlichen Datenschutzstellen einhalten.

In den Mitgliedstaaten, die ein solches Verfahren vorsehen, unterliegt die Verarbeitung möglicherweise einer Vorabkontrolle durch die nationale Datenschutzstelle, soweit diese Verarbeitungen spezifische Risiken für die Rechte und Frei-

heiten der Betroffenen beinhalten können. Dies könnte der Fall sein, wenn einzelstaatliche Rechtsvorschriften die Verarbeitung von Daten über mutmaßliche Straftaten von privaten rechtlichen Einheiten unter besonderen Bedingungen ermöglichen, unter anderem die Vorabkontrolle durch die zuständige einzelstaatliche Aufsichtsbehörde. Dies könnte ferner der Fall sein, wenn die einzelstaatliche Behörde der Auffassung ist, dass die Verarbeitung gemeldete Personen möglicherweise von einem Recht, einem Vorteil oder einem Vertrag ausschließt. Die Abwägung, ob solche Verarbeitungen unter die Vorabkontrolle fallen, obliegt der einzelstaatlichen Gesetzgebung und den Praktiken der nationalen Datenschutzbehörde.

V. SCHLUSSFOLGERUNGEN

Die Gruppe erkennt an, dass Verfahren zur Meldung von Missständen ein sinnvoller Mechanismus sein können, um ein Unternehmen oder eine Organisation bei der Überwachung der Einhaltung von Regeln und Vorschriften im Zusammenhang mit der Unternehmensführung zu unterstützen, insbesondere in Bezug auf Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und Vorschriften über die Bekämpfung von Korruption und Banken- und Finanzkriminalität und Strafrecht. Sie können ein Unternehmen bei der ordnungsgemäßen Umsetzung der Grundsätze der Unternehmensführung und der Ermittlung von Tatsachen unterstützen, die sich auf die Position des Unternehmens auswirken würden.

Die Gruppe weist darauf hin, dass die Einrichtung von Verfahren zur Meldung von Missständen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und Bekämpfung von Korruption und Banken- und Finanzkriminalität, auf die sich die vorliegende Stellungnahme bezieht, im Einklang mit den Grundsätzen des Datenschutzes gemäß Richtlinie 95/46/EG erfolgen muss. Sie ist der Auffassung, dass die Einhaltung dieser Grundsätze den Unternehmen und Systemen zur Meldung von Missständen dabei hilft, die richtige Funktionsweise solcher Verfahren zu gewährleisten. Tatsächlich ist es wesentlich, dass bei der Umsetzung eines Verfahrens zur Meldung von Missständen das grundlegende Recht auf den Schutz personenbezogener Daten, sowohl des Hinweisgebers als auch der beschuldigten Person, während des gesamten Meldeverfahren gewährleistet wird.

Die Gruppe weist darauf hin, dass die Datenschutzgrundsätze nach Richtlinie 95/46/EG vollständig auf die Verfahren zur Meldung von Missständen angewandt werden müssen, insbesondere hinsichtlich der Rechte der beschuldigten Person auf Mitteilung, Zugang, Berichtigung und Löschung von Daten. In Anbetracht der unterschiedlichen Interessen erkennt die Gruppe jedoch an, dass die Ausübung dieser Rechte in ganz bestimmten Fällen beschränkt werden kann, um ein

Gleichgewicht zwischen dem Recht auf Schutz der Privatsphäre und den Interessen des Systems herzustellen. Derartige Beschränkungen sollten jedoch restriktiv gehandhabt und nur in dem Maß angewandt werden, das erforderlich ist, um die Ziele des Systems zu erreichen.

Brüssel, 1. Februar 2006

Für die Gruppe

Der Vorsitzende
Peter Schaar

Stellungnahme 3/2006 zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (WP 119)

Angenommen am 25. März 2006

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

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

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

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

Am 21. Februar 2006 nahm der Rat die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher

[1] ABl. L 281 vom 23.11.1995, S. 31; http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_de.htm.

elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG[2] an. Zuvor hatte das Europäische Parlament den im Zuge der Verhandlungen mit dem Rat geänderten Kommissionsvorschlag KOM (2005) 438[3] genehmigt und am 14. Dezember 2005 eine legislative Entschließung (C6-0293/2005 – 2005/0182(COD)) angenommen.

In ihrer letzten Stellungnahme WP 113 zum Richtlinienentwurf vom 21. Oktober 2005 äußerte die Datenschutzgruppe Bedenken, da die Bestimmungen der Richtlinie für alle europäischen Bürger und deren Privatsphäre weit reichende Konsequenzen haben werden. Die Entscheidung, wonach zur Bekämpfung schwerer Straftaten Daten auf Vorrat gespeichert werden dürfen, stellt ein absolutes Novum mit historischem Ausmaß dar. Sie hat direkte Auswirkungen auf den Alltag der Bürger in Europa und kann eine Gefahr für deren Grundwerte und Freiheiten darstellen. Die Datenschutzgruppe weist erneut auf die Überlegungen und Bedenken der oben erwähnten Stellungnahme hin, die nach wie vor Gültigkeit haben. Es ist daher äußerst wichtig, dass die Umsetzung der Richtlinie in jedem Mitgliedstaat von Maßnahmen begleitet wird, die den Eingriff in die Privatsphäre begrenzen.

Die Artikel-29-Datenschutzgruppe stellt fest, dass in der Richtlinie angemessene und besondere Schutzvorkehrungen fehlen, die bei der Verarbeitung der Verbindungsdaten angezeigt sind, und es so zu einer unterschiedlichen Auslegung und Umsetzung in den Mitgliedstaaten kommen kann. Solche Vorkehrungen sind jedoch notwendig, um die wesentlichen Interessen des Einzelnen gemäß der Richtlinie 2002/58/EG zu schützen, insbesondere was das Recht auf Vertraulichkeit bei der Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste betrifft. Die Datenschutzgruppe ist der Ansicht, dass eine einheitliche Auslegung und Umsetzung der Bestimmungen ebenfalls sehr wichtig ist, damit die Bürger überall in der Europäischen Union den gleichen Schutz genießen.

Daher schlägt die Datenschutzgruppe eine einheitliche EU-weite Umsetzung der Richtlinie vor. Dieser Ansatz soll eine einheitliche Anwendung der Richtlinienbestimmungen und einen bestmöglichen Schutz personenbezogener Daten gewährleisten. Dahinter steht auch der Gedanke, dass die erheblichen Kosten gesenkt werden sollen, die den Diensteanbietern bei der Umsetzung der Richtlinienbestimmungen entstehen.

Damit die Richtlinienbestimmungen einheitlich umgesetzt und die Anforderungen gemäß Artikel 8 des Europäischen Menschenrechtsübereinkommens erfüllt

---

2 Abl. L 105 vom 13.4.2006, S. 54.

3 ABl. C 49 vom 28.2.2006, S. 42.

werden, müssen die Mitgliedstaaten angemessene und besondere Schutzvorkehrungen einführen. Diese sollten mindestens Folgendes umfassen:

1) **Angabe des Zwecks:** Die Daten dürfen nur für bestimmte Zwecke gespeichert werden. Dazu muss der Begriff „schwere Straftat" klar definiert werden. Jede weitere Verarbeitung muss durch besondere Schutzvorkehrungen ausgeschlossen oder streng begrenzt werden.

2) **Begrenzter Zugang:** Zugang zu den Daten dürfen nur eigens benannte Strafverfolgungsbehörden erhalten, und zwar zum Zwecke der Ermittlung, Feststellung und Verfolgung der in dieser Richtlinie genannten Straftaten. Eine Liste dieser Strafverfolgungsbehörden muss veröffentlicht werden. Alle Datenabrufe müssen protokolliert und die Aufzeichnungen den Datenschutzbehörden zu Kontrollzwecken zur Verfügung gestellt werden.

3) **Datensparsamkeit:** Es sollten so wenig Daten wie möglich auf Vorrat gespeichert werden. Die Aufstellung der zu speichernden Daten darf nur dann geändert werden, wenn erwiesenermaßen die Notwendigkeit hierzu besteht.

4) **Kein Datenschürfen:** Bei der Ermittlung, Feststellung und Verfolgung der in der Richtlinie aufgeführten Straftaten dürfen die dabei auf Vorrat gespeicherten Daten nicht mittels eines groß angelegten Datenschürfens ausgewertet werden, etwa zum Zwecke der Feststellung des Reise- und Kommunikationsverhaltens von Personen, die von den Strafverfolgungsbehörden nicht zum Kreis der Verdächtigen gezählt werden.

5) **Richterliche/unabhängige Prüfung der Zugangsgenehmigung:** Der Zugang zu den Daten muss grundsätzlich in jedem Einzelfall von einer Justizbehörde ordnungsgemäß genehmigt werden, es sei denn, in einem Mitgliedstaat ist die Möglichkeit des Datenzugriffs bereits gesetzlich geregelt und unterliegt der Aufsicht durch eine unabhängige Instanz. Gegebenenfalls müssen in der Genehmigung die genauen Daten aufgeführt werden, die für den speziellen Fall benötigt werden.

6) **Datenspeicherung für andere Zwecke:** Anbieter öffentlicher elektronischer Kommunikationsdienste oder Betreiber öffentlicher Kommunikationsnetze dürfen Daten, die gemäß der Richtlinie über die Vorratsspeicherung allein zu Zwecken der öffentlichen Ordnung gespeichert wurden, nicht für andere (z. B. ihre eigenen) Zwecke auswerten.

7) **Getrennte Systeme:** Wichtig ist, dass die Systeme, in denen Daten zu Zwecken der öffentlichen Ordnung gespeichert werden, von den Systemen logisch getrennt werden, die die Anbieter für ihre geschäftlichen Zwecke verwenden.

8) **Sicherheitsmaßnahmen:** Die allgemeinen Anforderungen der Richtlinie müssen durch Mindeststandards ergänzt werden, die genau regeln, welche technischen und organisatorischen Sicherheitsvorkehrungen die Anbieter treffen müssen.

Die Datenschutzgruppe fordert die Mitgliedstaaten auf, die Umsetzung der Richtlinie über die Vorratsspeicherung zu koordinieren, um auf EU-Ebene ein einheitliches Vorgehen sicherzustellen und den weit reichenden Datenschutz gemäß den Richtlinien 1995/46/EG und 2002/58/EG aufrecht zu erhalten.

Brüssel, den 25. März 2006

Für die Datenschutzgruppe

Der Vorsitzende
Peter Schaar

Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP 128)

Angenommen am 22. November 2006

Zusammenfassung

Diese Stellungnahme enthält die Feststellungen der Artikel-29-Datenschutzgruppe zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide Interbank Financial Telecommunication (SWIFT)*.

In diesem Zusammenhang betont die Artikel-29-Gruppe, dass auch im Kampf gegen Terrorismus und Kriminalität die Grundrechte gewahrt bleiben müssen. Sie besteht daher auf der Achtung weltweiter Datenschutzprinzipien.

SWIFT ist ein weltweit agierender Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen. SWIFT speichert alle

Überweisungsdaten für 124 Tage in zwei Rechenzentren, von denen sich eines in der EU, das andere in den USA befindet – eine Form der Datenverarbeitung, die in diesem Dokument als „Spiegelung" bezeichnet wird. Die Zahlungsanweisungen enthalten personenbezogene Daten wie Namen des Zahlungsanweisenden oder des Zahlungsempfängers. Nach den Terrorangriffen vom September 2001 verlangte das US-Finanzministerium (UST) von SWIFT Zugang zu den in den USA gespeicherten Daten. SWIFT gab diesen Anordnungen nach, konnte aber gewisse Einschränkungen aushandeln. Aufgrund von Presseberichten Ende Juni/Anfang Juli 2006 erfuhr die Öffentlichkeit erstmals von dieser Angelegenheit.

SWIFT unterliegt als in Belgien ansässige Genossenschaft belgischem Datenschutzrecht, das die EU-Datenschutzrichtlinie 95/46/EG („die Richtlinie") umsetzt. Die Finanzinstitute in der EU, die sich der Dienstleistungen von SWIFT bedienen, unterliegen den jeweils nationalen Datenschutzvorschriften – in Umsetzung der Richtlinie – in den Mitgliedstaaten, in denen sie angesiedelt sind.

Die Artikel-29-Gruppe kommt zu folgenden Schlussfolgerungen:

– SWIFT und die Auftrag gebenden Finanzinstitute tragen als „für die Verarbeitung Verantwortlicher" im Sinne von Artikel 2 Buchstabe d) der Richtlinie gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten, wenn auch in unterschiedlichem Maße.

– Die Weiterverarbeitung von personenbezogenen Daten stellt angesichts der umfangreichen Anordnungen des US-Finanzministeriums (UST) einen weiteren Zweck dar, der mit der ursprünglichen kommerziellen Zweckbestimmung im Sinne von Artikel 6 Absatz 1 Buchstabe b) der Richtlinie, für die die personenbezogenen Daten erhoben wurden, nicht vereinbar ist.

– Weder SWIFT noch die Finanzinstitute in der EU haben die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informiert, wie dies gemäß Artikel 10 und Artikel 11 der Richtlinie vorgeschrieben ist, so insbesondere bezüglich der Weitergabe ihrer Daten an die Vereinigten Staaten.

– Die von SWIFT durchgeführten Kontrollmaßnahmen, so insbesondere in Bezug auf den Zugang des US-Finanzministeriums (UST) zu den Daten, ersetzen keineswegs die unabhängigen Überprüfungen, die von den gemäß Artikel 28 der Richtlinie eingerichteten Kontrollstellen hätten vorgenommen werden können.

– In Bezug auf die Übermittlung personenbezogener Daten an das Rechenzentrum in den USA kann sich SWIFT nicht auf Artikel 25 der Richtlinie berufen, um die Verarbeitung der personenbezogenen Daten zu rechtfertigen.

– Keiner der Ausnahmetatbestände nach Artikel 26 Absatz 1 der Richtlinie trifft auf die Verarbeitung von personenbezogenen Daten in den USA zu.

– SWIFT bediente sich auch nicht der nach Artikel 26 Absatz 2 der Richtlinie vorgesehenen Mechanismen, um von der belgischen Kontrollstelle für Datenschutz eine Genehmigung für die betreffende Datenverarbeitung zu erhalten.

– Die Artikel-29-Gruppe fordert SWIFT und die Finanzinstitute auf, unverzüglich Maßnahmen zu ergreifen, die die gegenwärtige unrechtmäßige Situation beenden.

– Außerdem verlangt die Artikel-29-Gruppe eine Klärung der Aufsichtsstrukturen bei SWIFT.

Die Artikel-29-Gruppe wird alle vorstehenden Punkte überwachen und einer Erfolgskontrolle unterziehen.

INHALT

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

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf deren Artikel 12 und 14 –

gibt folgende Stellungnahme ab:

[1] Amtsblatt L 281 vom 23.11.1995, S. 31, abzurufen über: http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm.

1. HINTERGRUND

Die unabhängigen Aufsichtsbehörden für den Datenschutz in der Europäischen Union[2] bewerten zurzeit die wichtige Frage der Übermittlung umfangreicher Finanzdaten von einem in der Europäischen Union ansässigen Unternehmen (SWIFT) an die US-Behörden. Die Umstände und die Einzelheiten dieser Übermittlung, insbesondere die Verarbeitung personenbezogener Daten von natürlichen Personen in Europa, erregten die Besorgnis der Datenschutzbehörden, die bei der Untersuchung des Datenflusses und bei der Analyse der Vereinbarkeit mit den europäischen Grundsätzen zum Schutz der Privatsphäre und insbesondere mit der Datenschutzrichtlinie („Richtlinie") mit gemeinsamen Kräften vorgehen.

1.1. Sachverhalt

Ende Juni/Anfang Juli 2006 beschäftigte sich die Presseberichterstattung in den europäischen und den US-Medien mit dem Thema und stellte die Rolle und die Zuständigkeit der *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) in Bezug auf die Übermittlung von personenbezogenen Daten an das *Office of Foreign Assets Control* (OFAC, Büro zur Kontrolle ausländischen Guthabens) des US-Finanzministeriums (UST) infrage. SWIFT ist eine in Belgien ansässige Genossenschaft, die als Geldüberweisungsdienst tätig ist. Dabei wurde aufgedeckt, dass personenbezogene Daten, die im Wege des SWIFT-Netzes für internationale Zahlungsanweisungen unter Verwendung des internationalen Bankleitzahl-Codes („BIC") oder des „SWIFT"-Codes erhoben und verarbeitet wurden, seit Ende 2001 aufgrund von Anordnungen nach US-amerikanischem Recht zu Zwecken der Terrorismusermittlungen an das US-Finanzministerium weitergegeben worden sind.

In der Folge dieser Presseberichterstattung gab SWIFT am 23. Juni 2006 eine erste Presseerklärung[3] heraus. Dieser Stellungnahme zufolge ist SWIFT „eine von der Banken-Industrie betriebene genossenschaftliche Gesellschaft, die ein sicheres und standardisiertes Interbankdatennetz betreibt, an das mehr als 7.800 Bank- und Investmenthäuser weltweit angeschlossen sind".

Die Europäische Kommission beschloss, diesen Fall genau zu verfolgen und forderte die belgischen Behörden im Juli 2006 auf, Informationen über die Umstände vorzulegen, unter denen SWIFT personenbezogene Daten verarbeitet, und ob diese dabei die belgischen Datenschutzvorschriften in Umsetzung der EU-Daten-

[2] Außer den in der EU zuständigen Behörden haben auch andere Datenschutzaufsichtsbehörden Untersuchungen in dieser Angelegenheit angestrengt, so in Australien, Kanada, Neuseeland, der Schweiz und Island.

[3] „Offizielle Stellungnahme von SWIFT" zu ihren Richtlinien zur Einhaltung von Recht und Gesetz, veröffentlicht unter http://www.swift.com/index.cfm?item_id=59897

schutzrichtlinie einhält. Die Kommission überprüft bei den Mitgliedstaaten auch, ob Banken, die zur Ausführung von Zahlungsaufträgen auf SWIFT zurückgreifen, bei der Verarbeitung personenbezogener Daten im Zusammenhang mit solchen Zahlungen die jeweiligen nationalen Datenschutzvorschriften einhalten.

Mit Entschließung vom 6. Juli 2006[4] forderte das Europäische Parlament die Mitgliedstaaten zur Überprüfung und Sicherstellung auf, dass auf nationaler Ebene keine Gesetzeslücken vorhanden sind, und dass die Datenschutzvorschriften der Gemeinschaft auch für die Zentralbanken gelten. In dieser Entschließung brachte das Europäische Parlament auch ernsthafte Bedenken bezüglich der jeweiligen Zweckbestimmungen der Übermittlung von Daten an das US-Finanzministerium (UST) zum Ausdruck. Ebenso missbilligte es energisch „jegliche heimlichen Vorgänge auf dem Hoheitsgebiet der EU", die die Privatsphäre von EU-Bürgern beeinträchtigen. Darüber hinaus erklärte es seine tiefe Besorgnis darüber, dass derartige Vorgänge stattfinden können, ohne dass die Bürger Europas und ihre parlamentarische Vertretung davon in Kenntnis gesetzt wurden. Schließlich forderte es die USA und ihre Geheim- und Sicherheitsdienste mit Nachdruck auf, im Geiste der guten Zusammenarbeit zu handeln und ihren Verbündeten alle Sicherheitsmaßnahmen mitzuteilen, die sie auf dem Hoheitsgebiet der EU durchführen wollen. Dabei wurde erörtert, dass es möglich ist, die Übermittlungen von Daten im Zusammenhang mit „illegalen Aktivitäten" zu nutzen, aber auch zur Weitergabe von Informationen über wirtschaftliche Tätigkeiten von bestimmten Einzelpersonen oder Ländern, die „Anlass zu entsprechenden Formen der Wirtschafts- und Industriespionage in großem Umfang" geben könnten. In der Entschließung werden die Mitgliedstaaten aufgefordert, die Ergebnisse ihrer Überprüfungen der Europäischen Kommission, dem Rat und dem Europäischen Parlament mitzuteilen.

Am 27. Juli 2006 kündigte der Vorsitzende der Artikel-29-Datenschutzgruppe an, dass die europäischen Datenschutzbehörden beschlossen haben, ihre Tätigkeiten zu koordinieren. Bei ihrer darauf folgenden Sitzung am 26. und 27. September 2006 nahm die Artikel-29-Gruppe eine erste Erörterung in Vollsitzung vor.[5]

Am 4. Oktober 2006 wurde die Angelegenheit bei einer öffentlichen Anhörung der Ausschüsse des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres und für Wirtschaft und Währung mit dem Finanzvorstand von

---

4 Entschließung des Europäischen Parlaments zur unberechtigten Überwachung von Banküberweisungsdaten aus dem SWIFT-System durch die US-Geheimdienste (P6_TAPROV(2006)0317)

5 Presseerklärungen der Artikel-29-Datenschutzgruppe: Presseerklärung der Artikel-29-Datenschutzgruppe zum Fall SWIFT vom 28.7.2006:
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf;
Press Presseerklärung der Artikel-29-Datenschutzgruppe zum Fall SWIFT vom 27.9.2006;
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf.

SWIFT und mit der Europäischen Zentralbank sowie mit anderen Teilnehmern erörtert[6].

Der Europäische Datenschutzbeauftragte machte einige Vorbemerkungen zu seinen Untersuchungen über die Rolle der Europäischen Zentralbank (EZB) gemäß der Verordnung (EG) 45/2001.[7]

Auf nationaler Ebene haben die Datenschutzbehörden Kontakt zu ihren jeweiligen Bankenorganisationen aufgenommen.

Die Datenschutzbehörde Belgiens untersuchte die Rechtmäßigkeit der Verarbeitung der Daten durch SWIFT. Im Laufe dieser Untersuchung nahm die belgische Datenschutzbehörde direkten Kontakt zu SWIFT auf, um sowohl den Umfang als auch das Ausmaß der Überwachung und Übermittlung von Daten festzustellen. Die belgische Datenschutzbehörde stellte in ihrer Entscheidung vom 27. September 2006 fest, dass die Übermittlung von personenbezogenen Daten durch SWIFT an die SWIFT-Außenstelle in den USA gegen das belgische Gesetz vom 8. Dezember 1992 zum Schutz der Privatsphäre bei der Verarbeitung von personenbezogenen Daten verstößt[8]. Insbesondere fand die belgische Datenschutzbehörde heraus, dass SWIFT wesentliche Bestimmungen bezüglich der Informationspflichten, der Begrenzung der Zweckbestimmung der Verarbeitung der personenbezogenen Daten und der Übermittlung der personenbezogenen Daten an Drittländer übertreten hat. Die belgische Datenschutzbehörde traf die Feststellung, dass SWIFT *„die grundlegenden europäischen Datenschutzgrundsätze intransparent, systematisch, massiv und dauerhaft verletzt hat“*.

Die Artikel-29-Gruppe möchte auf der Grundlage der bei diesen Untersuchungen zusammengetragenen Informationen untersuchen, ob SWIFT die Datenschutzgrundsätze eingehalten hat, die in der Datenschutzrichtlinie enthalten sind und in allen Mitgliedstaaten durch nationale Datenschutzgesetze mit weitem Anwendungsbereich umgesetzt werden.

SWIFT übersandte dem Vorsitzenden der Artikel-29-Datenschutzgruppe auch eine Kopie ihrer Antwortschreiben an die belgische, die spanische und die französische Datenschutzbehörde[9].

---

6 Der vollständige Meinungsaustausch der öffentlichen Anhörung ist abrufbar unter http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default_en.htm

7 http://www.edps.europa.eu/Press/EDPS-2006-10-EN%20swift.pdf

8 http://www.privacycommission.be/communiqu%E9s/AV37-2006.pdf

9 Schreiben von SWIFT an den Vorsitzenden der Artikel-29-Datenschutzgruppe vom 31. Juli 2006.

1.2. Fakten

1.2.1. Datenverarbeitungstätigkeiten der SWIFT in Zahlen

Im Durchschnitt verarbeitet SWIFT täglich 12 Millionen Überweisungsdaten[10]. Der Gesamtumfang der jährlich verarbeiteten Überweisungsdaten belief sich beispielsweise im Jahr 2005 auf 2,5 Milliarden Überweisungsdaten, wovon 1,6 Milliarden für Europa und 467 Millionen für Nord-, Mittel- und Südamerika bestimmt waren. Die von SWIFT verarbeiteten Informationen betreffen die Überweisungsdaten der Finanzgeschäfte von Hunderttausenden von EU-Bürgern. Die europäischen Finanzinstitute (dieser Begriff ist nicht nur auf Banken beschränkt) nutzen den SWIFTNet-FIN-Service für die weltweite Übermittlung von Überweisungsdaten im Zusammenhang mit den jeweiligen Zahlungsanweisungen zwischen den Finanzinstituten. Diese Übermittlung erfolgt unabhängig davon, ob die Überweisungsdaten in der Europäischen Union (EU) bzw. im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland verarbeitet werden.

1.2.2. Kategorien der Verarbeitung personenbezogener Daten

Die über den SWIFTNet-FIN-Service übermittelten Überweisungsdaten enthalten personenbezogene Daten, wie z. B. die Namen des Zahlungsempfängers und des Zahlungsanweisenden. Die mit der Zahlung zusammenhängenden Überweisungsdaten können jedoch auch weitere Informationen enthalten, wie z. B. eine Geschäfts-/Bezugsnummer, damit der Zahlungsanweisende und der Zahlungsempfänger die jeweilige Zahlung mit ihren entsprechenden Buchungsunterlagen in Übereinstimmung bringen können. Darüber hinaus ist es bei bestimmten Arten von Überweisungsträgern möglich, nicht vorstrukturierte textliche Informationen anzufügen.

Abgesehen von ihren Verkaufsbüros in verschiedenen Ländern unterhält SWIFT zwei Rechenzentren, die in den beiden SWIFT-Außenstellen angesiedelt sind, von denen sich eine in einem EU-Mitgliedstaat und die andere in den Vereinigten Staaten befindet. In diesen Rechenzentren werden als Teil des SWIFTNet-FIN-Service alle von SWIFT verarbeiteten Überweisungsdaten für 124 Tage gespeichert und einer Form der Datenverarbeitung unterzogen, die in diesem Dokument als „Spiegelung“ bezeichnet wird, sozusagen als „Sicherungs- und Wiederherstellungsmechanismus“ für den Kunden im Falle von Streitigkeiten zwischen den Finanzinstituten oder Datenverlust. Nach dieser Zeitspanne werden die Daten gelöscht.

[10] SWIFT-Jahresbericht 2005, abzurufen unter http://www.swift.com/index.cfm?item_id=59684.

1.2.3. Anordnungen des US-Finanzministeriums (UST)

Seit den Terrorangriffen vom September 2001 erteilte das US-Finanzministerium (UST) dem SWIFT-Rechenzentrum in den Vereinigten Staaten vielfältige administrative Auflagen. Auf Anfrage erklärte SWIFT, dass sie bisher 64 Auflagen des UST erhalten und erfüllt hat.

Nach US-Recht handelt es sich bei einer administrativen Auflage um die Anordnung durch einen Regierungsbeamten einem Dritten gegenüber, durch die der Empfänger angewiesen wird, bestimmte Informationen vorzulegen.[11] Im vorliegenden Fall ist der Geltungsbereich der Anordnungen des US-Finanzministeriums (UST) materiell, territorial und zeitlich sehr weit gefasst und in den Auflagen und im Schriftverkehr über die Verhandlungen zwischen UST und SWIFT selbst bestimmt. Die Auflagen finden auf alle Geschäftsvorfälle Anwendung, die einen Zusammenhang mit Terrorismus aufweisen oder unter Umständen mit Terrorismus zusammenhängen können, beziehen sich auf *x* Länder und Gerichtsbarkeiten, auf *y* Daten oder auf Zeiträume *„von … bis …“*, die von einer bis zu mehreren Wochen reichen können, und gelten innerhalb und außerhalb der Vereinigten Staaten. Sie betreffen Überweisungsdaten von Interbankgeschäften innerhalb der USA, in die oder aus den USA wie auch Überweisungsdaten von außerhalb der USA, wie z. B. die Überweisungsdaten im Rahmen der EU.[12]

SWIFT handelte eine eigene Vereinbarung mit dem US-Finanzministerium über die Modalitäten aus, wie die Auflagen zu erfüllen sind. Aufgrund dieses Verfahrens behauptet SWIFT von sich, *„umfangreiche Sicherheiten und Zusicherungen hinsichtlich der Nutzung, der Vertraulichkeit, dem Ausmaß und der Kontrolle der Datensätze, die durch die Anweisung gefordert wurden“*, erhalten zu haben[13].

Den Feststellungen der belgischen Datenschutzbehörde zufolge wird die praktische Übermittlung der personenbezogenen Daten an das US-Finanzministerium (UST) vom SWIFT-Rechenzentrum in den USA in mehreren Schritten vollzogen. Es gibt kein unmittelbares Aussondern von individualisierten Daten, die in der SWIFT-Datenbank gespiegelt sind, sondern statt dessen die von SWIFT mit dem UST ausgehandelte Konstruktion des „Datenspeicher-Verfahrens“ („Black box“), das eine Übermittlung der Daten aus der gespiegelten SWIFT-Datenbank an

---

[11] Anhörung vor dem Justizausschuss des US-Senats, Unterausschuss für Terrorismusbekämpfung, technische und innere Sicherheit: „Mittel der Terrorismusbekämpfung sind: die Befugnis zur Erteilung von Anordnungen und die Inhaftierung von Terroristen bereits vor der Verurteilung durch Gerichtsverfahren“, Aussage von Rachel Brand, Principal Deputy Assistant Attorney General (etwa: Erster Stellvertretender Generalstaatsanwalt), Amt für Rechtspolitik, Justizministerium der Vereinigten Staaten, am 22. Juni 2004; http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf

[12] Vgl. Stellungsnahme der belgischen Datenschutzbehörde, B.2 (nichtamtliche Übersetzung ins Englische), Fußnote 8.

[13] „Offizielle Stellungnahme von SWIFT“ zu ihren Richtlinien zur Einhaltung von Recht und Gesetz, veröffentlicht unter http://www.swift.com/index.cfm?item_id=59897.

einen speziellen Datenspeicher ermöglichte. Sobald die Daten in den von den USA betriebenen Datenspeicher gelangen, führt das US-Finanzministerium (UST) zielgerichtete Durchsuchungsaktionen durch.

Der belgischen Datenschutzbehörde wurden weitere Einzelheiten über die Übermittlung von personenbezogenen Daten an das US-Finanzministerium (UST) zugänglich gemacht und sind ihrer Stellungnahme zu entnehmen[14].

2. GELTENDER RECHTLICHER RAHMEN FÜR DEN DATENSCHUTZ

2.1. Anwendbarkeit der Richtlinie 95/46/EG

Da in den Überweisungsdaten, die durch den SWIFTNet-FIN-Service übermittelt werden, personenbezogene Daten enthalten sind, ist die Artikel-29-Gruppe der Auffassung, dass die Datenschutzrichtlinie auf die Verarbeitung von personenbezogenen Daten im Wege des SWIFTNet-FIN-Service anwendbar ist.

Wie die Artikel-29-Gruppe betont, ist die Tatsache, dass die Verarbeitung von personenbezogenen Daten eine Begleitmaßnahme zu der Erbringung der eigentlichen Dienstleistung darstellt, nicht relevant für die Entscheidung darüber, ob die betreffende Organisation die Eigenschaft eines für die Verarbeitung von Daten Verantwortlichen erfüllt. Artikel 2 der Datenschutzrichtlinie enthält eine eindeutige Legaldefinition der Begriffe „Verarbeitung personenbezogener Daten" und „personenbezogene Daten". Fallen die von einem Rechtssubjekt durchgeführten Tätigkeiten unter diese Legaldefinitionen, so findet die Datenschutzrichtlinie Anwendung, und somit sind alle Tätigkeiten der Verarbeitung von Daten in uneingeschränkter Übereinstimmung mit dieser Richtlinie durchzuführen.

2.2. Auf SWIFT anzuwendendes Recht

Nach Artikel 4 Absatz 1 Buchstabe a) der Datenschutzrichtlinie wendet jeder Mitgliedstaat die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an, „(…) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt".

Die Zentrale von SWIFT befindet sich in La Hulpe, Belgien. SWIFT unterhält auch zwei Rechenzentren (davon eines in Europa und das andere in den USA, die im Rahmen der Vollspiegelung tätig sind). Darüber hinaus hat SWIFT mehrere

[14] Siehe Fußnote 8.

Verkaufsbüros im Vereinigten Königreich, in Frankreich, Deutschland, Italien, Spanien usw. Über die entscheidenden Fragen in Sachen Verarbeitung von personenbezogenen Daten und Übermittlung der Daten an das US-Finanzministerium (UST) wurde durch die Zentrale in Belgien entschieden.

Folglich unterliegt die Verarbeitung der personenbezogenen Daten durch SWIFT dem die europäische Datenschutzrichtlinie umsetzenden belgischem Recht, und zwar unabhängig davon, wo die Verarbeitung der betreffenden Daten stattfindet.

2.3. Auf die Finanzinstitute anzuwendendes Recht

Finanzinstitute, die für ihre internationalen Zahlungsaufträge die Dienstleistungen von SWIFT nutzen, sind bezüglich der Verarbeitungsvorgänge als für die Verarbeitung Verantwortliche anzusehen, und somit ergibt sich das geltende nationale Recht aus Artikel 4 Absatz 1 Buchstabe a) der Datenschutzrichtlinie; bezüglich der Verarbeitungsvorgänge der Organe und Einrichtungen der Gemeinschaft gilt Artikel 3 der Verordnung (EG) 45/2001[15]. Dies bedeutet, dass bei Finanzinstituten zwar harmonisierte, aber doch verschiedene Gesetze zur Anwendung kommen.

Die Artikel-29-Gruppe betont, dass die zur Umsetzung der europäischen Datenschutzrichtlinie erlassenen nationalen Datenschutzgesetze der jeweiligen Mitgliedstaaten anzuwenden sind, da die die Finanzgeschäfte von hunderttausenden von Bürgern betreffenden personenbezogenen Daten durch in der EU niedergelassene Einrichtungen (durch die Genossenschaft SWIFT selbst wie auch durch die Finanzinstitute, die den SWIFTNet-FIN-Service nutzen) verarbeitet werden.

3. ROLLE VON SWIFT UND DER FINANZINSTITUTE

Nach der Richtlinie hat der für die Verarbeitung Verantwortliche sicherzustellen, dass die Verpflichtungen bezüglich der Verarbeitung personenbezogener Daten erfüllt werden.

Fraglich ist, ob SWIFT und/oder die Finanzinstitute als „für die Verarbeitung von Daten Verantwortlicher“ oder als „Auftragsverarbeiter“ anzusehen sind.

Nach der Legaldefinition der Datenschutzrichtlinie ist ‚für die Verarbeitung Verantwortlicher‘ „die natürliche oder juristische Person, Behörde, Einrichtung oder

[15] 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.

jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Artikel 2 Buchstabe d)); ‚Auftragsverarbeiter‘ ist „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet“ (Artikel 2 Buchstabe e)).

3.1. Rolle von SWIFT

Nach ihrer eigenen Darstellung war SWIFT stets *„ausschließlich eine Plattform zum sicheren Austausch vertraulicher Finanzdaten zwischen Finanzinstitutionen. SWIFT ist keine Bank und unterhält auch keine Konten von Kunden“*. Diese Darstellung bildete auch die Grundlage für die von einigen Datenschutzbehörden der Mitgliedstaaten vorgenommenen Bewertungen zur Genehmigung von Daten verarbeitenden Tätigkeiten ihrer jeweiligen Banken.

Die internationalen Dienstleistungsstrukturen der SWIFT und die Vertragsvereinbarungen zwischen der SWIFT und den Finanzinstituten sind ziemlich komplex. Die Artikel-29-Gruppe weist jedoch darauf hin, dass diese Art von Struktur einschließlich der Rolle des Dienstleistungserbringers, der mit anderen Wirtschaftsbeteiligten zusammenarbeitet, keinen Einzelfall darstellt. Die SWIFT-Struktur scheint ein Beispiel für ein formelles genossenschaftlich organisiertes Netz zu sein. SWIFT wurde 1973 durch eine Gruppe von europäischen Banken ins Leben gerufen, die eine neue Standardmethode zur Übermittlung von Zahlungsanweisungen an die jeweiligen Korrespondenzbanken entwickeln wollten. Zu diesem Zweck wurde eine genossenschaftliche Gesellschaft mit beschränkter Haftung nach belgischem Recht gegründet.

Die Artikel-29-Gruppe verweist auf ähnliche Fälle von genossenschaftlich organisierten Netzen, wie z. B. im Falle von „Terminated Merchant Databases“ (Datenbanken über gekündigte Händler), die von VISA und Mastercard in Zusammenarbeit mit den Finanzinstituten zur Analyse der Risiken betrieben werden, die mit der Aufnahme eines bestimmten Händlers im ISA- oder Mastercard-System verbunden sind[16]. Die Artikel-29-Gruppe verweist auch auf die Fälle der Verrechnungs- (Clearing-) und Saldenausgleichssysteme für Finanzgeschäfte und auf die Sitzplatzreservierungssysteme für Flugreisende, bei denen die Reisebüros und die Fluggesellschaften einerseits und die Geschäftsführer dieser Systeme (wie z. B. Galileo) andererseits unterschiedliche Verantwortlichkeiten innehaben.

[16] Siehe z. B. die „Leitlinien für Terminated Merchant Databases“ der Artikel-29-Datenschutzgruppe, abzurufen unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf.

Unabhängig vom bürgerlich-rechtlichen oder handelsrechtlichen Vertragsverhältnis zwischen SWIFT und den Finanzinstituten, das auch den Begriff „Unterauftragnehmer“ mit umfassen kann, ist SWIFT unter datenschutzrechtlichen Gesichtspunkten nicht einfach nur ein „Unterauftragnehmer“ oder „Auftragsverarbeiter“ im Sinne von Artikel 2 der Datenschutzrichtlinie für die normale Verarbeitung von personenbezogenen Daten zu gewöhnlichen kommerziellen Zwecken. Die Fakten zeigen, dass sich SWIFT in den letzten Jahrzehnten weiterentwickelt hat und mehr tut, als nur im Auftrag ihrer Kunden zu handeln. Selbst wenn man für einen Moment unterstellt, SWIFT habe als „Auftragsverarbeiter“ gehandelt, so hat SWIFT doch spezifische Verantwortlichkeiten übernommen, die über den Komplex der für einen Auftrag geltenden Anweisungen oder der einem Auftragsverarbeiter obliegenden Pflichten hinausgehen und nicht mit ihrer Behauptung zu vereinbaren sind, nur ein reiner „Auftragsverarbeiter“ zu sein.[17] Die Geschäftsleitung von SWIFT handelt im Gefüge eines formellen genossenschaftlich organisierten Netzes, das sowohl über die Zweckbestimmungen als auch über die Mittel der Verarbeitung von personenbezogenen Daten im Rahmen des SWIFTNet-Services sowie auch darüber entscheidet, welche personenbezogenen Daten durch diesen SWIFTNet-Dienst verarbeitet werden. Die Geschäftsleitung von SWIFT entscheidet in eigener Verantwortung darüber, in welchem Umfang die mit der Verarbeitung zusammenhängenden Informationen den Finanzinstituten bereitgestellt werden. Die Geschäftsleitung von SWIFT ist in der Lage, über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten zu entscheiden, und zwar durch die Weiterentwicklung, die Vermarktung und die Veränderung von bestehenden oder neuen SWIFT-Dienstleistungen wie auch der Verarbeitung der Daten, so z. B. durch die Festlegung von für ihre Kunden verbindlichen Normen und Standards bezüglich der Form und des Inhalts von Zahlungsaufträgen, ohne dabei der Zustimmung der Finanzinstitute zu bedürfen. Auch leistet SWIFT bei der Verarbeitung personenbezogener Daten eine gewisse Wertschöpfung, so z. B. durch die Aufbewahrung und Richtigkeitsprüfung von personenbezogenen Daten und den Schutz von personenbezogenen Daten mittels hoher Sicherheitsstandards. Die Geschäftsleitung von SWIFT verfügt über die Befugnisse, bei der Verarbeitung der Daten Entscheidungen mit Gestaltungskraft zu treffen, so z. B. über die Sicherheitsstandards und die Standorte der Rechenzentren. Und schließlich besitzt die Geschäftsleitung von SWIFT uneingeschränkte Autonomie bei der Aushandlung und Kündigung der jeweiligen Dienstleistungsvereinbarungen wie auch bei der Ausarbeitung und Änderung der verschiedenen Vertragsdokumente und Geschäftspolitiken[18]. Die vorstehenden Merkmale fallen unter die praktischen und die rechtlichen Mittel der Verarbeitung.

[17] Der Auftragsverarbeiter von Daten muss in jedem Falle die Anforderungen der Datenschutzrichtlinie erfüllen, siehe z. B. Art. 17 Absatz 3 über Maßnahmen zur Sicherheit der Verarbeitung.

[18] Vgl. Ziffer 4.5.3 der allgemeinen Geschäftsbedingungen, wonach „die Zustimmung des Kunden zu einer solchen Verarbeitung vermutet wird…“.

In der Angelegenheit der Übermittlung von personenbezogenen Daten an das US-Finanzministerium (UST) hat SWIFT die Entscheidung getroffen, die Auflagen der USA zu erfüllen. Auch hat SWIFT die Initiative ergriffen, die Bedingungen für die Weitergabe der personenbezogenen Daten an das US-Finanzministerium (UST) in undurchsichtiger Art im Rahmen eines Verwaltungsschriftwechsels mit diesem auszuhandeln. So hat SWIFT auch bewusst entschieden, die betroffenen Finanzinstitute nicht von diesen Verhandlungen in Kenntnis zu setzen. Tatsächlich beeinträchtigten die von SWIFT erreichten und auch ausgeübten Kontrollfunktionen den Zweck und das Ausmaß der Übermittlung von Daten an das US-Finanzministerium (UST). Jedoch übersteigen diese Maßnahmen bei Weitem die normalen Funktionen eines Auftragsverarbeiters von Daten, da bei diesem zu unterstellen ist, dass er in Bezug auf die Anweisungen des für die Verarbeitung der Daten Verantwortlichen keinerlei Autonomie besitzt.

Zwar stellt sich SWIFT selbst als Auftragsverarbeiter der Daten dar, und einige Elemente könnten auch vermuten lassen, dass SWIFT bisher in bestimmten Fällen als Auftragsverarbeiter im Auftrag der Finanzinstitute tätig wurde, doch ist die Artikel-29-Gruppe nach Erwägung des tatsächlichen Handlungsspielraums, über den SWIFT in den vorgenannten Situationen verfügt, der Auffassung, dass SWIFT vielmehr ein für die Verarbeitung Verantwortlicher im Sinne von Artikel 2 Buchstabe d) der Datenschutzrichtlinie ist, und zwar sowohl für die normale Verarbeitung von personenbezogenen Daten im Rahmen des SWIFTNet-Service als auch für die weitere Verarbeitung im Rahmen der Weitergabe von personenbezogenen Daten an das US-Finanzministerium (UST).

3.2. Rolle der Finanzinstitute

Welche Rolle die Finanzinstitute bei der Inanspruchnahme des SWIFTNet-FIN-Service spielen, ist folgendermaßen zu bewerten: Einige Finanzinstitute waren von SWIFT nicht vollständig über das Ausmaß und die genauen Merkmale der Verarbeitung und Spiegelung der personenbezogenen Daten informiert worden, so auch nicht hinsichtlich der weiteren Übermittlung der gespiegelten personenbezogenen Daten an das US-Finanzministerium (UST). Nach der Aufdeckung dieser Fakten am und nach dem 23. Juni 2006 ist diese Situation jedoch allen Finanzinstituten bekannt, die im Rahmen von internationalen Geldüberweisungen personenbezogene Daten über den SWIFTNet-FIN-Service versenden.

Von den Finanzinstituten, die mit SWIFT arbeiten, wird vermutet und erwartet, dass sie ihren Einfluss auf die Politik der Genossenschaft in gewissem Umfang beibehalten. Einige Finanzinstitute sind im Vorstand von SWIFT vertreten; auch wurde die derzeitige Managementstruktur von SWIFT ursprünglich so ausgestaltet, dass die Banken und Finanzinstitute auch weiterhin Einfluss auf die Entscheidungsprozesse von SWIFT nehmen können. Diese Finanzinstitute sind

daher so einzustufen, dass sie an der Entscheidung des Zwecks und der Mittel der Verarbeitung bei der Genossenschaft, deren Mitglieder sie sind, beteiligt sind. Auch haben sie direkten Kontakt mit den betreffenden natürlichen Personen und spielen eine wesentliche Rolle bei der Durchführung der internationalen Zahlungsaufträge ihrer Kunden.

Dabei ist jedoch stets zu berücksichtigen, dass die Finanzinstitute eigenständig sind und auf der Interbankebene ihre eigenen Ziele verfolgen können. Die Artikel-29-Gruppe hält daher fest, dass die Finanzinstitute im Rahmen des Interbankverkehrs häufig wichtige Entscheidungen über die Übermittlung personenbezogener Daten an SWIFT treffen, und dies oftmals sogar ohne ihre Kunden davon in Kenntnis zu setzen. Dies ergibt sich aus folgenden Gesichtspunkten:

- Auf der Interbankebene entscheiden die Finanzinstitutionen häufig eigenständig über die Mittel, die zur Abwicklung von Zahlungsanweisungen eingesetzt werden. Zur Übermittlung der Überweisungsdaten innerhalb des Interbanksystems können sie alternative oder konkurrierende Dienste nutzen oder entwickeln (z. B. elektronische Post, Fax, Telefon). Die auf dieser Ebene getroffene Auswahl entscheidet umfassend über die jeweiligen Merkmale des Schutzes der Privatsphäre bei den von den Finanzinstituten abgewickelten Zahlungsanweisungen. Wird ein Interbank-Service gewählt, so haben die Finanzinstitute angesichts der Vielfalt der Dienstleistungen auf der Interbankebene freie Hand, sich von anderen Elementen als der Informationssicherheit leiten zu lassen – die natürlich immer erforderlich ist – so z. B. von der jeweiligen Geschäftspolitik eines professionellen Dienstleisters in Sachen Schutz der Privatsphäre. Die Finanzinstitute haben die Wahlmöglichkeit zwischen den strengen Maßnahmen eines bestimmten Anbieters zum Schutz der Privatsphäre und einer anderen Lösung, nämlich z. B. der Nutzung eines eigenen virtuellen Netzes als höchstmögliche Schutzgarantie für das Vertrauen ihrer Kunden und für ihre Dienstleistungen.

- Die Finanzinstitute akzeptieren und erfüllen das für den SWIFTNet-FIN-Service geltende vertragliche Rahmenwerk[19]. Die Vertragsunterlagen (Maßnahmen zur Wiedergewinnung und Abfrage von Daten[20]) und die SWIFT-Richtlinien zur Einhaltung von Recht und Gesetz weisen die Kunden von SWIFT auf den allgemeinen Grundsatz hin, dass personenbezogene Daten weitergegeben

[19] Vertraglicher Bestandteil ist auch das „SWIFT-Benutzerhandbuch", das Angaben zu den zu verwendenden standardisierten Überweisungsdaten enthält.

[20] Hier findet sich folgende Regelung: *„Zur Vermeidung von Unklarheiten können diese Maßnahmen oder ganz allgemein die Verpflichtungen von SWIFT, das Vertrauen ihrer Kunden zu schützen, niemals so ausgelegt werden, dass SWIFT von der Wiedergewinnung und Abfrage, der Verwendung oder der Offenlegung der Zahlungsverkehrs- oder der Überweisungsdaten abgehalten werden kann, wenn diese Tätigkeiten als angemessen und notwendig anzusehen sind, um eine berechtigte Auflage oder ein anderes gesetzliches Verfahren, die durch eine Gericht oder eine andere zuständige Behörde angeordnet werden, zu erfüllen"*. Vgl. Stellungnahme der belgischen Datenschutzbehörde, D.2, Fußnote 8.

werden, wenn diese Gegenstand einer Auflage sind, die entweder gegenüber dem Kunden oder gegenüber SWIFT angeordnet wird. Der Stellungnahme der belgischen Datenschutzbehörde zufolge behauptete SWIFT, die Zahl der gegenüber Finanzinstituten angeordneten Auflagen könne sich auf Tausende oder sogar Zehntausende pro Jahr belaufen. Daher darf angezweifelt werden, dass Finanzinstitute, die auf dem internationalen Zahlungsmarkt tätig sind, den allgemeinen Grundsatz der angeordneten Auflagen nicht kennen.

- Die Finanzinstitute müssen die möglichen Auswirkungen und die Risiken für den Schutz der Privatsphäre bewerten, einschließlich der Risiken für den Schutz der Privatsphäre ihrer Kunden, die sich aus der Nutzung des SWIFT-Net-FIN-Service ergeben, dessen sie sich als professionelle Dienstleister bedienen. Es ist daher wichtig, zu überprüfen, ob die Richtlinien zum Schutz der Privatsphäre des die Zahlungsanweisung erteilenden Finanzinstituts Klauseln bezüglich dieser Risiken enthalten.

- Angesichts der Tatsache, dass die Finanzinstitute bei der Erteilung von Zahlungsanweisungen im Auftrag ihrer Kunden handeln, sind diese nicht befugt, die dazu erforderlichen Daten zu anderen Zwecken als zur Zahlungsanweisung weiterzugeben. Ist einem Finanzinstitut bekannt, dass SWIFT die ihr anvertrauten Daten auch noch in anderer Weise als nur zur Zahlungsanweisung verwendet, und bedient sich dieses Finanzinstitut trotzdem auch weiterhin der Dienste von SWIFT, so ist die Frage nach der Rechtsgrundlage für derartige Überweisungen und Verwendungen zu stellen: Besteht nämlich keine besondere Vereinbarung zwischen dem Finanzinstitut und seinen Kunden, so scheint es nicht gerechtfertigt, SWIFT Bankdaten noch zu anderen Zwecken als zu der angegebenen und dem Kunden bestätigten Dienstleistung anzuvertrauen.

Folglich erfüllen die Finanzinstitute die Eigenschaft des für die Verarbeitung Verantwortlichen im Sinne des Artikels 2 Buchstabe d) der Datenschutzrichtlinie nicht nur in Bezug auf ihre eigenen Datenverarbeitungstätigkeiten, sondern sie tragen auch in gewissem Umfang Verantwortung für die Datenverarbeitungstätigkeiten von SWIFT. Die Tatsache, dass sich die Managementstruktur der genossenschaftlichen Gesellschaft SWIFT anscheinend im Laufe der Zeit dahin weiterentwickelt hat, dass die Geschäftsleitung von SWIFT unabhängiger geworden ist als dies ursprünglich vorgesehen war, enthebt ihre Gründer, d. h. die Finanzinstitute nicht der Pflicht, ihre Eigenschaft als für die Verarbeitung der Daten Verantwortliche im Sinne der Datenschutzrichtlinie beizubehalten.

Aufgrund der vorstehenden Gesichtspunkte ist die Artikel-29-Gruppe der Auffassung, dass ausreichend Anhaltspunkte zur Stützung der Einschätzung vorliegen, der zufolge die genossenschaftliche Gesellschaft SWIFT und die Finanzinstitute, sofern sie vertreten sind, gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten durch den SWIFTNet-FIN-Service tragen.

Gemeinsame Verantwortung bedeutet jedoch nicht unbedingt auch gleiche Verantwortung. Auch wenn SWIFT die Hauptverantwortung für die Verarbeitung personenbezogener Daten durch den SWIFTNet-FIN-Service trägt, sind die Finanzinstitute in gewissem Umfang für diese Verarbeitung der personenbezogenen Daten ihrer Kunden in diesem Dienst mitverantwortlich.

3.3. Rolle der Zentralbanken

Unter Berücksichtigung der unterschiedlichen Rollen, die sie in Bezug auf SWIFT und bei der Aufsicht im Sektor der Finanzgeschäfte spielen, ist auch die Beteiligung der Zentralbanken zu untersuchen. Zunächst unterliegt SWIFT im Rahmen der Zusammenarbeit der gemeinsamen Aufsicht durch die Zentralbanken der G-10-Staaten (Gruppe der G-10)[21]. Diese Aufsicht konzentriert sich vorwiegend auf die Sicherstellung, dass SWIFT über effektive Kontrollen und Verfahren zur Bewältigung von Risiken für die finanzielle Stabilität und das reibungslose Funktionieren der Finanzinfrastrukturen verfügt. Darüber hinaus „überprüfen die Aufsichtsführenden auch, wie SWIFT operationelle Risiken feststellt und entschärft, und sie können auch rechtliche Risiken, die Transparenz der jeweiligen Regelungen und Verfahrensmodalitäten und die Maßnahmen zur Gewährleistung des Auskunftsrechts für die Kunden überprüfen. Auch die strategische Ausrichtung von SWIFT kann mit dem Vorstand und den Führungskräften erörtert werden“[22]. Das wichtigste Instrument, das die Aufsichtsbehörde für die Aufsicht über SWIFT anwenden kann, ist die Einflussnahme und Überzeugungskraft („moralischer Druck“). Die Aufsichtsführenden können Empfehlungen an SWIFT formulieren; es ist jedoch auch klar, dass diese Aufsicht über SWIFT der Genossenschaft keinerlei Bescheinigungen, Sichtvermerke oder Genehmigungen durch die Zentralbanken erteilen kann.

Die Bestimmungen über die vertrauliche Behandlung von nicht öffentlich zugänglichen Informationen sind Bestandteil der Gemeinsamen Vereinbarung zwischen SWIFT und den Zentralbanken.

Die Gruppe der G-10 wurde im Laufe des Jahres 2002 über die Übermittlung von Daten an die US-Behörden in Kenntnis gesetzt. Die Gruppe war jedoch der Auffassung, dass diese Angelegenheit nicht in den Geltungsbereich ihrer Aufsichtsrolle fällt. Außerdem legten viele Zentralbanken die Gemeinsame Vereinbarung

[21] Die Gruppe der G-10 setzt sich aus folgenden Zentralbanken zusammen: Nationalbank von Belgien, Bank von Kanada, Deutsche Bundesbank, Europäische Zentralbank, Banque de France, Banca d’Italia, Bank von Japan, De Nederlandsche Bank, Sveriges Riksbank, Schweizerische Nationalbank, Bank of England und Federal Reserve System (USA), vertreten durch die Federal Reserve Bank of New York und den Gouverneursrat des Federal Reserve System.

[22] Analyse der finanziellen Stabilität 2005, veröffentlicht von der Nationalbank von Belgien und abrufbar über ihre Website www.nbb.be.

über die Vertraulichkeit als Hinderungsgrund aus, diese Angelegenheit an die zuständigen Behörden auf nationaler und europäischer Ebene zu verweisen. Daher befasste sich die Gruppe der G-10 auch nicht mit den datenschutzrechtlichen Folgen der Datenübermittlung an die US-Behörden und informierte weder die zuständigen Behörden noch drängte sie SWIFT dazu, dies zu tun.

Darüber hinaus trug der Präsident der Europäischen Zentralbank (EZB) bei der öffentlichen Anhörung des Europäischen Parlaments vor, dass die Zentralbanken der G-10 *„das Vorgehen von SWIFT in Bezug auf die Erfüllung der angeordneten Auflagen in keiner Weise abgesegnet haben. Denn wir hätten keine derartige Einwilligung erteilen können, selbst wenn wir dies gewollt hätten, da dies außerhalb unserer Zuständigkeiten liegt. Daher blieb SWIFT für ihre Entscheidungen alleinverantwortlich“*.[23]

Zweitens ist hervorzuheben, dass aufgrund der begrenzten Rolle, die die Zentralbanken derzeit bei der Aufsicht über SWIFT spielen, nicht ausgeschlossen ist, dass auch eine Zentralbank unter Umständen – wie jedes andere Finanzinstitut, das den SWIFTNet-Service nutzt – als ein (gemeinsamer) für die Verarbeitung Verantwortlicher anzusehen ist, nämlich immer dann, wenn sie als Kunde von SWIFT handelt (siehe oben, Abschnitt 3.2) und sie personenbezogene Daten zu Zwecken von Interbankgeschäften verarbeitet. Unter diesem Gesichtspunkt könnte die Tatsache, dass einige Zentralbanken über die Übermittlung von Daten an die US-Behörden informiert waren, als relevant berücksichtigt werden, um ihre Verantwortung als Nutzer des SWIFT-Systems festzustellen.

4. BEWERTUNG DER VEREINBARKEIT MIT DEN DATENSCHUTZVORSCHRIFTEN

4.1. Anwendung der Grundsätze in Bezug auf die Qualität der Daten und die Verhältnismäßigkeit (Artikel 6 der Datenschutzrichtlinie)

Gemäß Artikel 6 der Richtlinie sind personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise zu verarbeiten;[24] sie sind für festgelegte, eindeutige und rechtmäßige Zwecke zu erheben[25] und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterzuverarbeiten. Darüber hinaus müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht

[23] Jean-Claude Trichet: Stellungnahme des Präsidenten der EZB bei der öffentlichen Anhörung im Europäischen Parlament zur unberechtigten Überwachung von Banküberweisungsdaten aus dem SWIFT-System durch die US-Geheimdienste.

[24] Artikel 6 Absatz 1 Buchstabe a) der Richtlinie.

[25] Artikel 6 Absatz 1 Buchstabe b) der Richtlinie.

darüber hinausgehen.[26] Diese letztgenannten Regeln werden zusammengenommen als „Verhältnismäßigkeitsgrundsatz“ bezeichnet. Schließlich noch sind alle angemessenen Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden.[27]

4.1.1. Kommerzielle Zweckbestimmung

Die personenbezogenen Daten wurden von den Finanzinstituten nur zu Zwecken der Verarbeitung der Zahlungsaufträge des Kunden und anschließend von SWIFT zu Zwecken der Durchführung des SWIFTNet-FIN-Service erhoben (kommerzieller Zweck). Als einziger festgelegter, eindeutiger und rechtmäßiger Zweck kann daher nur dieser kommerzielle Zweck für die Verarbeitung personenbezogener Daten berücksichtigt werden.

Was die Übermittlung von personenbezogenen Daten an Drittländer anbelangt, siehe weiter unten unter Abschnitt 4.6

4.1.2. Weiterverarbeitung in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise

aa) Personenbezogene Daten dürfen nicht zu Zwecken verarbeitet werden, die mit der ursprünglichen Zweckbestimmung nicht zu vereinbaren sind. Durch die Entscheidung über die Spiegelung aller Datenverarbeitungstätigkeiten in einem Rechenzentrum in den USA brachte SWIFT sich selbst in eine vorhersehbare Situation, in der sie den nach US-Recht angeordneten Auflagen unterliegt.

Im vorliegenden Falle erhielt SWIFT Auflagen, die vom US-Finanzministerium (UST) wegen der behaupteten Terrorismusermittlungen angeordnet worden waren. Dieser weitere Zweck ist ein vollkommen anderer als die ursprüngliche Zweckbestimmung und die damit verbundene Behandlung der betreffenden personenbezogenen Daten und kann unmittelbare Folgen für die Einzelpersonen haben, deren personenbezogene Daten verarbeitet werden. Dieser weitere Zweck ist nicht mit dem ursprünglichen, rein kommerziellen Zweck zu vereinbaren, für den die personenbezogenen Daten erhoben wurden.

SWIFT war dieser weitere Zweck bekannt. Die Geschäftsleitung von SWIFT billigte ihn und kooperierte. SWIFT hat auf diesen Zweck nicht hingewiesen, und zwar weder bei den Nutzern ihrer Dienstleistungen noch bei einer der Datenschutzaufsichtsbehörden.

---

[26] Artikel 6 Absatz 1 Buchstabe c) der Richtlinie.

[27] Artikel 6 Absatz 1 Buchstabe d) der Richtlinie.

bb) Auch wurde festgestellt, dass massive Datenübermittlungen von SWIFT an das US-Finanzministerium stattgefunden haben, ohne dass es effektiv möglich war, den individualisierten Charakter der geforderten Daten zu überprüfen. SWIFT zufolge könnten potenziell alle Überweisungsdaten über das „Datenspeicher-System" („Black box") vom US-Finanzministerium (UST) nachgeforscht werden. Mit diesem System ist es dem US-Finanzministerium (UST) möglich, aus dem „Datenspeicher" alle Überweisungsdaten – und die darin enthaltenen personenbezogenen Daten – abzufragen, die es für erforderlich hält.

Die Artikel-29-Gruppe weist darauf hin, dass SWIFT sogar für die Zwecke der behaupteten Terrorismusermittlungen nur spezifische und individualisierte Daten übermitteln sollte, und nur von Einzelfall zu Einzelfall und in vollständiger Übereinstimmung mit den Datenschutzgrundsätzen. Da dies nicht der Fall ist, ist die derzeit gehandhabte Praxis nicht verhältnismäßig und verletzt somit Artikel 6 Absatz 1 Buchstaben c) der Datenschutzrichtlinie.

cc) Gemäß Artikel 13 ist vorgesehen, dass „die Mitgliedstaaten Rechtsvorschriften erlassen können, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1 [Grundsatz der Zweckbeschränkung], Artikel 10, Artikel 11 Absatz 1 [Pflicht zur Information der betroffenen Person], Artikel 12 [Auskunftsrecht] und Artikel 21 [Öffentlichkeit der Verarbeitungen] beschränken, sofern eine solche Beschränkung notwendig ist für [es folgt eine Auflistung wichtiger öffentlicher Interessen] … c) die öffentliche Sicherheit; d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten [...]; …f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;".

Der Europäische Gerichtshof (EuGH) hat diese Bestimmungen beleuchtet und Ausführungen zu ihrem Verständnis gemacht. In den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 („Rechnungshof") vom 20. Mai 2003 stelle der Gerichtshof klar, dass die Übermittlung von ursprünglich für „kommerzielle" Zwecke erhobenen Daten an Dritte, einschließlich öffentlicher Behörden, „einen Eingriff im Sinne von Artikel 8 EMRK darstellt". Ferner müssen Ausnahmen von dem in der Datenschutzrichtlinie festgelegten Grundsatz der Zweckbeschränkung Artikel 13 dieser Richtlinie beachten, und daher müssen sie „unter dem Gesichtspunkt des Artikels 8 der Menschenrechtskonvention gerechtfertigt sein" (Rechnungshof, C-465/00, §68 ff).

Nach der Menschenrechtskonvention ist der Eingriff in das Recht auf die Privatsphäre nur gerechtfertigt, insoweit er „gesetzlich vorgesehen ist" und „in einer demokratischen Gesellschaft" in einem bestimmten öffentlichen Interesse „notwendig ist". Die Rechtsprechung in Straßburg hat wiederholt daran erinnert, dass

das Gesetz, nach dem der Eingriff vorgesehen ist, „auf das zulässige Ziel der bestimmten Maßnahme abstellen und dabei mit ausreichender Klarheit die Grenzen des auf die zuständigen Behörden übertragenen Ermessens abstecken sowie bestimmen muss, wie dieses Ermessen auszuüben ist, um dem Einzelnen angemessenen Schutz gegen willkürliche Eingriffe zu bieten."

Diese Bestimmungen können jedoch nicht zur Anwendung kommen, da SWIFT in diesen Angelegenheiten gegen belgisches Recht verstoßen hat.[28]

dd) Die Artikel-29-Gruppe weist außerdem auf die geltenden rechtlichen Strukturen auf Regierungsebene hin. Sie betont, dass bei der Nutzung der entsprechenden Systeme der Grundsatz des Bankgeheimnisses einzuhalten ist. Sie bezieht sich diesbezüglich auf die 40+9 Empfehlungen der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung" (FATF/GAFI), eines 1989 eingerichteten zwischenstaatlichen Gremiums, das nationale und internationale Fachpolitiken zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung entwickeln und fördern soll. Die Artikel-29-Gruppe verweist auch auf das System für Finanzinformationsaustausch, das von 96 Staaten zwischen den entsprechenden nationalen Zentralstellen für Geldwäscheverdacht (Egmont Secure Web, ESW) eingerichtet und vom FinCEN in den Vereinigten Staaten koordiniert wird. In diesem Rahmen können dem anfragenden Partner finanzielle Informationen in Einklang mit den nationalen Regeln des Landes erteilt werden, das die Informationen weitergibt.

Die Artikel-29-Gruppe verweist auch auf die vorhandenen Mechanismen der Zusammenarbeit, die im Rahmen der 3. Säule (polizeiliche und justizielle Zusammenarbeit) errichtet oder weiterentwickelt wurden, und insbesondere auf die am 25. Juni 2003 zwischen den USA und der EU unterzeichneten internationalen Übereinkommen[29] über die gegenseitige Rechtshilfe und, wenn auch etwas weiter von diesem Thema entfernt, das internationale Auslieferungsübereinkommen. Zwar sind diese Verträge noch nicht ratifiziert, doch ist ein Staat gemäß Artikel 18 der Wiener Vertragsrechtskonvention[30] verpflichtet, sich aller Handlungen zu enthalten, die den Vertragsgegenstand oder den Vertragszweck gefährden, wenn er diesen Vertrag bereits unterzeichnet oder die Ratifizierungsinstrumente ausgetauscht und nicht mitgeteilt hat, dass er keine Vertragspartei werden möchte.

---

[28] Stellungnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.

[29] „Auslieferungsübereinkommen zwischen der EU und den USA" und „Übereinkommen über die gegenseitige Rechtshilfe zwischen der EU und den USA".
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf und
http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[30] Wiener Vertragsrechtskonvention vom 23. Mai 1969. Die Vereinigten Staaten haben diese Konvention unterzeichnet.

Durch die Entscheidung über die Spiegelung aller Datenverarbeitungstätigkeiten in einem Rechenzentrum in den USA brachte sich SWIFT im Ergebnis selbst in eine vorhersehbare Situation, in der sie den nach US-Recht angeordneten Auflagen unterliegt, und in der die Verarbeitung von personenbezogenen Daten derart organisiert wurde, dass eine Umgehung der bereits bestehenden Strukturen und internationalen Übereinkommen vorzuliegen scheint.

Insgesamt gesehen ist die Artikel-29-Gruppe der Auffassung, dass die Grundsätze der Zweckbeschränkung und der Vereinbarkeit, der Verhältnismäßigkeit und der Erforderlichkeit der Verarbeitung personenbezogener Daten nicht eingehalten sind.

4.2. Zulässigkeit der Verarbeitung von Daten (Artikel 7 der Richtlinie)

Um als rechtmäßig zu gelten, muss die Verarbeitung personenbezogener Daten zulässig sein und einem der in Artikel 7 der Richtlinie aufgeführten Gründe genügen.

4.2.1. Die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags (Artikel 7 Buchstabe b) der Richtlinie)

SWIFT verarbeitet die in den Überweisungsdaten enthaltenen personenbezogenen Daten im Rahmen des SWIFTNet-Fin-Services nur zur Durchführung der Zahlungsaufträge, mit der die Finanzinstitute SWIFT betraut haben.

Selbst wenn man in diesem Zusammenhang der Auffassung ist, dass die Verarbeitung zu diesem kommerziellen Zweck notwendig ist, um den Vertrag zwischen SWIFT und den betreffenden Finanzinstituten zu erfüllen, so ist jedoch die Art der Ausführung, nämlich die Spiegelung der personenbezogenen Daten im Rechenzentrum in den USA, bereits aus anderen Gründen, die weiter unten unter Ziffer 4.6. erörtert werden, nicht akzeptabel.

4.2.2. Die Verarbeitung ist erforderlich für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt (Artikel 7 Buchstabe c) der Richtlinie)

Die Verarbeitung und die Spiegelung könnten erforderlich gewesen sein, um eine rechtliche Verpflichtung zu erfüllen, der der für die Verarbeitung Verantwortliche unterliegt.

SWIFT hat mit seiner Zentrale in Belgien für diese spezielle Verarbeitung formell keine Rechtsgrundlage nach belgischem oder europäischem Recht herangezogen. Die Artikel-29-Gruppe hält ferner fest, dass nach belgischem oder europäischem

Recht keine rechtliche Verpflichtung zu dieser speziellen Datenverarbeitung besteht. Ferner hat die Artikel-29-Gruppe bereits in ihrer „SOX-Stellungnahme“[31] dargelegt, dass *„eine Verpflichtung aufgrund eines ausländischen Statuts oder einer ausländischen Verordnung (…) möglicherweise nicht als rechtliche Verpflichtung gilt, die die Datenverarbeitung in der EU legitimieren würde. Jede andere Interpretation würde es ausländischen Vorschriften leicht machen, die EU-Vorschriften gemäß der Richtlinie 95/46/EG zu umgehen“*. Die Artikel-29-Gruppe ist der Auffassung, dass diese Schlossfolgerung auch für den vorliegenden Fall gilt.

Artikel 7 Buchstabe c) der Datenschutzrichtlinie kann daher in diesem Falle nicht zur Rechtfertigung der Verarbeitung und der Spiegelung der Daten herangezogen werden.

4.2.3. Die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird (Artikel 7 Buchstabe f) der Richtlinie)

Gemäß Artikel 7 Buchstabe f) der Richtlinie könnte die Verarbeitung und die Spiegelung zur Verwirklichung des berechtigten Interesses erforderlich sein, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt ist, überwiegen.

Fraglich ist, ob Artikel 7 Buchstabe f) der Richtlinie herangezogen werden kann, um die Verarbeitung und die Spiegelung zu rechtfertigen, mit den Folge nämlich, dass die Maßnahmen der Verarbeitung im Rechenzentrum in den USA den Auflagen nach US-Recht unterliegen.

Es ist nicht in Abrede zu stellen, dass SWIFT ein berechtigtes Interesse an der Erfüllung der Auflagen nach US-Recht hat. Hätte SWIFT diesen Anordnungen nicht Folge geleistet, so hätte sie sich dem Risiko von Sanktionen nach US-Recht gegen sie ausgesetzt. Andererseits ist es auch wichtig, ein „ordentliches Gleichgewicht“ zu finden und zu halten, nämlich zwischen den Risiken für SWIFT, von den USA mit Sanktionen wegen etwaiger Nichterfüllung der Auflagen belegt zu werden, und dem Schutz der Rechte des Einzelnen.

Artikel 7 Buchstabe f) der Richtlinie verlangt, dass ein Gleichgewicht hergestellt wird zwischen dem berechtigten Interesse, das durch die Verarbeitung der perso-

[31] Stellungnahme 1/2006 zur Anwendung von EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption sowie Banken- und Finanzkriminalität.

nenbezogenen Daten verwirklicht wird, und den Grundrechten der betroffenen Person. Bei der Prüfung des Gleichgewichts der Interessen sind die Fragen der Verhältnismäßigkeit, der Subsidiarität, der Schwere der behaupteten Rechtsverletzungen, die mitgeteilt werden können, und die Folgen für die betroffenen Personen zu berücksichtigen. Im Zusammenhang mit der Prüfung des Gleichgewichts der Interessen sind auch angemessene rechtliche Garantien zu gewährleisten. So bestimmt insbesondere Artikel 14 der Richtlinie, dass die betroffen Person das Recht hat, jederzeit aus überwiegenden, schützwürdigen Gründen dagegen Widerspruch einlegen können, dass sie betreffende Daten verarbeitet werden, wenn die Verarbeitung der Daten auf Artikel 7 Buchstabe f) beruht.

SWIFT führte die Verarbeitung und die Spiegelung ihrer Daten „intransparent, systematisch, massiv und dauerhaft“[32] durch, ohne zum Zeitpunkt der Verarbeitung der Daten den weiteren und nicht zu vereinbarenden Zweck spezifiziert und ohne die Nutzer ihrer Dienste auf diesen Zweck hingewiesen zu haben. Diese weitere Verarbeitung und Spiegelung für einen nicht zu vereinbarenden Zweck könnte weit reichende Auswirkungen auf jeden Einzelnen haben.

Die Artikel-29-Gruppe ist daher der Auffassung, dass das Interesse oder die Grundrechte und Grundfreiheiten von vielen betroffenen Personen die Interessen von SWIFT, nicht mit US-Sanktionen wegen etwaiger Nichterfüllung der Auflagen belegt zu werden, überwiegen.

4.3. Versorgung des Betroffenen mit eindeutigen und vollständigen Informationen über das Vorhaben (Artikel 10 und 11 der Richtlinie)

Gemäß Artikel 10 und Artikel 11 der Richtlinie ist der für die Verarbeitung Verantwortliche verpflichtet, betroffene Personen über die Tatsache, die Zweckbestimmung und die Funktionsweise seiner Datenverarbeitung, über die Empfänger der personenbezogenen Daten und über das Bestehen von Auskunfts-, Berichtigungs- und Löschungsrechten für den Betroffenen zu informieren. Alle Kunden von Finanzinstituten haben ungeachtet ihrer Nationalität oder ihres Wohnsitzlandes das Recht, zu wissen, was mit ihren „vertraulichen“ Daten passiert.

Die Artikel-29-Gruppe stellt fest, dass diese Informationen in Bezug auf die Verarbeitung und die Spiegelung der Daten im Rechenzentrum in den USA weder durch SWIFT noch durch die betreffenden Finanzinstitute erteilt wurden.

Aufgrund von Artikel 13 der Richtlinie können die EU-Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte nach dieser Richtlinie in

[32] Stellungnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.

gewissem Umfang beschränken. Eine solche Beschränkung muss eine notwendige Maßnahme sein, um z. B. die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen von Einzelfall zu Einzelfall zu gewährleisten, und dies nur, wenn dieser Eingriff unter dem Gesichtspunkt des Artikels 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist. Eine derart lange und umfassende Maßnahme ohne jegliche Information der Betroffenen kann jedoch nicht in Einklang mit Artikel 13 stehen.

4.4. Erfüllung der Meldepflichten (Artikel 18 bis 20 der Richtlinie)

Die für die Verarbeitung Verantwortlichen müssen die Anforderungen der Artikel 18 bis 20 der Datenschutzrichtlinie bezüglich der Meldung ihrer Datenverarbeitungstätigkeiten an die nationalen Datenschutzbehörden bzw. der Vorabkontrolle durch diese erfüllen.

In den Mitgliedstaaten, in denen ein solches Verfahren vorgesehen ist, unterliegen die Verarbeitungen unter Umständen insofern einer Vorabkontrolle durch die nationale Datenschutzbehörde, als diese Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können. Die Bewertung, ob solche Verarbeitungen unter das Erfordernis der Vorabkontrolle falle, hängt von den nationalen Rechtsvorschriften und von der Praxis der nationalen Datenschutzbehörden ab.

Die Artikel-29-Gruppe hält fest, dass SWIFT der belgischen Datenschutzbehörde zwar einige Verarbeitungsarten gemeldet hat[33], nicht aber die Verarbeitung und die Spiegelung im Rechenzentrum in den USA, die der Durchführung von internationalen Zahlungsaufträgen diente, und auch nicht den weiteren Zweck mitgeteilt hat.

4.5. Aufsichtsmechanismen

Die Einrichtung von Datenschutzaufsichtsbehörden in den EU-Mitgliedstaaten, die ihre Aufgaben völlig unabhängig wahrnehmen, stellt eine wesentliche Komponente für den Schutz des Bürgers bei der Verarbeitung personenbezogener Daten dar. Dieser Grundsatz der völligen Unabhängigkeit der Kontrollstelle ist in Artikel 28 der Richtlinie festgelegt.

Aufgrund der mangelnden Informationen durch SWIFT, die Finanzinstitute und die Aufsichtsführenden in der nationalen Datenkontrollstelle konnten die

[33] Stellungsnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.

vorhandenen Datenschutz-Kontrollmechanismen der Richtlinie nicht effektiv angewandt werden. Die Artikel-29-Gruppe bedauert, dass keine formelle oder informelle Vorabkonsultation der SWIFT oder der Finanzinstitute mit den Datenschutzbehörden in Bezug auf die Verarbeitung und Spiegelung von personenbezogenen Daten im Rechenzentrum in den USA stattgefunden hat.

Die Überprüfungen durch die nationalen Behörden ergaben, dass die Kontrollmaßnahmen, die SWIFT zur Übermittlung der SWIFT-Daten an das US-Finanzministerium (UST) durchführte, hauptsächlich aus den Kontrollen einer privaten Wirtschaftsprüfungsgesellschaft bestanden sowie aus der Überprüfung durch SWIFT-Angestellte („Innenrevisoren"), die aber aus Sicherheitsgründen keine Einzelheiten über die internen Feststellungen berichten durften. SWIFT gab ferner an, von einem hochrangigen Ausschuss aus Vertretern der G-10-Zentralbanken beaufsichtigt zu werden und dieses Aufsichtsgremium in der Angelegenheit der US-Anweisungen informiert zu haben.

Zwar können die von SWIFT durchgeführten Kontrollmaßnahmen zur einer erhöhten Sicherheit der Datenverarbeitung beitragen, doch besteht die Artikel-29-Gruppe mit Nachdruck auf der Tatsache, dass keine anderweitigen Mechanismen, die von den für die Verarbeitung Verantwortlichen bereitgestellt werden, die Kontrolle der Datenverarbeitung durch eine öffentliche und unabhängige Kontrollstelle gemäß den Anforderungen nach Artikel 28 der Richtlinie ersetzen können. Jedenfalls erklärte sich die von den G-10-Zentralbanken eingesetzte Aufsichtsgruppe für unzuständig, Fragen im Zusammenhang mit dem Schutz von personenbezogenen Daten zu untersuchen.

Die Artikel-29-Gruppe missbilligt im Ergebnis die Tatsache, dass die vorhandenen Mechanismen für eine unabhängige Kontrolle durch die öffentlichen Kontrollstellen für die Verarbeitung von personenbezogenen Daten bei den durch den SWIFTNet-FIN-Service verarbeiteten personenbezogenen Daten umgangen worden sind.

4.6. Grenzüberschreitender Datenfluss (Artikel 25 und 26 der Richtlinie)

Artikel 25 und 26 der Richtlinie finden Anwendung, wenn personenbezogene Daten in ein Drittland übermittelt werden. Jegliche Übermittlung von Daten, die im Hoheitsgebiet der EU erhoben wurden und außerhalb des EU-Territoriums verwendet werden sollen, muss nach der Richtlinie einer Bewertung der Angemessenheit des Schutzniveaus unterzogen werden. Darüber hinaus können die Bestimmungen der Richtlinie, die sich auf die Übermittlung von personenbezogenen Daten an Drittländer beziehen, nicht getrennt von den übrigen Bestimmungen der Richtlinie angewandt werden. Wie in Artikel 25 Absatz 1 ausdrücklich bestimmt ist, gelten diese Bestimmungen „vorbehaltlich der Beachtung der

aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften". Dies bedeutet, dass ungeachtet der Bestimmungen, auf sich die Übermittlung von Daten an ein Drittland stützt, auch noch die anderen einschlägigen Bestimmungen der Richtlinie einzuhalten sind[34].

Die normale Funktionsweise des SWIFTNet-FIN-Services umfasst aufgrund der Standorte der SWIFT-Rechenzentren auch einen ständigen und massiven grenzüberschreitenden Datenfluss. Die Rechenzentren von SWIFT sind keine eigenständigen Rechtssubjekte, sondern Außenstellen (*„succursales"*) der genossenschaftlichen Gesellschaft nach belgischem Recht. Die Übertragungsschaltung und Zwischenspeicherkapazität der beiden Rechenzentren von SWIFT in Europa und in den USA funktioniert folgendermaßen: Die Überweisungsdaten werden in den Rechenzentren automatisch entschlüsselt, um die Informationen in nur wenigen tausendstel Sekunden zwischenzuspeichern. Dieser „Zwischenspeicherungsprozess" dient der Zulässigkeitsprüfung (Kontrolle auf Richtigkeit oder auf Eintragungen von Buchstaben/Zahlen in den obligatorischen Mitteilungsfeldern) der Informationen (z. B. der Sicherstellung, dass das richtige Währungskürzel für die Geldüberweisung eingetragen ist, z. B. „EUR") auf der Grundlage von standardisierten Inhalten. Während dieses Prozesses werden die Informationen aus Sicherheitsgründen (Sicherungskopie) auch für 124 Tage in beiden Rechenzentren abgespeichert und stellen dann perfekte „Spiegelbilder" dar. Damit wird sichergestellt, dass die Datenspeicherung parallel erfolgt und die Daten identisch sind. Damit SWIFT personenbezogene Daten rechtmäßig in den USA verarbeiten und spiegeln kann, müssen zunächst diese Daten aus der EU dorthin übermittelt werden, und zwar gemäß belgischem Recht, das in Umsetzung der Datenschutzrichtlinie erlassen wurde, und insbesondere in Übereinstimmung mit den Artikeln 25 und 26 über die Übermittlung personenbezogener Daten in Drittländer. Die Datenübermittlungen von SWIFT in die Vereinigten Staaten sind daher unter Berücksichtigung von zweierlei Gesichtspunkten zu betrachten: Erstens unter dem Gesichtspunkt der wirtschaftlichen Verarbeitung und Spiegelung der personenbezogenen Daten durch SWIFT Belgien im Wege der Übermittlung an ihr Rechenzentrum in den USA und zweitens unter dem Gesichtspunkt der Verarbeitung dieser Daten für einen weiteren Zweck im Wege der mit SWIFT vereinbarten Nutzung durch das US-Finanzministerium (UST).

4.6.1. Angemessener Datenschutz (Artikel 25 Absatz 1 der Richtlinie)

Gemäß Artikel 25 Absatz 2 der Richtlinie wird die Angemessenheit des Schutzniveaus, das ein Drittland bietet, „unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbe-

[34] Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114.

stimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt."

Unter Berücksichtigung der vorstehenden Kriterien und in Anwendung der in der Arbeitsunterlage WP12[35] festgelegten Grundsätze ist die Artikel-29-Gruppe der Auffassung, dass in den USA derzeit nur die „Safe Harbour"-Nichtbeanstandungsregelung ein angemessenes Schutzniveau für Datenübermittlungen aus der EU an die US-Organisationen bietet, die dieser Regelung beigetreten sind. Finanzielle Dienstleistungen werden von ihr jedoch nicht erfasst[36].

Daher konnte sich SWIFT als belgisches Rechtssubjekt für die Verarbeitung und Spiegelung in seinem Rechenzentrum in den USA nicht auf Artikel 25 der Richtlinie stützen.

4.6.2. Der Empfänger der Daten garantiert angemessene Datenschutzmaßnahmen (Artikel 26 Absatz 2 der Richtlinie)

Gemäß Artikel 26 Absatz 2 der Richtlinie kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch dann genehmigen, wenn der für die Verarbeitung der Daten Verantwortliche *„ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet"*. Nach dem letzten Halbsatz von Artikel 26 Absatz 2 *„können sich diese Garantien insbesondere aus entsprechenden Vertragsklauseln ergeben"*. Zur Erleichterung der Verwendung von Vertragsklauseln hat die Europäische Kommission drei Entscheidungen hinsichtlich Standardvertragsklauseln veröffentlicht, wovon zwei die Übermittlung von einem für die Verarbeitung von Daten Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen regeln, während die dritte die Übermittlung von einem für die Verarbeitung von Daten Verantwortlichen an einen Auftragsverarbeiter betrifft[37]. Abgesehen von der Möglichkeit, Vertragsklauseln zu benutzen, um so ausreichende Garantien zu

---

35 „Übermittlung personenbezogener Daten an Drittländer : Anwendung von Artikeln 25 und 26 der EU-Datenschutzrichtlinie", von der Art. 29-Gruppe angenommen am 24. Juli 1998; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

36 vgl. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

37 In Bezug auf die Übermittlung von einem für die Verarbeitung Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen veröffentlichte die Kommission den ersten Satz Standardvertragsklauseln am 15. Juni 2001; in der Folge ergänzte sie diese Entscheidung, um einen neuen Satz alternativer Klauseln anzufügen (mit Entscheidung vom 27. Dezember 2004). In Bezug auf die Übermittlung von einem für die Verarbeitung Verantwortlichen an einen Auftragsverarbeiter veröffentlichte die Kommission einen Satz Standardvertragsklauseln am 27. Dezember 2001. Alle diese Klausen sind auf folgender Website abzurufen: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

bieten, hat die Artikel-29-Gruppe seit 2003 zusätzlich an der Möglichkeit gearbeitet, dass multinationale Unternehmensgruppen „verbindliche unternehmensinterne Vorschriften“ für dieselben Zwecke verwenden können[38].

Im vorliegenden Fall hat SWIFT jedoch für die Verarbeitung und Spiegelung in seinem Rechenzentrum in den USA keinen Gebrauch von diesen Möglichkeiten gemacht.[39]

4.6.3. Ausnahmen (Artikel 26 der Richtlinie)

Nach Artikel 26 Absatz 1 der Richtlinie können Übermittlungen von personenbezogenen Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, vorgenommen werden, wenn eine der folgenden unter Buchstaben a) bis f) aufgeführten Voraussetzungen erfüllt ist. Wie die Artikel-29-Gruppe bereits in ihrem oben erwähnten Arbeitsdokument WP12[40] ausgeführt hat, ist Artikel 26 Absatz 1 zwangsläufig eng auszulegen.

In dieser Hinsicht möchte die Artikel-29-Gruppe betonen, dass diese Logik dieselbe ist wie die des Zusatzprotokolls zur Konvention 108 des Europarates. Im Bericht über dieses Protokoll wird festgestellt, dass „es im Ermessen der Vertragsparteien steht, Ausnahmen vom Grundsatz des angemessenen Schutzniveaus festzulegen. Die entsprechenden innerstaatlichen Rechtsvorschriften müssen jedoch den dem europäischen Recht innewohnenden Grundsatz beachten, dass Ausnahmeklauseln eng auszulegen sind, damit die Ausnahme nicht zur Regel wird“.[41]

Im vorliegenden Falle sind die folgenden Ausnahmen möglich:

4.6.3.1. Die betroffene Person hat ihre Einwilligung gegeben (Artikel 26 Absatz 1 Buchstabe a) der Richtlinie)

Damit man sich rechtswirksam auf diese Ausnahme berufen kann, muss die betroffene Person ohne jeden Zweifel ihre Einwilligung zu der betreffenden

---

38 Vgl. Arbeitsdokument WP 74, „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“, von der Artikel-29-Gruppe angenommen am 3. Juni 2003 mit weiteren ergänzenden Dokumenten WP107 und WP108.

39 Sollte SWIFT jedoch Gebrauch von diesen Möglichkeiten machen, so möchte die Artikel-29-Gruppe in Erinnerung rufen, dass die Ausnahmen vom geltenden Datenschutzrecht für alle künftigen Datenübermittlungen in jedem Falle nicht über die in einer demokratischen Gesellschaft notwendigen Beschränkungen hinausgehen dürfen.

40 Vgl. oben, Fußnote 35.

41 Vgl. Bericht über das Zusatzprotokoll zur Konvention 108 über Kontrollbehörden und grenzüberschreitende Datenströme, Artikel 2 Absatz 2 Buchstabe a); dieses Dokument ist abzurufen unter http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

Übermittlung gegeben haben. Wie bereits im Arbeitsdokument WP 12 der Artikel-29-Gruppe ausgeführt, muss diese Einwilligung, wie auch immer die Umstände sind, unter denen sie gegeben wird, gemäß der Legaldefinition des Artikels 2 Buchstabe h) der Richtlinie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben sein und den Willen des Betroffenen zu Ausdruck bringen.[42] Die betroffene Person muss darüber informiert sein, dass es sich bei der betreffenden Übermittlung um ein Drittland ohne angemessenes Schutzniveau oder um ein Drittland handelt, in dem keine ausreichenden Garantien geboten werden, und kann aufgrund dessen entscheiden, ob er das damit verbundene Risiko eingehen will oder nicht.

SWIFT hat keine ‚Einwilligung ohne jeden Zweifel' von den Personen erhalten, die von der Verarbeitung und Spiegelung im Rechenzentrum in den USA betroffen sind, und kann sich daher nicht auf Artikel 26 Absatz 1 Buchstabe a) der Richtlinie berufen.

4.6.3.2. Die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe b) der Richtlinie)

Diese Ausnahme bedeutet, dass die übermittelten Daten auch tatsächlich zu Zwecken der Erfüllung dieses Vertrags oder dieser vorvertraglichen Maßnahmen erforderlich sein müssen. Daher vertritt die Artikel-29-Gruppe die Rechtsauffassung, dass diese Bedingung nicht auf die Datenübermittlungen von SWIFT an ihr Rechenzentrum in den USA anwendbar ist, da SWIFT keine direkten Vertragsbeziehungen mit den betroffenen Personen unterhält. Ebenso wenig ist diese Ausnahme auf die Übermittlung von zusätzlichen Informationen, die nicht zu Übertragungszwecken benötigt werden, oder auf eine Übermittlung, die einem anderen Zweck als der Erfüllung des Vertrags dient, anwendbar. Ganz allgemein gesagt gestatten es die Ausnahmen nach Artikel 26 Absatz 1 Buchstaben b) bis e) nur, dass die Daten, die zu Übermittlungszwecken erforderlich sind, auf der Grundlage der individuellen Ausnahme übermittelt werden dürfen; für Zusatzdaten ist auf andere Mittel zurückzugreifen, um den Beweis der Angemessenheit zu erbringen.

4.6.3.3. Die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder werden soll (Artikel 26 Absatz 1 Buchstabe c) der Richtlinie)

[42] Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114.

Wie dies schon bei der Ausnahme nach Artikel 26 Absatz 1 Buchstabe b) der Fall war, kann bei einer Übermittlung von Daten in ein Drittland, das keinen angemessenen Schutz gewährleistet, auch nicht davon ausgegangen werden, dass sie unter den Ausnahmetatbestand von Artikel 26 Absatz 1 Buchstabe c) fällt, es sein denn sie gilt als tatsächlich „zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll", und sie besteht die entsprechende „Erforderlichkeitsprüfung". Dabei ist nachzuweisen, dass ein enger und substanzieller Zusammenhang zwischen dem Interesse der betroffenen Person und dem Vertragszweck besteht.[43]

Die Artikel-29-Gruppe ist der Auffassung, dass auch diese Voraussetzung nicht auf die Datenübermittlungen von SWIFT an sein Rechenzentrum in den USA anwendbar ist.

4.6.3.4. Die Übermittlung ist entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben (Artikel 26 Absatz 1 Buchstabe d) der Richtlinie)

SWIFT legte dar, die Spiegelung der Datenverarbeitung an ihre Rechenzentren gelte als wichtiger Baustein im globalen Finanzsystem, diese Spiegelung der Datenverarbeitung sei von den Aufsichtsführenden (G-10 Zentralbanken) aus Sicherheits- und Verlässlichkeitsgründen vorgeschlagen worden und die Infrastruktur von SWIFT werde als für das globale Finanzgewerbe wesentlich angesehen. SWIFT behauptet, dieser Grund rechtfertige die Übermittlung auf der Rechtsgrundlage von Artikel 26 Absatz 1 Buchstabe d) der Richtlinie.

Die Artikel-29-Gruppe kann dieser Auslegung nicht folgen. Selbst wenn erwiesen wäre, dass die internationale Spiegelung der Verarbeitung (auf einem anderen als dem europäischen Kontinent) im Sinne von Artikel 26 Absatz 1 Buchstabe d) der Richtlinie „für die Wahrung eines wichtigen öffentlichen Interesses erforderlich oder gesetzlich vorgeschrieben ist", so ist es immer möglich, die Spiegelung einer solchen Verarbeitung in einem Land außerhalb der EU oder des EWR, das ein angemessenes Schutzniveau bereitstellt, vorzunehmen. Die Artikel-29-Gruppe bezieht sich dabei auf Länder wie z. B. Argentinien[44] oder Kanada[45], die nach den Entscheidungen der Europäischen Kommission den Anforderungen der Richtlinie genügen. Die „Spiegelung" in einem Nicht-EU-Land ohne ein ange-

[43] Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114

[44] Entscheidung der Kommission C(2003) 1731 vom 30. Juni 2003; ABl. L 168 vom 5.7.2003.

[45] Entscheidung der Kommission 2002/2/EG vom 20.12.2001 über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet; ABl. L 2/13 vom 4.1.2002.

messenes Datenschutzniveau war und ist nicht erforderlich und auch nicht im Rahmen von Artikel 26 Absatz 1 Buchstabe d) zu rechtfertigen.

Darüber hinaus wurden personenbezogene Daten, die im Rahmen des SWIFT-Netzes für internationale Geldüberweisungen unter Nutzung des BIC- oder des SWIFT-Codes erhoben und verarbeitet und in den USA gespiegelt worden waren, seit Ende 2001 aufgrund von Anordnungen nach US-Recht dem US-Finanzministerium (UST) bereitgestellt.

Die vollkommene Rückverfolgbarkeit von Geldüberweisungen kann ein besonders wichtiges und wertvolles Instrument bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Geldwäsche und Terrorismusfinanzierung sein und war Gegenstand einer Regelung nach EU-Recht[46].

Die Artikel-29-Gruppe erkennt an, dass demokratische Gesellschaften die Terrorismusbekämpfung im Interesse der staatlichen Sicherheit als legitimes Ziel verfolgen, und dass zu diesem berechtigten Zweck Maßnahmen ergriffen werden können, die mit dem fundamentalen Recht auf Schutz der personenbezogenen Daten im Widerstreit stehen. Sie erinnert daran, dass sie sich diesen Aufgaben uneingeschränkt verpflichtet fühlt, aber auch der Ansicht ist, dass die internationalen Instrumente sehr wohl ein angemessenes rechtliches Rahmenwerk liefern, auf der Grundlage dessen eine internationale Zusammenarbeit möglich ist. Zu diesem Zweck sollten nach Auffassung der Artikel-29-Gruppe die bereits vorhandenen Möglichkeiten, die durch die aktuellen Formen der internationalen Zusammenarbeit geboten werden, und die im Hinblick auf die Terrorismusbekämpfung und die Terrorismuserforschung entstanden sind, noch mehr ausgeschöpft und zugleich das erforderliche Maß an Grundrechtsschutz sichergestellt werden.

Die Artikel-29-Gruppe stellt aber nichtsdestoweniger fest, dass Artikel 26 Absatz 1 Buchstabe d) der Richtlinie auch nicht greift, da die Übermittlung nicht für die Wahrung eines wichtigen öffentlichen Interesses eines EU-Mitgliedstaates (Belgien) erforderlich oder gesetzlich vorgeschrieben ist. Bei diesem Punkt der Richtlinie hatten die Verfasser ganz klare Vorstellungen, dass in diesem Zusammenhang nur wichtige öffentliche Interessen darunter fallen, die von der nationalen Gesetzgebung, die auf die in der EU niedergelassenen für die Verarbeitung von Daten Verantwortlichen Anwendung findet, auch als solche bezeichnet sind. Jede andere Auslegung würde es einer ausländischen Behörde leicht machen, das in der Richtlinie festgelegte Erfordernis eines angemessenen Schutzes im Empfängerland zu umgehen.

---

[46] Z. B. Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, verabschiedet am 8. November 2006, noch nicht veröffentlicht; ursprünglich Vorschlag der Kommission, KOM (2005) 343.

4.6.3.5. Die Übermittlung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe e) der Richtlinie)

Diese Ausnahme trifft auf Übermittlungen zu, die mit dem individuellen Interesse der betroffenen Person zusammenhängen müssen, und, wenn es sich um Gesundheitsdaten handelt, so muss die Übermittlung für eine wichtige Diagnose erforderlich sein. Demzufolge könnte dieser Ausnahmetatbestand nicht herangezogen werden, um die Übermittlung von personenbezogenen medizinischen Daten zu Zwecken wie etwa allgemeinen medizinischen Forschungsarbeiten zu rechtfertigen.[47]

SWIFT hat nicht behauptet, dass die Übermittlung zur Wahrung lebenswichtiger Interessen der von der Verarbeitung und Spiegelung im Rechenzentrum in den USA betroffenen Personen erforderlich ist. Die Artikel-29-Gruppe ist auch der Auffassung, dass diese Ausnahme hier in jedem Fall irrelevant ist. Artikel 26 Absatz 1 Buchstabe e) der Richtlinie kann also auch nicht herangezogen werden.

4.6.4. Feststellungen

SWIFT hätte aufgrund von Artikel 26 Absatz 2 der Richtlinie eine rechtmäßige Übermittlung von personenbezogenen Daten an ihr Rechenzentrum in den USA vornehmen können. Jedoch hat sich SWIFT dazu entschieden, die personenbezogenen Daten zu übermitteln, ohne die rechtlichen Anforderungen nach belgischem Recht zu erfüllen, denen derartige internationale Datentransfers unterliegen.

SWIFT kann keine der anderen Ausnahmen von Artikel 26 der Richtlinie für sich geltend machen.

Was die Verarbeitung und die Spiegelung in den USA anbelangt, so ist selbst die kommerzielle Verarbeitung und Spiegelung nicht rechtmäßig erfolgt. Die kontinuierliche Verarbeitung und Spiegelung bleibt angesichts ihres überdies nicht zu vereinbarenden Zwecks und ihres großen Ausmaßes nicht in den Grenzen dessen, was in einer demokratischen Gesellschaft erforderlich ist, und hindert SWIFT des Weiteren an der Übermittlung von personenbezogenen Daten in die USA.

[47] Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114;
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

5. SCHLUSSFOLGERUNGEN

Aufgrund dessen ist die Artikel-29-Gruppe folgender Auffassung:

5.1. Die EU-Datenschutzrichtlinie 95/46/EG ist auf den Austausch von personenbezogenen Daten durch den SWIFTNet-FIN-Service anwendbar.

5.2. SWIFT und die Finanzinstitute tragen nach den Vorgaben der Richtlinie gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten durch den SWIFTNet FIN Service. Auch wenn SWIFT dabei die Hauptverantwortung trägt, sind die Finanzinstitute in gewissem Umfang für diese Verarbeitung der personenbezogenen Daten ihrer Kunden mitverantwortlich.

5.3. SWIFT und die Finanzinstitute in der EU haben die Vorgaben der Richtlinie nicht beachtet:

5.3.1. *SWIFT*: Hinsichtlich der Verarbeitung und der Spiegelung personenbezogener Daten im Rahmen des SWIFTNet-FIN-Services muss SWIFT seinen Verpflichtungen nach der Richtlinie als der für die Verarbeitung verantwortlichen Stelle nachkommen; dies betrifft insbesondere die Informationspflichten, die Meldepflicht und die Verpflichtung zur Wahrung eines angemessenen Schutzniveaus bei internationalen Datentransfers;

5.3.2. *Finanzinstitute*: Die Finanzinstitute in der EU müssen als die für die Verarbeitung von personenbezogenen Daten verantwortlichen Stellen ihrer rechtlichen Verpflichtung nachkommen und sicherstellen, dass SWIFT vollständig die rechtlichen Anforderungen, insbesondere auch des Datenschutzrechts, erfüllt, um den Schutz ihrer Kunden zu gewährleisten. Die Finanzinstitute müssen sich auch über die unterschiedlichen Zahlungssysteme, deren technische und rechtliche Ausgestaltung und die damit verbundenen Risiken informieren. Soweit Finanzinstitute sich nicht (hinreichend) bemüht haben, sich diese Kenntnisse zu beschaffen, haben sie wesentliche rechtliche Risiken hinsichtlich ihrer grundlegenden Sorgfaltspflichten gegenüber ihrer Kunden in Kauf genommen. Die Artikel-29-Gruppe hält es für unabdingbar, dass die Finanzinstitute als professionelle Dienstleister ihre Kunden in Übereinstimmung mit den Transparenzforderungen der Richtlinie hinreichend unterrichten, insbesondere über die Inanspruchnahme von Dienstleistern wie z. B. den SWIFTNet-FIN-Service, die umfangreiche Übermittlungen in Länder ohne adäquates Datenschutzniveau nach der Richtlinie durchführen, oder wenn solche Übermittlungen besondere Bedenken oder Risiken aus Datenschutzsicht hervorrufen.

5.4. Die Artikel-29-Gruppe vertritt zudem die Auffassung, dass der Mangel an Transparenz sowie an angemessenen und effektiven Kontrollmechanismen beim gesamten Prozess der Übermittlung von personenbezogenen Daten in die USA und weiter an das US-Finanzministerium eine schwere Verletzung der Richtlinie darstellt. Darüber hinaus sind auch die Garantien für die Datenübermittlung in ein Drittland, wie sie die Richtlinie vorsieht, und die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit nicht beachtet worden.

Bezüglich der Übermittlung von personenbezogenen Daten an UST ist die Artikel-29-Gruppe der Ansicht, dass der intransparente, systematische, massive und dauerhafte Transfer von personenbezogenen Daten von SWIFT an UST in einer heimlichen, intransparenten und systematischen Art über Jahre hinweg ohne geltende Rechtsgrundlage und ohne die Möglichkeit einer unabhängigen Überprüfung durch öffentliche Aufsichtsbehörden eine Verletzung europäischer Datenschutzgrundsätze darstellt und nicht in Übereinstimmung mit belgischem und europäischem Recht steht. Für den Kampf gegen den Terrorismus gibt es bereits einen internationalen Rechtsrahmen. Die dort bestehenden Möglichkeiten sollten konsequent unter Sicherstellung des erforderlichen Schutzes der Grundrechte genutzt werden.

5.5. Die Artikel-29-Gruppe erinnert noch einmal[48] an die Verpflichtung der demokratischen Gesellschaften, die Grundrechte und Grundfreiheiten des Einzelnen zu achten. Der Schutz der personenbezogenen Daten des Einzelnen ist Teil dieser Grundrechte und Grundfreiheiten[49]. Die Datenschutzrichtlinien 95/46/EG und 2002/58/EG der Gemeinschaft bilden einen Teil dieser Verpflichtung[50]. Beide Richtlinien zielen auf die Achtung der Grundrechte und Grundfreiheiten und insbesondere auf das Recht auf Privatsphäre einschließlich des Schutzes von personenbezogenen Daten ab. Sie zielen auch auf die Achtung der Rechte, die durch Art. 8 der Europäischen Menschenrechtskonvention (EMRK) und durch Art. 8 der Europäischen Charta der Grundrechte geschützt werden. In all diesen Rechtsinstrumenten sind Ausnahmen für die Verbrechensbekämpfung unter klar definierten Bedingungen vorgesehen.

---

48 Artikel-29-Datenschutzgruppe: Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm.

49 Siehe insbesondere Art. 8 der Charta der Grundrechte der Europäischen Union wie auch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in den Rechtssachen „Aman“ vom 16. Februar 2000 und „Rotaru“ vom 4. Mai 2000.

50 Siehe die Erwägungsgründe 1, 2, 10 und 11 der Richtlinie 95/46/EG.

6. SOFORTIGER HANDLUNGSBEDARF ZUR VERBESSERUNG DER GEGENWÄRTIGEN SITUATION

Daher fordert die Artikel-29-Gruppe folgende sofortige Maßnahmen zur Verbesserung der derzeitigen Situation:

6.1. **Beendigung der Rechtsverletzungen:** SWIFT und die Finanzinstitute müssen ihren rechtlichen Verpflichtungen nach nationalem und europäischem Recht nachkommen. Dies beinhaltet Maßnahmen, die sicherstellen, dass alle Datenübermittlungen in Übereinstimmung mit geltendem Recht erfolgen. Im Falle der Nichtbeachtung müssen die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen mit Sanktionen zur Rechtsdurchsetzung durch die zuständigen Aufsichtsbehörden nach den Vorgaben der Richtlinie und jeweiligem nationalem Recht rechnen.

6.2. **Rückkehr zur rechtmäßigen Datenverarbeitung:** Die Artikel-29-Gruppe fordert SWIFT und die Finanzinstitute dazu auf, unverzüglich Maßnahmen zu ergreifen, die die gegenwärtige unrechtmäßige Situation beenden und nur noch internationale Datenüberweisungen durchzuführen, die in vollständiger Übereinstimmung mit dem Datenschutzrecht stehen. Die Artikel-29-Gruppe begrüßt, dass einige Aufsichtsbehörden die Finanzinstitute bereits dazu drängen, unverzüglich eine Lösung zu suchen.

6.3. **Handlungsbedarf gegenüber SWIFT:** SWIFT als für die Datenverarbeitung verantwortliche Stelle muss hinsichtlich aller seiner Daten verarbeitenden Tätigkeiten die erforderlichen Maßnahmen ergreifen, zu denen sie das belgische Datenschutzgesetz in Umsetzung der Richtlinie verpflichtet.

6.4. **Handlungsbedarf gegenüber den Zentralbanken:** Die jetzige Situation bedarf einer Klärung der Aufsichtsstrukturen bei SWIFT. Die Artikel-29-Gruppe empfiehlt deshalb angemessene Lösungen. Dazu gehört insbesondere, dass die Umsetzung von datenschutzrechtlichen Regelungen klar unter diese Aufsichtspflicht fällt, unbeschadet der Befugnisse der nationalen Datenschutzaufsichtsbehörden. Auch gehört dazu sicherzustellen, dass die zuständigen Behörden, wenn notwendig, vorschriftsmäßig und rechtzeitig unterrichtet werden. Die Artikel-29-Gruppe vertritt die Ansicht, dass die Nichtbefolgung von Datenschutzgesetzen das Vertrauen der Kunden in ihre Banken erschüttern kann und dies auch die finanzielle Stabilität von Zahlungssystemen zu beeinträchtigen vermag (Vertrauensrisiko). Rechtliche Hindernisse, wie die Verpflichtung zur Einhaltung des Berufsgeheimnisses durch die Aufsichtsgremien, die als Argumente dazu benutzt werden könnten, die effektive Kontrolle der unabhängigen Aufsichtsbehörden einzuschränken, können im Falle einer möglichen Verletzung von verfassungsmäßigen Rechten oder Menschenrechten nicht angeführt werden.

6.5. **Handlungsbedarf gegenüber den Finanzinstituten:** Alle Finanzinstitute in der EU, einschließlich der Zentralbanken, die die Dienstleistungen des SWIFTNet Fin Service benutzen, haben gemäß Artikeln 10 und 11 der Richtlinie 95/46/EG sicherzustellen, dass sie ihre Kunden angemessen darüber unterrichten, wie deren Daten verarbeitet werden und welche Rechte die Betroffenen haben. Sie haben sie auch darüber zu informieren, dass die US-Behörden Zugriff auf die Daten haben können. Die Datenschutzaufsichtsbehörden werden diese Informationspflicht durchsetzen, um sicherzustellen, dass sie europaweit von allen Finanzinstituten eingehalten werden. Sie werden auch bei der Abfassung einheitlicher Informationstexte zusammenarbeiten. Die Artikel-29-Gruppe erinnert in diesem Zusammenhang an ihre Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten[51]. Es scheint auch angemessen, dass die Finanzinstitute und Zentralbanken technische Alternativen zu den derzeitigen Verfahren in Erwägung ziehen, um einen Zahlungstransfer zu gewährleisten, der im Einklang mit den Grundsätzen der Richtlinie steht.

Die Artikel-29-Gruppe hebt Folgendes hervor:

6.6. **Wahrung unserer Grundwerte im Kampf gegen das Verbrechen:** Die Artikel-29-Gruppe erinnert daran, dass jede im Kampf gegen Verbrechen und Terrorismus getroffene Maßnahme nicht die Standards hinsichtlich des Schutzes von Grundrechten beeinträchtigen soll und darf, die unsere demokratischen Gesellschaften auszeichnen. Im Kampf gegen den Terrorismus ist es unabdingbar, dass die Grundwerte geschützt werden, die die Basis unserer demokratischen Gesellschaft bilden und bei denen es sich genau um die Werte handelt, die Terroristen zu zerstören suchen.

6.7. **Globale Datenschutzgrundsätze:** Die Artikel-29-Gruppe erachtet es als wesentlich, dass die Grundsätze zum Schutz personenbezogener Daten einschließlich der Kontrolle durch unabhängige Aufsichtsbehörden auch im Rahmen eines weltweiten Austauschs von Informationen vollständige Beachtung finden.

Die Artikel-29-Gruppe wird alle vorstehenden Punkte überwachen und einer Erfolgskontrolle unterziehen.

Brüssel, den 22. November 2006
Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar

51 Artikel-29-Datenschutzgruppe: „Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten" vom 25. November 2004, WP 100;
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

V. Internationale Konferenz der Datenschutzbeauftragten

Entschließungen der 28. Konferenz vom 2./3. November 2006 in London

ABSCHLUSSKOMMUNIQUE

Am 2. und 3. November fand in London die 28. Internationale Konferenz der Datenschutzbeauftragten statt. Bei der Konferenz waren Abgeordnete von 58 Datenschutzbehörden aus der ganzen Welt anwesend.

Der Hauptteil der Konferenz, bei der auch Vertreter verschiedener Organisationen aus dem staatlichen, dem Vollzugs- sowie aus dem zivilgesellschaftlichen und privatwirtschaftlichen Sektor vertreten waren, befasste sich mit den Auswirkungen einer Überwachungsgesellschaft.

Die Beauftragten hoben eine Reihe von Themen besonders hervor.

- **Die „Überwachungsgesellschaft" ist bereits Realität.** Überwachung bedeutet Einsatz technischer Mittel zur gezielten, routinemäßigen und systematischen Erfassung der Bewegungen und Aktivitäten des Einzelnen im öffentlichen und privaten Bereich. Im täglichen Leben begegnet man modernen und aufstrebenden Technologien zur Erfassung, Sortierung und Auswahl von Personendaten z. B. in folgender Form:

  – Systematisches Verfolgen, Überwachen und Aufzeichnen von Identitäten, Bewegungen und Aktivitäten

  – Analyse von Einkaufsgewohnheiten, Finanztransaktionen und anderen Interaktionen

  – Ständig wachsender Einsatz neuer Technologien, z. B. automatische Videokameras, RFID usw.

  – Überwachen von Telefon-, E-Mail- und Internetverwendung

  – Überwachen der Aktivitäten am Arbeitsplatz

- **Überwachungsaktivitäten können gut gemeint und nützlich sein.** In demokratischen Gesellschaften haben sich diese Aktivitäten bislang relativ gutartig und in kleinen Schritten entwickelt – und nicht unbedingt deshalb, weil Regierungen oder Unternehmen auf ungerechtfertigte Weise in das Leben einzelner

Bürger einzudringen beabsichtigen. Einige dieser Aktivitäten sind im Prinzip notwendig und wünschenswert – zum Beispiel zur Bekämpfung von Terrorismus und Schwerkriminalität, zur Verbesserung der Anspruchsberechtigung und des Zugriffs auf öffentliche Dienste sowie zur Verbesserung des Gesundheitswesens.

- **Unkontrollierte oder übermäßige Überwachungsaktivitäten können jedoch unbemerkt zu Risiken führen, die wesentlich mehr als nur eine Beeinträchtigung der Privatsphäre nach sich ziehen.** Sie können ein Klima voller Misstrauen hervorrufen und Vertrauen untergraben. Die Erfassung und Verwendung umfangreicher Personendaten durch öffentliche und private Organisationen führt zu Entscheidungen, die einen direkten Einfluss auf das Leben der Menschen haben. Durch eine automatische oder willkürliche Klassifizierung und Profilerstellung können Menschen auf eine Art und Weise stigmatisiert werden, die Gefahren für den Einzelnen mit sich bringen und deren Zugriffsmöglichkeiten auf Dienstleistungen beeinträchtigen. Insbesondere wird das Risiko einer sozialen Ausgrenzung immer größer.

- **Die Kontrolle des Schutzes der Privatsphäre und des Datenschutzes ist eine wichtige Maßnahme, aber nicht die einzige Antwort.** Die Überwachung des Einzelnen bedeutet nicht nur eine Einschränkung der Privatsphäre. Sie kann außerdem einen Einfluss auf Aussichten, Lebenschancen und Lebensstil eines Menschen haben. Übermäßige Überwachung hat ferner einen Einfluss auf das Wesen der Gesellschaft selbst. Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre tragen dazu bei, die Überwachung, z. B. durch bestimmte Schutzmaßnahmen, in legitimen Grenzen zu halten. Diese Kontrolle muss jedoch differenzierter angegangen werden.

- **Die Auswirkungen sollten systematisch bewertet werden.** Derartige Bewertungen würden nicht nur eine Beurteilung der Beeinträchtigung unserer Privatsphäre beinhalten, sondern darüber hinaus auch die gesellschaftlichen Auswirkungen sowie die Möglichkeiten zur Minimierung unerwünschter Folgen für den Einzelnen und die Gesellschaft identifizieren.

- **Die Probleme sind vielfältig und können nicht allein von den Datenschutzbehörden beantwortet werden.** Es sollten sich alle engagieren, denen bestimmte Entwicklungen Bedenken bereiten. Die Datenschutzbeauftragten sollten mit maßgeblichen zivilgesellschaftlichen Organisationen, aber auch mit Regierungen, dem Privatsektor, gewählten Vertretern und Individuen zusammenarbeiten, um unerwünschten Folgen vorzubeugen.

- **Öffentliches Vertrauen ist von größter Bedeutung.** Obgleich ein großer Teil der von der Überwachungsgesellschaft verwendeten Infrastruktur für gutartige

Zwecke errichtet wurde, gibt es keine Garantie für das langfristige Vertrauen der Öffentlichkeit. Der Einzelne muss zuversichtlich sein können, dass jeder Eingriff in sein Leben einen notwendigen und angemessenen Zweck verfolgt. Öffentliches Vertrauen ist wie die Privatsphäre einer Person – ist es erst einmal verloren, lässt es sich nur schwer, wenn nicht unmöglich, wiedergewinnen.

Obwohl die Themen im Zusammenhang mit einer Überwachungsgesellschaft über den Datenschutz und den Schutz der Privatsphäre hinausgehen, spielen die Datenschutzbehörden eine unentbehrliche Rolle. In einer Überwachungsgesellschaft hat der Einzelne immer häufiger keine echten Wahlmöglichkeiten, immer weniger Kontrolle und immer weniger Möglichkeiten zur Selbsthilfe. Personendaten werden auf eine für den Normalbürger unsichtbare Art und Weise erhoben und verwendet.

Die Welt hat sich seit Beginn der Datenschutzkontrolle immer weiter entwickelt. Die Forderungen der Staaten, des Privatsektors und der Bürger haben sich geändert, die Datenverarbeitungstechnologie hat sich mit hohem Tempo weiterentwickelt. Die Datenschutzbehörden müssen sich überlegen, ob ihre bisherige Arbeitsweise noch immer relevant und effektiv ist. Aktivitäten wie der Umgang mit Beschwerden oder Audits/Inspektionen sind so wichtig wie eh und je, gleichzeitig sind aber kontinuierliche Verbesserungen, z. B. im Dialog mit Bürgern und Entscheidungsträgern, unerlässlich geworden.

Bei der geschlossenen Sitzung der Konferenz begrüßten die Datenschutzbeauftragten eine Initiative von Alex Türk, dem Vorsitzenden der französischen Datenschutzkommission *Commission Nationale de l'Informatique et des Libertés* (CNIL), mit der dringlichen Aufforderung, die fundamentale Bedeutung des Datenschutzes und des Schutzes der Privatsphäre in einer sich rasch ändernden Welt erneut zu Gehör zu bringen und zu betonen, dass neue Herausforderungen dringender Maßnahmen bedürfen. Eine Kopie des Berichts „Datenschutz vermitteln und effektiver gestalten“ findet sich in der Anlage zu diesem Kommunique.

Die Datenschutzbeauftragten setzten sich mit ihrer eigenen Rolle und den Herausforderungen auseinander, die diese Veränderungen für sie bedeuten. Folgende Bereiche wurden von den Datenschutzbeauftragten als erforderlich erachtet, um sich den Herausforderungen stellen zu können:

- **Für die Gesellschaft ist der Schutz der Personendaten ihrer Bürger unerlässlich.** Er steht auf gleicher Ebene wie die Presse- und die Bewegungsfreiheit. Datenschutz ist möglicherweise genauso kostbar wie die Luft, die wir atmen. Beide sind unsichtbar, aber ihr Verlust ist gleichermaßen mit katastrophalen Folgen verbunden.

- **Datenschutzbeauftragte sollten eine neue Kommunikationsstrategie** entwickeln, um die Öffentlichkeit und maßgebliche Interessenvertreter auf ihre Rechte und deren Bedeutung aufmerksam zu machen. Datenschutzbeauftragte sollten wirkungsvolle langfristige Kampagnen zur Bewusstseinssteigerung ins Leben rufen und die Effektivität dieser Maßnahmen messen.

- **Datenschutzbeauftragte sollten ihre eigenen Aktivitäten besser vermitteln** und Datenschutz konkreter machen. Nur wenn diese Aktivitäten für die Bevölkerung insgesamt bedeutungsvoll, zugänglich und relevant sind, ist es möglich, die Macht zu erhalten, die erforderlich ist, um die öffentliche Meinung zu beeinflussen und von Entscheidungsträgern gehört zu werden.

- **Datenschutzbeauftragte sollten ihre Effizienz und Effektivität beurteilen** und – sofern nötig – ihre Praktiken entsprechend anpassen. Sie sollten mit ausreichenden Befugnissen und Mitteln ausgestattet werden und diese auf selektive und pragmatische Weise einsetzen. Sie sollten sich auf schwere mögliche Schäden und Hauptrisiken konzentrieren, denen der Einzelne ausgesetzt ist.

- **Datenschutzbeauftragte sollten ihre Kapazitäten im technologischen Bereich ausweiten** und mit fortgeschrittenen Studien, Fachwissen und Interventionen arbeiten. Sie sollten im Bereich der neuen Technologien eng mit Forschung und Industrie zusammenarbeiten und sich diese Arbeit untereinander teilen. Das übermäßig „rechtsbetonte“ Image des Datenschutzes muss korrigiert werden.

- **Datenschutzbeauftragte sollten die Internationale Konferenz neu strukturieren**, sodass diese bei internationalen Themen eine stärkere Stimme erhält und bei landesübergreifenden Initiativen, die einen Einfluss auf den Datenschutz haben, zu einem unvermeidbaren Diskussionspartner wird.

- **Datenschutzbeauftragte sollten sich für die Einrichtung einer Internationalen Konvention** und die Entwicklung anderer globaler Instrumente einsetzen. Probleme allgemeiner oder spezifischer Art, die nur auf internationaler Ebene effektiv bewältigt werden können, sollten auf diese Weise mit geeigneten Mitteln angegangen werden.

- **Datenschutzbeauftragte sollten die Einbeziehung anderer, nationaler wie auch internationaler Interessenvertreter** aus dem Bereich des Datenschutzes und des Schutzes der Privatsphäre fördern, z. B. die Zivilgesellschaft und Nichtregierungsorganisationen, um geeignete strategi-

sche Partnerschaften mit dem Ziel aufzubauen, ihre Arbeit effektiver zu machen.

In diesem Sinne werden die Datenschutzbeauftragten eine Reihe von Folgeaktivitäten ergreifen und deren Fortschritt bei der nächsten Internationalen Konferenz beurteilen.

Die Datenschutzbeauftragten setzten sich nicht nur mit ihrer eigenen Rolle auseinander, sondern fassten auch die folgenden wichtigen Beschlüsse:

- Akkreditierung von acht neuen Mitgliedern, den Datenschutzbehörden von:

  – Andorra
  – Liechtenstein
  – Estland
  – Rumänien
  – Kanada - New Brunswick
  – Kanada - Northwest Territories
  – Kanada - Nunavut
  – Gibraltar

- Beschluss zur Konferenzorganisation

- Beschluss zum Schutz der Privatsphäre und zu Suchmaschinen

Zum Abschluss: Die Herausforderungen, denen Gesellschaft und Datenschutzbeauftragte gegenüberstehen, sind erheblich, nicht nur in Bezug auf die Überwachung, sondern auch aufgrund der rapiden Veränderungen in der Datenverarbeitungstechnologie, der zunehmenden Globalisierung, der Unumkehrbarkeit bestimmter Entwicklungen und des Mangels an öffentlichem Bewusstsein und Aufklärung. Datenschutzvorkehrungen und die unabhängigen Behörden, die bei Entwurf und Durchsetzung dieser Vorkehrungen helfen, sind im modernen Informationszeitalter unerlässlich. Die Datenschutzbeauftragten haben sich der Herausforderung gestellt und dazu verpflichtet, ihren Einsatz zu verdoppeln und dafür zu sorgen, dass Datenschutzkontrollen heute und in Zukunft mehr Relevanz haben als zu der Zeit, als viele der heutigen Entwicklungen noch in den Kinderschuhen steckten.

Entschließung zum Datenschutz bei Suchmaschinen[1]

– Übersetzung aus dem Englischen –

Vorgeschlagen von: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützer: Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Irland (Datenschutzbeauftragter), Neuseeland (Datenschutzbeauftragter), Norwegen (Datatilsynet), Polen (Generalinspektor für den Schutz personenbezogener Daten)

Entschließung[2]

Heutzutage sind Suchmaschinen der Schlüssel zum „cyberspace" geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

Die steigende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer solcher Suchmaschinen.

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Viele IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heute unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensitive Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

---

[1] Diese Entschließung bezieht sich nicht auf Suchfunktionen, die von Inhalteanbietern für ihre eigenen Angebote angeboten werden. Für den Zweck dieser Entschließung wird „Suchmaschine" definiert als ein Service zum Auffinden von Ressourcen im Internet über verschiedene Websites hinweg und basierend auf nutzerdefinierten Suchbegriffen.

[2] Diese Entschließung betrifft nicht Probleme, die durch die Praxis vieler Betreiber von Suchmaschinen aufgeworfen werden, Kopien des Inhalts von Internetseiten einschließlich darauf enthaltener personenbezogener Daten, die dort legal oder illegal veröffentlicht werden, zu speichern und zu veröffentlichen („caching").

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen[3]. Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Es ist offensichtlich, dass diese Informationen unter Umständen auf einzelne Personen zurückgeführt werden können. Deswegen sind sie nicht nur für die Betreiber von Suchmaschinen selbst von Nutzen, sondern auch für Dritte. So hat zum Beispiel vor kurzem ein Ereignis das Interesse unterstrichen, dass Strafverfolgungsbehörden an diesen Daten haben: Im Frühjahr 2006 forderte das Justizministerium der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer kombinierten Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL umgehend zurückgezogen wurde, als der Fehler dort erkannt worden war – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in durchsuchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur die Verkehrsdaten, sondern auch der Inhalt von Suchanfragen personenbezogene Informationen darstellen können.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen können. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zur einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrs- und Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt

[3] Vgl. z. B. den gemeinsamen Standpunkt zu Datenschutz und Suchmaschinen (zuerst verabschiedet auf der 23. Sitzung in Hongkong SAR, China, 15. April 1998, überarbeitet und aktualisiert bei der 39. Sitzung, 6.–7. April 2006, Washington D. C.) der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation; http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_de.pdf. Vgl. ebenfalls Kapitel 5: „Surfen und Suchen“ des Arbeitsdokuments der Artikel-29-Gruppe „Privatsphäre im Internet – ein integrierter EU-Ansatz zum Online-Datenschutz“; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpddocs/2000/wp37de.pdf.

werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

Empfehlungen

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz, und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.

2. Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z. B. zur Nutzung für spätere Suchvorgänge).

3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.[4]

[4] Für den Zweck dieser Erklärung bedeutet „Dritter" jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle außer der betroffenen Person, dem für die Verarbeitung Verantwortliche, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

Entschließung zur Konferenzorganisation
„Datenschutz vermitteln und effektiver gestalten“

Ursprung dieser Initiative

Dieser Bericht hat seinen Ursprung in der Rede von Alex Türk, dem Vorsitzenden der französischen Datenschutzbehörde (CNIL), anlässlich einer im Mai 2006 vom polnischen Generalinspektor für Datenschutz in Warschau abgehaltenen Konferenz zum Thema „Öffentliche Sicherheit und Schutz der Privatsphäre“. Alex Türk sprach über seine ernste Besorgnis angesichts der Herausforderungen, denen die Datenschutzbehörden zurzeit gegenüberstehen. Er betonte, dass die Datenschutzbehörden ihre Aktivitäten dringend auf diese Herausforderungen ausrichten müssten, da andernfalls Gefahr bestehe, dass die den Datenschutzbestimmungen zugrunde liegende Philosophie in kürzester Zeit an Gehalt verliere.

Im Anschluss an die Konferenz lud der Europäische Datenschutzbeauftragte (EDPS) den CNIL ein, eine gemeinsame Initiative ins Leben zu rufen, um die Notwendigkeit dieser dringlichen Maßnahmen bei der Konferenz in London zu präsentieren. Der britische Datenschutzbeauftragte gab der Initiative sofort volle Unterstützung. Vorliegender Bericht wurde in enger Zusammenarbeit der drei genannten Datenschutzbehörden erstellt.

Durch ihren Beitritt zu dieser Initiative verpflichten sich die teilnehmenden Datenschutzbehörden, ihre Aktivitäten im Hinblick auf die folgenden Ziele zu koordinieren:

– Entwicklung von Kommunikationsaktivitäten auf der Grundlage gemeinsamer Ideen, von denen einige in beigefügtem Text zum Ausdruck gebracht werden

– Anpassung der eigenen Verfahrensweisen und Methoden durch eingehende Beurteilung ihrer Effektivität und Effizienz sowie durch Ausweitung ihrer Kapazitäten in den Bereichen technische Kompetenz, Trendprognose und Intervention im technologischen Bereich

– Beitrag zur institutionellen Anerkennung von Datenschutzbehörden auf internationaler Ebene und Förderung der Einbeziehung anderer relevanter Interessenvertreter auf nationaler und internationaler Ebene

Zum gegenwärtigen Zeitpunkt haben die folgenden Datenschutzbehörden bestätigt, diese Initiative grundsätzlich zu unterstützen:

– Commission nationale de l’informatique et des libertés (Frankreich)
– European Data Protection Supervisor (Europäische Union)
– Information Commissioner (Großbritannien und Nordirland)

– Privacy Commissioner of Canada (Kanada)
– Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Deutschland)
– Agencia Española de Protección de Datos (Spanien)
– Garante per la Protezione dei Dati Personali (Italien)
– College Bescherming Persoonsgegevens (Niederlande)
– Privacy Commissioner (Neuseeland)
– Préposé fédéral à la protection des données et à la transparence (Suisse) / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland)

Die gemeinsame Initiative wird während der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London am 2. – 3. November präsentiert. Sie ist nicht als Beschluss formuliert. Das Dokument wird als gemeinsame Initiative des französischen, europäischen und britischen Datenschutzbeauftragten präsentiert, unterstützt von den oben genannten Datenschutzbehörden, die sich auf diese Weise verpflichten, die Initiative in ihren Aktivitäten zu berücksichtigen. Die anderen bei der Konferenz vertretenen Datenschutzbehörden werden eingeladen, ihre Unterstützung der Initiative zum Ausdruck zu bringen oder auch beizutreten, wenn sie dies wünschen. Sie werden nicht aufgefordert, dieses Dokument offiziell zu verabschieden.

Nach einer einführenden Erinnerung, warum Datenschutz für unsere Gesellschaften unerlässlich ist (I), analysiert der Text im Einzelnen die Bedrohungen, denen persönliche Freiheiten und Datenschutz heute weltweit ausgesetzt sind und die ebenso viele Herausforderungen für die Aufsichtsbehörden darstellen (II). Aus den Ausführungen werden verschiedene Vorschläge für koordinierte Aktivitäten und Initiativen hergeleitet (III), wie auch für die Entwicklung einer neuen Kommunikationsstrategie (IV).

I – DATENSCHUTZ IST FÜR DIE GESELLSCHAFT UNERLÄSSLICH

1. Für die Gesellschaft ist der Schutz der Personendaten ihrer Bürger unerlässlich. Er steht auf gleicher Ebene wie die Presse- und die Bewegungsfreiheit. Da unsere Gesellschaften zunehmend auf Informationstechnologie angewiesen sind und immer mehr Personendaten erhoben oder erstellt werden, ist es wichtiger als je zuvor, dass individuelle Freiheiten und andere legitime Interessen der Bürger durch geeignete Datenschutzpraktiken auf angemessene Weise respektiert werden.

2. Datenschutz ist kein abstraktes, theoretisches, ganz zu schweigen ein „theologisches“ Thema und darf nicht als solches betrachtet werden. Bestimmungen zum *Datenschutz* dienen dem Schutz des *Einzelnen*. Sie zielen auf die Wahrung des Rechts ab, nicht auf missbräuchliche oder unkontrollierte

Weise erfasst oder überwacht zu werden. Sie zielen auf die Verteidigung der menschlichen Würde ab und sollen den Einzelnen in die Lage versetzen, seine Rechte auszuüben und seine legitimen Interessen zu schützen.

3. Datenschutz kann nur dann Realität werden, wenn Datenschutzbestimmungen in der Praxis befolgt werden. Datenschutzbehörden spielen eine wichtige Rolle, indem sie dafür sorgen, dass die Bestimmungen eingehalten werden. Sie können aber nur dann erfolgreich sein, wenn sie das Thema Datenschutz auf effektive Weise vermitteln, andere relevante Interessenvertreter involvieren und – falls nötig – ihre Ermittlungs- und Durchsetzungsrechte auf effektive Weise ausüben.

II – ZWEI GEFAHRENWELLEN, DREI HERAUSFORDERUNGEN

4. Die Freiheit des Einzelnen, aber auch die Datenschutzbehörden selbst sind bislang nicht da gewesenen Risiken ausgesetzt. Sie sind der Bedrohung unterworfen, von zwei Gefahrenwellen überrollt zu werden, stehen aber zusätzlich noch vor einer dritten Herausforderung.

A – Die erste Herausforderung gründet sich auf viele unterschiedliche Faktoren, die mit dem Tempo technologischer Veränderungen in Zusammenhang stehen

5. **Beschleunigung:** Internet, RFID, Nanotechnologien etc. Datenschutzbehörden sind Innovation und technologischem Fortschritt gegenüber nicht feindlich eingestellt. Aber der Zeitraum von der Entdeckung eines Phänomens bis zu dessen technischer Umsetzung, von einer Innovation zur nächsten, von der Entwicklung eines Prototyps bis zu dessen industrieller Anwendung wird kürzer und kürzer. Versuche zur Gesetzesanpassung und Gesetzgebung können immer weniger mit der technologischen Entwicklung Schritt halten. Das Tempo der technologischen Entwicklung wird immer schneller, während das Tempo der Gesetzgebung nach wie vor sehr langsam ist, da es an den von demokratischen Verfahrensweisen auferlegten Rhythmus angepasst ist.

6. **Globalisierung:** Die örtliche Verlagerung der Datenverarbeitung steht in voller Blüte. Es lässt sich wohl kaum bestreiten, dass der internationale Datentransfer sehr schwer zu kontrollieren ist. Dieser Trend hin zur Globalisierung steht im Konflikt mit einem der Hauptmerkmale der Rechtsstaatlichkeit – ihrer geografisch beschränkten Anwendbarkeit.

7. **Ambivalenz:** Technologische Innovation bringt sowohl Fortschritt als auch Gefahren mit sich. Für den Einzelnen mögen die aus Technologie erwachsenden Vorteile und Bequemlichkeiten eine große Verlockung darstellen, die

Risiken werden ihm vielleicht jedoch erst dann bewusst, wenn er oder jemand anders zu Schaden gekommen und es zu spät ist. Vielen Menschen ist es egal, dass alle ihre Bewegungen, Aktivitäten und Beziehungen nachvollzogen und potenziell überwacht werden können. Diese Zwiespältigkeit gegenüber der Technologie lässt sich nur schwer mit der Rechtsstaatlichkeit vereinbaren, die definitionsgemäß fest umrissene Antworten geben möchte.

8. **Unvorhersehbarkeit:** Die Anwendung neuer Technologien entwickelt sich manchmal in Richtungen, die anfangs selbst von den Entwicklern der Technologie nicht vorhergesehen wurden. Diese nicht vorhersehbaren Einsatzmöglichkeiten können schwer zu kontrollieren sein, insbesondere wenn die Anwendung einer Technologie von den ursprünglich geplanten Einsatzmöglichkeiten – auf die das Gesetz einfach anwendbar erschien – völlig abweicht.

9. **Unsichtbarkeit (virtuelle Unsichtbarkeit/körperliche Unsichtbarkeit):** Die Datenverarbeitung ist immer weniger sichtbar und greifbar, gleichzeitig auch immer weniger kontrollierbar. Moderne Technologien tendieren zu Unsichtbarkeit, erstens, weil ein großer Teil der Datenverarbeitung stattfindet, ohne dass sich der Einzelne ihrer Existenz bewusst ist (z. B. Nachverfolgbarkeit der Nutzung öffentlicher Verkehrsmittel, des Surfverhaltens im Internet, der elektronischen Kommunikation, der Telefonkommunikation usw.). Da die Prozesse unsichtbar sind, kann man hier von virtueller Unsichtbarkeit sprechen. Technologie wird aber auch unsichtbar aufgrund ihrer extremen Miniaturisierung, die man als körperliche Unsichtbarkeit bezeichnen kann. In ein paar Jahren wird die Entwicklung von Nanotechnologien dazu führen, dass man die in einem Gegenstand enthaltene Technologie mit dem bloßen Auge nicht mehr erkennen kann. Wie will man Verarbeitungsprozesse überwachen, die von unsichtbaren Technologien ausgeführt werden?

10. **Irreversibilität:** Technologischer Fortschritt lässt sich nicht umkehren: Wir werden nie wieder in einer Welt ohne Computer, Internet, Handys, biometrischer Identifizierung, Geolokalisierung und Videoüberwachung leben. In dem Maße, wie diese Technologien konvergieren und immer stärker miteinander verwoben werden, können sie in ihrer Gesamtheit eine echte Gefahr für unsere Gesellschaft darstellen.

B – Die zweite Herausforderung ist gesetzlicher Art, insbesondere in Bezug auf die neuen Antiterrorgesetze

11. Der Erlass von Antiterrorgesetzen bedeutet eine Herausforderung für die Datenschutzbehörden, die in diesem Zusammenhang Fallen vermeiden, Illusionen aufgeben und Mythen bekämpfen müssen.

12. **Die Notwendigkeit von Ausgewogenheit:** Unabhängige Datenschutzbehörden sind weder Gesetzgeber noch Gerichtshöfe noch Aktivisten, spielen aber dennoch eine äußerst spezifische Rolle. In den seltensten Fällen ist es ihnen möglich, Probleme auf klar umrissene Weise zu lösen. Alle Datenschutzbehörden erkennen die Legitimität von Antiterrorgesetzen an, wie sie in den vergangenen Jahren entwickelt wurden. Vor dem Hintergrund des Auftrags, den die Datenschutzbehörden vom Gesetz erhalten haben, und im Auftrag der Gesellschaft insgesamt ist es jedoch ihre Pflicht, kontinuierlich nach dem richtigen Gleichgewicht zwischen den Erfordernissen der öffentlichen Sicherheit einerseits und der Notwendigkeit des Datenschutzes und des Schutzes der Privatsphäre andererseits zu streben. Sie müssen diese Rolle vollkommen unabhängig erfüllen und die inakzeptablen Anschuldigungen verantwortungslosen Handelns von sich weisen, die gelegentlich gegen sie vorgebracht werden.

13. **Die Gefahr, in einen Teufelskreis zu geraten:** Dieses Risiko – eine Art „schleichende Funktionsausweitung" – sieht folgendermaßen aus: Eine Datenbank wird zu einem bestimmten Zeitpunkt in einer bestimmten Situation angelegt. Die Aufsichtsbehörde ist in die Entwicklung der Datenbank involviert. Zu einem späteren Zeitpunkt erweitert sich der Wirkungsbereich dieser Datenbank. Beispielsweise werden zunächst die Kategorien der erfassten Personen erweitert, dann die Gründe, warum jemand registriert werden kann, später wiederum die Kategorien der Personen, die Zugriff auf die Datenbank haben. In diesen späteren Phasen steht die Behörde dem Argument gegenüber, dass sie eine einfache Erweiterung nicht verweigern kann, da sie das Prinzip zur Erstellung der ursprünglichen Datenbank akzeptiert hat, und so weiter. Und dies, obwohl der ursprünglich akzeptierte Umfang des Systems zwischen der ersten und der letzten Entwicklungsphase so stark vergrößert wurde, dass er nicht länger akzeptabel ist.

14. **Das Trugbild der mustergültigen Natur von Präzedenzfällen in anderen Ländern:** Landesregierungen bringen als Angriff auf die landeseigene Datenschutzbehörde häufig das Argument vor, dass ein anderes Land bereits ein bestimmtes System eingeführt hat, wenn diese sich sträubt, ein in anderen Ländern verwendetes System diskussionslos zu akzeptieren. Dies führt zu ernsten Harmonisierungsproblemen und dazu, dass die Datenschutzbehörden einen gemeinsamen Nenner finden und gemeinsam nachdenken müssen.

15. **Die Illusion der Datenbank als Allheilmittel:** Die Datenschutzbehörden müssen Öffentlichkeit und Regierung fortwährend daran erinnern, dass durch die Schaffung von Datenbanken mit immer mehr Personendaten nicht alle Probleme gelöst werden können. Der „Glorienschein" der angeblich unfehlbaren Computerdatei erweist sich häufig als Illusion. Außerdem steigt

mit der Verarbeitung von immer mehr Personendaten auch das Risiko falscher Zuordnungen, veralteter Informationen und anderer Fehler. Dies kann den Lebenschancen, der Gesundheit, dem Wohlstand und selbst der Freiheit des Einzelnen ernstlich schaden.

16. **Der Mythos der unfehlbaren Datei (das „Mehrheits-/Minderheitsproblem"):** Nur allzu häufig wird völlig unfundiert angenommen, dass wir alle aus gutem Grund in einer Datenbank erfasst werden – mit dem Ergebnis, dass sich Personen, die unnötig oder unangemessen erfasst werden („die Minderheit"), gelegentlich in unmöglichen Situationen wiederfinden, da jeder der Ansicht ist, es sei praktisch unmöglich, in einem derart effizienten System grundlos erfasst zu werden. Aus diesem Grund ist es aus ethischer Sicht äußerst wichtig, immer wieder darauf hinzuweisen, dass Technologie nicht unfehlbar ist, und die automatische Entscheidungsfindung, insbesondere in Bereichen wie Sicherheit und Recht, zu verbieten.

C – Bei der dritten Herausforderung geht es um den Ruf

17. Zumindest in einigen Ländern genießen Datenschutz und Datenschutzbehörden nicht den guten Ruf, den sie verdienen. Es kann die Auffassung herrschen, dass die Bestimmungen komplex sind und sich in der Praxis nur schwer auf konsequente, vorhersehbare und realistische Weise umsetzen lassen. Manche kritisieren die Kontrolle des Datenschutzes als übertrieben abstrakt und nicht ausreichend auf tatsächliche und potenzielle Gefahren ausgerichtet, die sowohl für den Einzelnen als auch für die Gesellschaft insgesamt erwachsen, wenn die Bestimmungen nicht beachtet werden. Andere kritisieren die Art und Weise, in der diese Bestimmungen umgesetzt und durchgesetzt werden, und den Mangel an positiven oder negativen Anreizen zur Einhaltung der Bestimmungen oder zur Investition in angemessene Maßnahmen. Negative Auffassungen wie diese werden von Politikern, Verwaltungsbeamten, Unternehmen, den Medien und manchmal auch von Privatpersonen vertreten. Es ist wichtig, gegen derartige Ansichten vorzugehen, die praktische Bedeutung des Datenschutzes aufzuzeigen, die viel besprochenen Grundrechte und Grundfreiheiten zur Realität zu machen und die derzeitigen Praktiken – sofern angemessen – zu überdenken.

III – AUFGABEN UND INITIATIVEN FÜR DATENSCHUTZBEHÖRDEN

18. Die Datenschutzbehörden müssen dringend Maßnahmen ergreifen, um in ihren Bürgern ein gesteigertes Bewusstsein und ein besseres Verständnis der ernsten Risiken zu wecken, die ihre persönlichen Freiheiten in ihrem jeweili-

gen Land bedrohen. Sie müssen ferner ihre Arbeitsmethoden und ihre Effizienz und Effektivität überdenken.

A – Die Datenschutzbehörden müssen gemeinsam Änderungen und koordinierte Strategien vorbringen, um so auf neue, effektivere und sachdienlichere Weise zu handeln

19. **Stärkung der Kapazitäten in den Bereichen Fachwissen, fortgeschrittene Studien und Intervention im Technologiesektor:** Der Datenschutz leidet zurzeit unter seinem übermäßig „rechtsbetonten" Image. Die Glaubwürdigkeit unserer Institutionen hängt jedoch schon heute und auch in Zukunft immer mehr von unserer Fähigkeit ab, technologische Entwicklungen zu verstehen, zu analysieren und vorherzusehen.

20. Zur Analyse dieser neuen Trends müssen die Datenschutzbehörden Strategien erarbeiten, um sich die Arbeit abhängig vom jeweiligen Fall, ihren Erfahrungen, Zuständigkeiten und praktischen Maßnahmen zu teilen.

21. Sie müssen überlegen, welche Beziehungen sie im Bereich neue Technologien zu Forschung und Industrie aufbauen wollen. Sie müssen die Vorteile eines guten Datenschutzes gegenüber Wirtschaft und öffentlichen Körperschaften betonen.

22. **Beurteilung unserer Effektivität und Änderung unserer Praktiken:** Wir müssen unbedingt eine detaillierte und ehrliche Beurteilung der Effektivität einer jeden Behörde durchführen. Zeigt die Arbeit der jeweiligen Behörde wirklich Auswirkungen, erreicht sie etwas in der Praxis? Werden Worte in Taten umgesetzt? Durch derartige Beurteilungen lernen wir, wie wir unsere Ergebnisse verbessern können.

23. Die Beurteilung der Effektivität aller Behörden wird sicherlich dazu führen, dass einige von ihren Gesetzgebern verlangen, sie mit ausreichend Befugnissen und Mitteln auszustatten. Möglicherweise werden auch Fragen zu den Praktiken einiger Behörden aufgeworfen. Wir alle müssen Prioritäten setzen, insbesondere was Gefahr und Schwere eines möglichen Unheils anbelangt. Wir müssen uns primär auf die Hauptrisiken konzentrieren, denen der Einzelne ausgesetzt ist, und vorsichtig sein, dass wir bei Angelegenheiten, die es nicht verdienen, nicht übermäßig puristisch und rigide vorgehen. Wir müssen zu größerem Pragmatismus und mehr Flexibilität bereit sein.

B – Datenschutzbehörden müssen gemeinsam überlegen, wie sie auf internationaler Ebene eine bessere institutionelle Anerkennung ihrer Aktivitäten erzielen und andere Interessenvertreter involvieren können

24. **Eine notwendige Umstrukturierung der Internationalen Konferenz:** Globale Herausforderungen brauchen globale Lösungen. Die Internationale Konferenz der Datenschutzbeauftragten muss an der Spitze unserer Aktivitäten auf internationaler Ebene stehen. Wir müssen für die Lebens- und Existenzfähigkeit der Konferenz sorgen, ihre Funktionsweise verbessern, sie sichtbarer und effizienter machen und einen Aktionsplan – ein Kommunikationsprogramm – erarbeiten. Dazu gehört möglicherweise, dass wir darüber nachdenken, ein permanentes Sekretariat für die Konferenz einzurichten. Die Konferenz muss zu einem unvermeidbaren Gesprächspartner bei allen internationalen Initiativen werden, die einen Einfluss auf den Datenschutz haben. Sie muss Raum für Gespräche bieten und Vorschläge aufkommen lassen, damit internationale Initiativen besser verfolgt, Praktiken aufeinander abgestimmt und gemeinsame Standpunkte bezogen werden.

25. **Ausarbeitung einer internationalen Konvention und anderer globaler Instrumente:** In der Erklärung von Montreux (2005) forderten die Datenschutzbeauftragen eine universelle Konvention für den Datenschutz. Diese Initiative muss von den Datenschutzbehörden mit den zuständigen Institutionen unterstützt werden, mit gebührlichem Respekt für deren institutionelle Position und ggf. für die notwendigen Vorbedingungen einer landesinternen Koordination. Innerhalb dieses Rahmenwerks sollten sich die Datenschutzbehörden bemühen, die Initiative in ihrem jeweiligen Einflussbereich voranzutreiben, vor allem innerhalb der regionalen Organisationen und der Sprachzonen, in denen sie tätig sind. In bestimmten Sektoren (z. B. Internetkontrolle, Finanztransaktionen, Flugverkehr) kann die Notwendigkeit globaler Lösungen zur Respektierung von Privatsphäre und Datenschutz entstehen, worauf die Datenschutzbehörden mit allen geeigneten Mitteln eingehen müssen.

26. **Involvierung anderer Interessenvertreter (Einrichtungen der Zivilgesellschaft, Nichtregierungsorganisationen usw.):** Zurzeit sind sowohl national als auch international diverse andere Interessenvertreter für den Datenschutz und den Schutz der Privatsphäre aktiv, auf unterschiedlichen Ebenen und in unterschiedlichen Sektoren. Derartige Organisationen können als strategische Partner agieren und wesentlich dazu beitragen, dass die Datenschutzbehörden effektiver werden. Die Kooperation mit anderen geeigneten Interessenvertretern sollte daher gefördert oder aktiv entwickelt werden.

IV – EINER NEUEN KOMMUNIKATIONSSTRATEGIE ENTGEGEN

27. Kommunikation ist eine Hauptvoraussetzung, um Datenschutz effektiver zu machen. Eine Botschaft, die nicht ankommt und nicht verstanden wird, ist im

Grunde genommen nicht existent. Eine Meinung oder Entscheidung, auf die sich nicht zugreifen lässt, ist in ihrer Wirkung begrenzt und möglicherweise nicht die auf ihre Ausarbeitung verwendete Mühe wert.

A – Wir müssen dringend eine neue Kommunikationsstrategie entwickeln, sowohl auf nationaler als auch auf internationaler Ebene

28. **Kommunikation als Ziel.** Eine sehr viel bessere Kommunikation mit der Öffentlichkeit muss eines der Hauptziele aller Datenschutzbehörden sein. Es ist inakzeptabel, dass in einigen Ländern, in denen das Recht auf Datenschutz – ebenso wie die Bewegungs- und Pressefreiheit – zu den Grundrechten gehört, die große Mehrheit unserer Mitbürger sich dieser Rechte und ihrer Bedeutung nicht bewusst ist. Noch viel weniger akzeptabel ist dies, wenn eine negative Einstellung gegenüber dem Datenschutz herrscht.

29. Wir müssen wirkungsvolle Kampagnen zur langfristigen Bewusstseinssteigerung ins Leben rufen, die den Einzelnen über die Existenz und den Inhalt seiner Rechte informieren. Die Wirksamkeit dieser Maßnahmen muss gemessen werden. Dabei gibt es zwei spezifische Ziele:

    - Gewählte Vertreter auf landesweiter und kommunaler Ebene – die meisten von ihnen sind nicht besser informiert als der Durchschnittsbürger.

    - Junge Menschen, die wenig Interesse an diesen Fragen haben, da sie so sehr an neue Technologien gewohnt sind. Wir müssen so bald wie möglich im Bereich der Bildung und Aufklärung aktiv werden.

30. **Kommunikation als wirkungsvolles Hebelwerkzeug.** Es ist wichtig und dringlich, dass unsere Datenschutzbehörden bessere Handlungsmittel erhalten und Anerkennung auf internationaler Ebene zugesichert bekommen. Öffentliches Vertrauen und Unterstützung sind unerlässlich. Datenschutz muss konkreter gemacht werden. Nur Organisationen, die kommunizieren – normalerweise über die Medien und auf eine Art und Weise, die für die Öffentlichkeit insgesamt **bedeutungsvoll, zugänglich und relevant** ist – werden die Macht erhalten, die erforderlich ist, um die öffentliche Meinung zu beeinflussen, und somit von den Staaten und der internationalen Gemeinde gehört und ernst genommen zu werden. Nur wenn diese Bedingung erfüllt wird, können die Datenschutzbehörden unverzichtbare Handlungsmittel erhalten.

31. Das bedeutet, dass wir in allen unseren Behörden professionelle Kommunikationspartner einsetzen, und dass die vermittelten Botschaften in allen Datenschutzbehörden möglichst einheitlich sind.

B – Eine interessante Kommunikationsbotschaft könnte im Aufzeigen einer Parallele zwischen dem Schutz der persönlichen Freiheiten und dem Schutz der Umwelt liegen

32. Was die Umwelt anbelangt, so werden wir nicht ungestraft davonkommen. Auf die gleiche Weise müssen wir im Bereich des Datenschutzes bei jeder unkontrollierten technologischen Entwicklung und jedem Gesetz, das ohne klare Vision der potenziellen Risiken erlassen wird, höchste Vorsicht walten lassen. In einem solchen Fall besteht die Gefahr, dass unser „Kapital" in Form von Freiheit und Identität reduziert oder sogar zunichte gemacht wird. Auch kann es nicht wiedergewonnen werden, und zwar genau deshalb, weil technologische Innovation irreversibel ist.

33. Möglicherweise sind Datenschutz und der Schutz der Privatsphäre genauso kostbar wie die Luft, die wir atmen. Beide sind unsichtbar, aber ihr Verlust ist gleichermaßen mit katastrophalen Folgen verbunden.

V – PROGRAMM ANSCHLIESSENDER AKTIVITÄTEN

34. Die Besprechung dieser Initiative bei der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London sollte als erster Schritt in Richtung eines wachsenden Konsenses gesehen werden – eines Konsenses über die Notwendigkeit zur Ausarbeitung von Mitteln für bessere Kommunikation und effektiveren Datenschutz.

35. Datenschutzbehörden, die diese Initiative unterstützen, verpflichten sich zur Weiterentwicklung von und übernehmen ggf. die Verantwortung für eine Reihe von Aktivitäten, die bei der nächsten Konferenz in Montreal vorgestellt und weiter verfolgt werden, z. B.:

- Workshop zu strategischen Themen: Bedingungen, um Datenschutzbehörden effektiver zu machen; mögliche Entwicklung von „Prinzipien einer guten Überwachung" beim Datenschutz; Informationen zu Best Practice (Datenschutzbeauftragte und strategische Mitarbeiter); Überlegungen hinsichtlich der Entwicklung einer internationalen Konvention

- Workshop zum Thema Kommunikation: Verfügbares Expertenwissen im Bereich der Datenschutzkommunikation (z. B. Kampagnen, Meinungsforschung); Entwicklung einer gemeinsamen Botschaft und wirksamer Hilfsmittel für deren Verbreitung (professionelle Kommunikationspartner)

- Workshop zum Thema Durchsetzung: Verfügbares Expertenwissen im Bereich Überwachung und Gewährleistung der Vorschriftenbefolgung;

wirksame Mechanismen zur Inspektion (z. B. Audits) und Intervention (Datenschutzbeauftragte und Personal von Durchsetzungsbehörden)

- Workshop zur internen Organisation: Jüngste Erfahrungen mit organisatorischen Veränderungen; Projekte zur Verbesserung von Effizienz und Effektivität (Datenschutzbeauftragte und organisatorisches Personal)

- Alle sonstigen Aktivitäten, die für diese Initiative als relevant erachtet werden

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 39. Sitzung am 6./7. April 2006 in Washington D. C. (USA)

Arbeitspapier zur Online-Verfügbarkeit elektronischer Gesundheitsdaten

– Übersetzung –

Die Arbeitsgruppe hat die steigende Bedeutung Web-basierter Telemedizin bereits in der Vergangenheit unterstrichen[1]. Die Verfügbarkeit elektronischer Gesundheitsdaten in Netzwerken (insbesondere im Internet) während der Lebenszeit eines Patienten und darüber hinaus wirft komplexe zusätzliche Fragen auf. Diese Online-Verfügbarkeit elektronischer Gesundheitsdaten wird hauptsächlich aus den folgenden Gründen favorisiert:

– geringere Kosten für die Verarbeitung medizinischer Daten,

– die unmittelbare, „ubiquitäre“ und (scheinbar) komplette Verfügbarkeit der Daten
  - für Doktoren, um zur Gesundheit des Patienten beizutragen,
  - für die Patienten selbst,

– der Patient könnte seine oder ihre Einwilligung online leichter als offline geben.

Gesundheitsinformationen in Netzwerken könnten auch für Forschungs- und Qualitätsmanagementszwecke genutzt werden. Die Diskussion der weitergehenden Implikationen dieser Entwicklung kann in dieser Arbeitsgruppe nicht geführt werden. Es ist allerdings darauf hinzuweisen, dass elektronische Gesundheitsinformationen in Netzwerken generell das Interesse von Dritten auf sich ziehen werden, wie z. B. von Versicherungsunternehmen und Strafverfolgungsbehörden.

[1] Arbeitspapier zu „netzwerkbasierte Telemedizin“, angenommen auf der 31. Sitzung am 26./27. März 2002 in Auckland (Neuseeland) – aktualisiert auf der 38. Sitzung am 6./7. September 2005 (Berlin) <http://ww.datenschutz-berlin.de/doc/int/iwgdpt/wpmed_en.pdf>

Die besondere Sensitivität von Gesundheitsdaten muss bedacht werden, wenn die Online-Verfügbarkeit elektronischer Gesundheitsdaten erwogen wird. Ärzte haben von je her die Verpflichtung gehabt, Informationen von Patienten unter dem hippokratischen Eid[2] sind vertraulich zu behandeln. Die Aufgabe, sich um die Gesundheit und das Leben des Patienten zu kümmern, war nie eine Rechtfertigung dafür, solche Informationen an Dritte weiterzugeben, die nicht an der Behandlung des einzelnen Patienten beteiligt sind.

Heutzutage ist die Vertraulichkeit medizinischer Informationen in den meisten Ländern durch Strafgesetze geschützt. In einigen Ländern ist sogar die Beschlagnahme medizinischer Daten für Strafverfolgungszwecke verboten, soweit diese Daten im Besitz eines Arztes oder eines Krankenhauses sind. Dieser Standard muss auch aufrecht erhalten werden, wenn elektronische Gesundheitsdaten online gestellt werden sollen. Der Grad des Schutzes für Gesundheitsdaten des Patienten darf nicht davon abhängen, ob diese in konventioneller Weise in einer Akte gespeichert werden oder in einem Netzwerk.

Gesundheitsdaten zählen zu den sensitivsten und privatesten Informationen über den Einzelnen. Die Offenlegung eines Gesundheitszustandes oder einer Diagnose könnte das persönliche und berufliche Leben eines Einzelnen negativ beeinflussen. Sogar die Offenlegung einer geringfügigen Gesundheitsangelegenheit kann für den Patienten peinlich sein und ihn möglicherweise davon abhalten, in Zukunft professionelle medizinische Beratung in Anspruch zu nehmen. Beispiele für Diskriminierung infolge von nicht-autorisierter Weitergabe medizinischer Daten existieren auch bei traditioneller, papierener Aktenhaltung[3]. Betroffenen sind bereits die Einstellung in ein Arbeitsverhältnis, Versicherungen und Kreditzusagen wegen der Offenlegung medizinischer Informationen an unberechtigte Parteien verweigert worden. Die Aufbewahrung medizinischer Daten in elektronischer Form erhöht das Risiko, dass Patienteninformationen unbeabsichtigt offenbart oder in einfacher Weise an unberechtigte Parteien weitergegeben werden können.

Darüber hinaus gibt die Nutzung des unsicheren Internets und – sogar in noch größerem Maße – von ungeschützten drahtlosen Netzwerken[4] zur Speicherung und Übertragung von Gesundheitsdaten Anlass zu besonderen Besorgnissen.

---

2 „Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und was man nicht nach außen tragen darf, werde ich schweigen und es geheim halten. Wenn ich diesen Eid erfülle und ihn nicht verletzte, so möge ich mein Leben und meine Kunst genießen, respektiert von allen Menschen für alle Zeiten. Wenn ich ihn aber übertrete oder ihn verletze, dann soll das Gegenteil davon mein Los sein."

3 Siehe „Health Privacy Project, Medical Privacy True Stories" (10. November 2003), unter http://www.patientprivacyrights.org/site/DocServer/True_Stories.pdf?docID=321.

4 Vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen; verabschiedet am 15. April 2004 bei 35. Sitzung in Buenos Aires; http://www.datenschutz-berlin.de/doc/int/iwgdpt/1_de.pdf

Empfehlungen

Die Arbeitsgruppe gibt daher die folgenden vorläufigen Empfehlungen, die im Lichte zukünftiger rechtlicher Entwicklungen und technologischer Innovationen überprüft werden müssen:

1. Es muss sorgfältig evaluiert werden, welche Kategorien medizinischer Daten in elektronischer Form verfügbar gemacht oder online gestellt werden sollen. Bestimmte Kategorien von Gesundheitsdaten wie genetische oder psychiatrische Daten könnten von der Online-Verarbeitung insgesamt ausgeschlossen werden, oder zumindest besonders strikten Zugriffsbeschränkungen unterliegen müssen.

2. In jedem Fall sollte es der autonomen und freien Entscheidung des Patienten – unterstützt durch nutzerfreundliche Technologien – überlassen werden, welche personenbezogenen Gesundheitsdaten über ihn in einem elektronischen Gesundheitsdatensatz oder in einem Netzwerk gespeichert oder weitergegeben werden sollen, soweit dies nicht ausdrücklich durch nationales Gesetz verlangt wird. Diese Entscheidung soll die Möglichkeit der relevanten Gesundheitsdienste oder Ärzte, solche Informationen für Behandlungszwecke zu speichern, unberührt lassen. Die Einwilligung muss immer eine fundamentale Anforderung im medizinischen Bereich sein. Eine strikte Zweckbindung ist auch in einer online-Umgebung essentiell. Zu diesem Zweck müssen Gesundheitseinrichtungen ein internes Zugriffskontrollsystem implementieren, das ausreichend ist, die Privatsphäre des Patienten zu schützen.

3. Die Patienten müssen umfassend über die Art der Daten und die Struktur der elektronischen Gesundheitsdatensätze, in denen die Daten enthalten sind, informiert werden. Die Patienten sollten eine Alternative (konventionelle) Möglichkeit haben, über die auf sie bezogenen medizinischen Informationen Zugriff zu erhalten.

4. Es gibt zusätzliche Herausforderungen für die Vertraulichkeit, die der Online-Verfügbarkeit von Gesundheitsdaten inhärent ist. Die bloße Übertragung von gesetzlichen Standards zur Vertraulichkeit, die in einem traditionellen Umfeld mit papierenen Akten gelten, könnte unzureichend sein, um das Interesse eines Patienten an seiner Privatsphäre zu schützen, wenn elektronische Gesundheitsinformationen online verfügbar gemacht werden. Personenbezogene Gesundheitsinformationen dürfen nur in offenen Netzwerken verarbeitet werden, wenn diese durch starke Verschlüsselung und sichere Authentifizierungsmechanismen geschützt sind. Nur autorisiertem, medizinisch qualifiziertem Personal sollte erlaubt werden, auf spezifische Teile der elektronischen Gesundheitsakte online zuzugreifen, soweit dies unbedingt notwendig ist, und Zugriffe sollten protokolliert werden. Die Daten müssen und richtig und

aktuell gehalten werden. Patienten sollte eine nutzerfreundliche Möglichkeit haben, auf seine Protokolldaten online zuzugreifen, um in der Lage zu sein, festzustellen, wer auf seinen oder ihren Gesundheitsdatensatz zugegriffen hat.

5. Die Arbeitsgruppe empfiehlt die Entwicklung von Sicherheitsmindeststandards für den Umgang mit elektronischen Gesundheitsdaten. Diese sollten Standards zur Datenverschlüsselung enthalten, sowie Autorisierungsmechanismen, Transaktionsüberwachungsprozeduren, und Zugriffskontrollsysteme. Die Entwicklung von Grundschutzstandards würde betriebliche Datenschutzbeauftragte und Archivare von Daten in die Lage versetzen, den Patientendatenschutz sicherzustellen und gleichzeitig die Vorteile eines elektronischen Aktenhaltungssystems zu genießen. Die Arbeitsgruppe ermutigt alle Interessengruppen (öffentliche Einrichtungen, den Gesundheitssektor, die Industrie und Standardisierungsorganisationen) datenschutzkonforme Technologien für das elektronische Gesundheitswesen zu entwickeln und anzuwenden, die die notwendige Vertraulichkeit und Sicherheit bieten. Die Arbeitsgruppe begrüßt die gegenwärtig in der Internationalen Organisation für Standardisierung (ISO) diskutierte Initiative zur Verabschiedung eines Sicherheitsstandards für den Medizin- und Gesundheitssektor (mit dem Entwurf des ISO-Standards 27799, der den Informationssicherheits-Management ISO-Standard 17799 für den Gesundheitssektor adoptiert). Es muss jedoch festgestellt werden, dass diese internationalen Standards nationale Gesetzgebung zum Datenschutz nicht ersetzen können.

Die Arbeitsgruppe lädt den medizinischen Berufsstand und die Öffentlichkeit dazu ein, diese Empfehlungen zu kommentieren.

Gemeinsamer Standpunkt zu Datenschutz bei Suchmaschinen im Internet

– zuerst verabschiedet auf der 23. Sitzung in Hong Kong SAR, China, 15. April 1998 –

– überarbeitet und aktualisiert auf der 39. Sitzung, 6. – 7. April 2006, Washington, D.C. (USA) –

– Übersetzung –

Gegenwärtig enthält das Internet eine riesige Menge an Informationen über fast jeden Sachverhalt, den man sich vorstellen kann. Zum Auffinden der gewünschten Information im Internet sind Suchmaschinen zu einem unverzichtbaren Werkzeug geworden. Sie sind die Schlüssel zum „cyberspace“.

Mit diesen Suchmaschinen kann man nach veröffentlichten personenbezogenen Daten suchen. Als Ergebnis erhält man ein Profil der Aktivitäten einer bestimmten Person im Internet. Suchmaschinen können auch für das „data-mining“ genutzt werden. Da das Internet für den Austausch von Informationen und andere Aktivitäten (z. B. den elektronischen Geschäftsverkehr) immer populärer wird, kann dies zu einer Gefährdung der Privatsphäre führen.

Darüber hinaus können Betreiber von Suchmaschinen detaillierte Profile der Interessen ihrer Nutzer erstellen. IP-Protokolldaten ermöglichen die Identifizierung von Nutzern, insbesondere dann, wenn sie mit entsprechenden bei Zugangsdiensteanbietern gespeicherten Daten kombiniert werden. Da die Nutzung von Suchmaschinen heutzutage eine gängige Praxis unter Nutzern des Internet darstellt, ermöglichen bei den Betreibern populärer Suchmaschinen gespeicherte Verkehrsdaten detaillierte Profile über Interessen, Meinungen und Aktivitäten über verschiedene Bereiche hinweg (z. B. Beruf, Freizeit, politische Meinungen, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit besonders besorgt über die Möglichkeit gezeigt, Persönlichkeitsprofile von Bürgern zu erstellen. Dies ist jetzt in einem gewissen Maß auf globaler Ebene durch die im Internet zur Verfügung gestellte Technologie möglich geworden.

Die Arbeitsgruppe hat bereits in der Vergangenheit Probleme des Datenschutzes und der Privatsphäre im Zusammenhang mit der Nutzung des Internet betont und Empfehlungen zu möglichen Schritten zur Lösung dieser Probleme gegeben. Im Hinblick auf übermittelte oder veröffentlichte personenbezogene Daten erinnert die Arbeitsgruppe daran, dass auch personenbezogene Daten, die der Nutzer freiwillig veröffentlicht hat, auch dann noch den für sie geltenden Schutzbestimmungen unterliegen.

Empfehlungen

Nutzer des Internets können gleichzeitig auch Informationsanbieter sein. Sie sollten sich darüber im klaren sein, daß jedes personenbezogene Datum, das sie im Netz publizieren (z. B. bei der Einrichtung ihrer eigenen Homepage, oder bei der Veröffentlichung von Artikeln in newsgroups), von Dritten für die Erstellung eines Profils genutzt werden kann.

So können zum Beispiel Nachrichten in newsgroups oder bei „social networking“ Angeboten von Suchmaschinen durchsucht und indexiert werden, und damit zur Anreicherung von Profilen darüber beitragen, wer sich zu welchem Thema wie geäußert hat. Eine Möglichkeit, diese Gefährdung für die Privatsphäre zu redu-

zieren kann zum Beispiel bei der Teilnahme an newsgroups in der Nutzung von Pseudonymen bestehen.

Daher sollten Diensteanbieter und Softwarehersteller im Internet ihren Nutzern die Nutzung ihrer Dienste unter Pseudonym anbieten. Jedenfalls sollten die Nutzer auf das Risiko aufmerksam gemacht werden, das sie eingehen, wenn sie an News-Diensten, chat-Räumen oder „social networking"-Angeboten unter ihrer echten E-mail-Adresse oder sogar ihrem wirklichen Namen teilnehmen.

Die Nutzer sollten die Möglichkeit haben, die Nutzung ihrer Daten auf bestimmte Zwecke zu beschränken. Sie sollten darüber hinaus in die Lage versetzt werden, ihre eigenen Informationen im Netz (oder Teile davon) gegen die Überwachung durch Suchmaschinen zu schützen. Dies kann zum Beispiel durch das Setzen einer „no-robots"-Option für eine Website erreicht werden. Allerdings setzt die Wirksamkeit dieser Einrichtung voraus, daß sie von den Anbietern von Suchmaschinen beachtet wird.

Anbieter von Suchmaschinen sollten die Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung ihrer Dienste informieren.

Sie sollten darüber hinaus den Betroffenen ein Mittel zur Verfügung stellen, um ihre Daten aus (veralteten) möglicherweise bei den Anbietern gespeicherten Kopien von Seiten löschen zu lassen („cache").

Im Hinblick auf die Sensibilität der Spuren, die Betroffene bei der Nutzung von Suchmaschinen hinterlassen, sollten Betreiber von Suchmaschinen ihre Dienste in datenschutzfreundlicher Weise anbieten. Insbesondere sollten sie keine Informationen über Suchvorgänge, die mit einzelnen Nutzern in Verbindung gebracht werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende einer Suchmaschinen-Sitzung sollten keine Daten gespeichert bleiben, die mit einem einzelnen Nutzer in Verbindung gebracht werden können, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung zur Speicherung von zur Erbringung eines Dienstes erforderlichen Daten gegeben.

Der Minimierung von Daten kommt in jedem Fall eine Schlüsselposition zu. Eine solche Praxis wäre auch im Interesse der Anbieter von Suchmaschinen, die zunehmend mit Forderungen Dritter nach nutzerspezifischen Informationen umgehen müssen.

Zum Schutz der Privatsphäre der Benutzer ist der umfassende Einsatz von datenschutzfreundlichen Technologien erforderlich, wo dies möglich ist.

2. 40. Sitzung am 5./6. September 2006 in Berlin

Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP)

– Übersetzung –

Das Angebot von Telefondiensten über das Internet (Internet-Telefonie oder „Voice over IP" – VoIP) ist auf dem Vormarsch. Bereits jetzt sind auf DSL oder anderen Breitbandverbindungen basierende Dienste erhältlich, die eine Ersetzung der Festnetztelefonleitungen ermöglichen. Auch haben Anbieter von „traditionellen" Telefondiensten bereits damit begonnen, Dienste unter Nutzung des VoIP-Protokolls anzubieten. Gleichzeitig sind mobile Geräte erhältlich, die es erlauben, Telefonanrufe über das Internet auch in einem mobilen Umfeld abzuwickeln. Diese Entwicklung steht erst noch am Anfang, und weitere Veränderungen in der Telefonlandschaft sind in der näheren Zukunft zu erwarten.

Die Einführung von VoIP-Diensten auf dem Massenmarkt geht einher mit Risiken für die Sicherheit und die Privatsphäre der Benutzer, die in angemessener Weise in einem frühen Stadium angepackt werden müssen.

Die Einführung von VoIP stellt Herausforderungen an die existierenden nationalen und regionalen Regulierungssysteme. Z. B. könnten Anbieter von VoIP-Diensten nicht durch die nationale Gesetzgebung verpflichtet sein, das Telekommunikationsgeheimnis zu wahren, ein Grundrecht, das in vielen nationalen Verfassungen wie auch in internationalen Regulierungsinstrumenten niedergelegt ist.

Viele nationale Regulierungssysteme enthalten gleichfalls Regelungen, die die Verarbeitung von Verkehrsdaten begrenzen, und zwar normalerweise auf Abrechnungszwecke. VoIP-Dienste könnten im Gegensatz dazu mehr personenbezogene Daten verarbeiten, als es für Abrechnungszwecke erforderlich ist (z. B. Daten über ankommende Gespräche), ohne dass der Nutzer sich dessen bewusst ist oder die Möglichkeit hat, solche Verarbeitungen zu begrenzen.

Die Herausforderungen, die die Einführung der Internet-Telefonie für das Telekommunikationsgeheimnis mit sich bringt, dürfen nicht unterschätzt werden[1]: VoIP-Telefone sind technisch gesehen Computer, die mit dem Internet verbunden sind. Als solche sind sie Ziel von Angriffen jeder Art, die alltäglich im Internet

[1] Eine im Jahr 2005 vom Deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in Auftrag gegebene Studie kam zu dem Ergebnis, dass VoIP-Systeme die Sicherheitsrisiken der IP-Welt erben und darüber hinaus die meisten aus der TK-Welt behalten;
vgl. http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf, S. 134.

stattfinden. Die verschiedenen Protokolle (z. B. das weithin genutzte SIP-Protokoll) implementieren ebenfalls bestimmte datenschutzbezogene Funktionen in verschiedener Weise. So kann z. B. die Unterdrückung der Rufnummer des Angerufenen für Gespräche zwischen VoIP-Telefonen nicht verfügbar seien.

Der Inhalt von Nachrichten in VoIP-Diensten wird über ein Netzwerk von im Vergleich mit dem Festnetz relativ unsicheren Knoten geleitet und damit verwundbar für mögliche Attacken einer potenziell großen Anzahl anderer Nutzer. Es ist daher von großer Bedeutung, sowohl Steuerungsinformationen als auch den Inhalt der übertragenen Nachrichten zu verschlüsseln. Da auch verschlüsselte Nachrichten aufgezeichnet und zu einem späteren Zeitpunkt decodiert werden können, ist eine hinreichend sichere Verschlüsselungsmethode erforderlich.

Die Sicherheit kann auch gefährdet sein, wenn VoIP-Technologien innerhalb eines Unternehmens oder einer Einrichtung der öffentlichen Verwaltung als Ersatz für konventionelle Nebenstellenanlagen eingesetzt wird. Sicherheitsaspekte müssen in Betracht gezogen werden, wenn VoIP-Technologie eingeführt wird.

Das Fernmeldegeheimnis hat seit der Gründung der Arbeitsgruppe im Mittelpunkt ihrer Tätigkeit gestanden[2]. Das Prinzip der Vertraulichkeit von Telefongesprächen wird in den Verfassungsdokumenten vieler Länder garantiert. Bei jeder Verarbeitung personenbezogener Daten müssen angemessene Maßnahmen für die Netzwerke und Server getroffen werden, die zur Erbringung von VoIP-Diensten genutzt werden, um die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der übertragenen Daten zu garantieren[3].

Im Lichte des oben Gesagten gibt die Arbeitsgruppe die folgenden Empfehlungen:

Die Regulierer sind aufgefordert, innerhalb des anwendbaren Regulierungsrahmens wie auch bei der Verhandlung zu internationalen Übereinkommen sicherzustellen, dass Anbieter von VoIP-Diensten verpflichtet werden, mindestens den selben Grad von Sicherheit und Schutz der Privatsphäre sicherzustellen, wie Anbieter traditioneller Festnetz- und Mobiltelefondienste[4].

---

2 Vgl. den Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 14. Konferenz, 29. Oktober 1992, Sydney <http://www.datenschutz-berlin.de/doc/int/iwgdpt/fernm_de.htm>

3 Vgl. den gemeinsamen Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilateraler Abkommen zum Datenschutz – 10 Gebote zum Schutz der Privatheit im Internet, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000 in Berlin <http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_de.htm>

4 VoIP-Datenschutzstandards sollten nicht an ein Mindestmaß von Datenschutzerwartungen in der Telefonie gebunden sein. Obwohl Einrichtungen zum Datenschutz in traditionellen Telefondiensten als unvollständige Beispiele wünschbarer Einrichtungen dienen können, sollten VoIP-Systeme unter der Maßgabe entwickelt werden, welche Einrichtungen am besten die Privatsphäre schützen können, egal ob diese in traditionellen Telefonnetzen implementiert worden sind oder nicht.

VoIP-Anbieter und Hersteller von diesbezüglicher Hard- und/oder Software sind aufgefordert,

1. ihre Kunden über Risiken für die Sicherheit und die Privatsphäre von VoIP-Diensten[5] und möglichen Abhilfen zu informieren[6],

2. angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzfreundliche Nutzung von VoIP-Diensten zu gewährleisten,

3. interoperable Ende-zu-Ende-Verschlüsselungseinrichtungen als ein Standardmerkmal ihrer Dienste ohne zusätzliche Kosten anzubieten,

4. sicherzustellen, dass Sicherheits- und Datenschutzmerkmale ihrer Produkte standardmäßig aktiviert sind,

5. sich bemühen, zügig jegliche Sicherheits- oder Datenschutzlücken aus den Protokollen und der genutzten Hard- und/oder Software zu eliminieren[7],

6. Offene Standards zu nutzen und ihre Nutzer und die breite Öffentlichkeit über die genutzten Protokolle und/oder Produkte zu informieren,

7. den Umfang der standardmäßig gespeicherten und verarbeiteten personenbezogenen Daten (z. B. Verkehrsdaten) auf das Maß zu begrenzen, das für die Erbringung und Abrechnung (soweit erforderlich) eines Dienstes nötig ist, falls nicht zusätzliche Speicherungen und Verarbeitungen von Daten ausdrücklich gesetzlich vorgeschrieben sind,

8. datenschutzrelevante Merkmale wenigstens in der selben Art wie im Festnetz anzubieten(z. B. die Unterdrückung der Anzeige der Rufnummer des Anrufers beim Angerufenen)[8],

9. keine Daten über die Erreichbarkeit eines Nutzers oder seinen physischen Aufenthaltsorts zu speichern, außer zur Erbringung von Notrufdiensten oder,

---

5 Unter anderem sollten VoIP-Anbieter ihre Nutzer informieren, wenn deren persönliche Informationen verloren gegangen sind, gestohlen wurden oder auf sie durch unauthorisierte Parteien zugriffen worden ist, während sie im Besitz des Diensteanbieters waren.

6 Im Fall des Angebots von VoIP über WLAN-Dienste sollte dies Information über Risiken und deren Beseitigung für WLAN-Technologie einschließen, vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen (14. – 15. April 2004, Buenos Aires);
<http://www.datenschutz-berlin.de/doc/int/iwgdpt/1_de.pdf>

7 Dies könnte eine Erweiterung oder Veränderung der genutzten Protokolle (z. B. des SIP-Protokolls) um eine Kontrolle des Nutzers über die übertragene Protokollinformation und deren Anzeige auf Einrichtungen des Angerufenen und des Anrufers einschließen.

8 Vgl. oben Fußnote 4 oben

soweit die Daten in anonymer Form gespeichert werden, zur Verbesserung der Servicequalität. Solche Informationen sollten nicht länger gespeichert werden, als es für diese Zwecke erforderlich ist, und sie sollten auch nur für diese Zwecke zugänglich sein. Diese Information sollte anderen Kunden – einschließlich anderen Teilnehmern irgendeines Kommunikationsvorganges – nicht angezeigt werden, soweit nicht der Betroffene willentlich und ausdrücklich eine entsprechende Wahl getroffen hat. Ein Nutzer sollte in der Lage sein, auszuwählen, welche anderen Nutzer (wenn überhaupt) seine Verfügbarkeits- und Aufenthaltsinformationen sehen können. Verfügbarkeits- und Aufenthaltsinformationen sollten nicht verkauft oder für gezielte Werbung genutzt werden, soweit der Nutzer darin nicht ausdrücklich eingewilligt hat.

10. die Möglichkeit aufrecht erhalten, Telekommunikationsnetze durch öffentliche Zugangspunkte in anonymer Weise zu nutzen.

Arbeitspapier

Trusted Computing, damit zusammenhängende Technologien zur digitalen Rechteverwaltung, und die Privatsphäre: Einige Fragestellungen für Regierungen und Softwareentwickler

– Übersetzung –

Trusted Computing und die damit zusammenhängenden Technologien zur digitalen Rechteverwaltung (TC/DRM) können für die Privatsphäre viele Vorteile bringen. Verbesserte Sicherheit von Systemen, in denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, ist ein lobenswertes Ziel. Jedoch ist eine informierte und verantwortungsvolle Implementierung dieser komplexen Technologien notwendig, um unabsichtliche Risiken für die Privatsphäre zu vermeiden[1].

Den Mittelpunkt der Datenschutzrisiken bildet die Einrichtung zur „Fernattestierung" („remote attestation"), einschließlich des Potenzials für einen langfristigen Mangel an Kontrolle über die Dokumente einer Organisation. So besteht z. B. eine der identifizierten Probleme in der Beeinträchtigung des Rechts eines Individuums, über seine bei einer Behörde gespeicherten personenbezogenen Daten

[1] Vgl. den gemeinsamen Standpunkt der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation „Datenschutz und Urheberrechts-Management", angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000; http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_de.htm

Auskunft zu erhalten, wenn die Zugriffsrechte auf das Dokument, das diese personenbezogenen Informationen enthält, abgelaufen sind.

Spezielle Bedingungen können für Regierungen bei der Implementierung von TC/DRM-Technologien wegen ihrer gesetzlichen Verpflichtungen bestehen, die eine Archivierung vorsehen. Aus diesem Gründe sind die folgenden Empfehlungen überwiegend, aber nicht ausschließlich an öffentliche Stellen gerichtet. Organisationen des Privatsektors werden in den meisten Fällen ähnliche, möglicherweise sogar gesetzlich festgelegte Verantwortlichkeiten haben.

Empfehlungen

Die Arbeitsgruppe empfiehlt, dass Regierungen die potenziellen Gefährdungen für den Datenschutz und die Langzeit-Aufbewahrung von Daten öffentlicher Stellen erwägen, die aus der unbedachten Implementierung solcher Technologien resultieren könnten. Eine Zusammenarbeit mit anderen Regierungen bei Verhandlungen mit Verkäufern (z. B. Ausschreibungen) könnte der effektivste Weg sein, diesen potenziellen Gefahren zu begegnen.

Regierungen sollten Regelungen etablieren, um sicherzustellen, dass die Vorteile der von TC/DRM-Technologien in Bezug auf Daten der Regierung nicht von unbeabsichtigten, die Privatsphäre beeinträchtigenden Effekten überwogen werden.

Regierungen sollten die Übernahmen oder Anpassung der von Neuseeland[2] entwickelten Prinzipien und Regelungen erwägen, die nachfolgend zusammengefasst sind:

Regierungen sollten TC/DRM-Technologien nicht in einer Weise implementieren, die

1. das Recht des Einzelnen auf Auskunft gefährden könnte, oder

2. die Vertraulichkeit und Integrität von Datenbeständen der öffentlichen Verwaltung gefährden könnte, oder

3. den Schutz personenbezogener Informationen gefährden könnte, oder

4. die Sicherheit von Informationssystemen der öffentlichen Verwaltung gefährden könnte.

[2] New Zealand State Services Commission: Trusted Computing and Digital Rights Management Principles and Policies, Version 1.0, 25. September 2006.

Die Arbeitsgruppe empfiehlt Software-Entwicklern und Verkäufern von TC/DRM-Produkten und ermutigt sie dazu, sich der Herausforderung, der sich Regierungen bei der Einführung und Implementierung von „Trusted Computing“ und digitaler Rechteverwaltung gegenüber sehen könnten, bewusst zu werden. Einige dieser Probleme mögen von denen der geschäftlichen Nutzer von TC/DRM abweichen, viele von gleicher Natur sein werden. Anbieter sollten sicherstellen, dass sie in der Lage sind, Anforderungen der Regierung im Hinblick auf die Transparenz der Anwendung dieser Systeme und Anwendungen zu entsprechen.

Anbieter könnten häufig vorfinden, dass Regierungen volle Kenntnis und Zustimmung brauchen werden zu:

1. externen Behinderungen im Hinblick auf Datensätze,

2. Datenflüssen, insbesondere solchen, die mit der Erhebung personenbezogener Daten einhergehen,

3. Übermittlungen außerhalb von Regierungssystemen (einschließlich Attestierung und anderen Hintergrundübermittlungen),

4. Regelungen, die den Zugriff auf Informationen öffentlicher Stellen kontrollieren und erlauben, und

5. Datensicherheitsrisiken im Zusammenhang mit schädlichen Inhalten wie z B. Viren und jeglichen anderen Einflüsse auf die Datensicherheit.

Anbieter sollten darauf vorbereitet sein, Regierungen unabhängige Bestätigungen darüber vorzulegen, dass ihre Systeme in der Weise funktionieren, wie es in der Spezifikation beschrieben ist.

B Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließung der 12. Konferenz am 26. Juni 2006 in Bonn

Verbraucherinformationsgesetz nachbessern

Die Informationsfreiheitsgesetze im Bund und in einigen Ländern stellen einen wichtigen Beitrag zu mehr Transparenz, Bürgerbeteiligung und gesellschaftlicher Offenheit dar. Folgerichtig bedarf es auch einer größeren Transparenz im Bereich des Verbraucherschutzes. Unter bestimmten Voraussetzungen sollte ein unmittelbarer Informationsanspruch gegen private Unternehmen gesetzlich verankert werden. Auch Daten, die in Unternehmen gespeichert werden, berühren unmittelbar Rechte der Bürgerinnen und Bürger und damit ihr Lebensumfeld. Dies gilt insbesondere bei verbraucherschutzrelevanten Produkten sowie Produkten des Energiemarktes. Die Transparenzrechte der Bürgerinnen und Bürger sollten deshalb in diesem Bereich ebenfalls durch Auskunftsansprüche gesetzlich geregelt werden.

Der Entwurf des Verbraucherinformationsgesetzes, der derzeit im Deutschen Bundestag beraten wird, schafft aber nur unzureichende Transparenzregelungen, die außerdem die Unternehmen nicht ausreichend zur Offenlegung der verbraucherschutzrelevanten Daten verpflichten. Die Informationsfreiheitsbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Verbraucherinformationsschutzgesetz erste Schritte für mehr Transparenz in der Wirtschaft umzusetzen.

Dazu gehören zumindest folgende Verbesserungen:

- die Erweiterung des Gesetzes über Lebens- und Futtermittel hinaus auf sonstige Produkte und Dienstleistungen,

- die Schaffung eines unmittelbaren Rechtsanspruchs auf Informationszugang gegenüber Unternehmen,

- die Schaffung einer Abwägungsregelung zwischen den unterschiedlichen Interessen, die unter Beachtung der tatsächlichen Betriebs- und Geschäftsgeheimnisse der Unternehmen den Betroffenen den Informationsanspruch sichert; amtlich festgestellte Verstöße der Unternehmen gegen verbraucher-

schutzrelevante Regelungen dürfen dabei nicht als Betriebs- und Geschäftsgeheimnis geltend gemacht werden,

- die Reduzierung der Ausnahmen vom Informationszugang auf wesentliche Ausnahmen und eine verbraucherschutzfreundliche Ausgestaltung des Verfahrens,

- Höchstgrenzen bei der Regelung von Gebühren für die Beauskunftung durch die Betroffenen.

2. Entschließungen der 13. Konferenz am 12. Dezember 2006 in Bonn

Transparenz der Verwaltung im Internet: Eigeninitiative ist gefragt!

Auf Bundesebene sowie in acht Bundesländern gibt es mittlerweile Informationsfreiheitsgesetze, die allen Interessierten die Einsicht in Behördenakten ermöglichen. Wer von diesem Recht Gebrauch machen möchte, steht erst einmal vor der Frage, welche Akten in den Ämtern überhaupt geführt werden. Der Blick auf die Internet-Seiten der einzelnen Behörden hilft dabei nur selten weiter. Übersichtliche Darstellungen des Aktenbestands? Inhaltlich aussagekräftige Dokumente, die über offizielle Verlautbarungen hinausgehen? Leider häufig Fehlanzeige!

Die Praxis in Großbritannien, Slowenien und den Vereinigten Staaten von Amerika zeigt, dass eine andere Herangehensweise durchaus Erfolg verspricht. Dort sind alle Behörden per Gesetz verpflichtet, eine spezielle Website zur Informationsfreiheit anzubieten. Auf dieser Seite informieren sie nicht nur über die Rechtslage zur Akteneinsicht, über die behördlichen Ansprechpersonen und den eigenen Informationsbestand, sondern halten auch einen virtuellen Lesesaal bereit. Dort müssen Dokumente, die bereits mehrfach zur Einsicht beantragt wurden und Daten von allgemeinem Interesse eingestellt werden. Seit Einführung dieser Regelung geht die Anzahl der Anfragen nach Akteneinsicht bei den Behörden deutlich zurück.

Einige Informationsfreiheitsgesetze sehen die Veröffentlichung bestimmter Dokumente bzw. die Meldung an ein zentrales elektronisches Informationsregister für öffentliche Stellen bereits jetzt zwingend vor. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland empfiehlt den Akten führenden Stellen deshalb, ihre Tätigkeit gegenüber der Öffentlichkeit im Internet transparenter zu machen. Damit wird auf der einen Seite den Bürgerinnen und Bürgern der Informationszugang erleichtert und gleichzeitig der Verwaltungsaufwand der öffentlichen Stellen reduziert.

1. Die Veröffentlichung von Organigrammen, Geschäftsverteilungsplänen und Listen mit Ansprechpersonen gehört bereits zum Standard. Darüber hinaus sollten vorhandene Aktenpläne und -verzeichnisse ebenfalls im Internet veröffentlicht werden, damit leichter zu erkennen ist, welche Kategorien von Akten überhaupt geführt werden.

2. Gerade bei größeren Behörden ist der Aktenplan allerdings oft so kompliziert, dass bereits seine interne Verwendung auf Schwierigkeiten stößt. Sinnvoll ist die Veröffentlichung in einem solchen Fall nur, wenn der Aktenplan erläutert oder vereinfacht dargestellt wird. Niemand wird sich freiwillig durch ein hundertseitiges Verzeichnis quälen. Handhabbare Findmittel sind somit Voraussetzung für die Wahrnehmung des Rechts auf Informationszugang.

3. Die meisten öffentlichen Stellen verfügen über Dokumente, die von allgemeinem Interesse sind und ohne weiteres eingesehen werden können. Grundsätzlich gilt: Stehen einem Informationszugang keine Ausnahmegründe entgegen, können die Dokumente im Regelfall auch ins Netz gestellt werden. Viele Kommunen stellen so bereits jetzt die Protokolle öffentlicher Sitzungen ihrer Vertretungen zur Verfügung. Einmal eingestellt, kann jede Person darauf zugreifen. Der Aufwand zur Bearbeitung von Anträgen auf Informationszugang entfällt.

4. Ein Indikator dafür, welche Informationen von allgemeinem Interesse sind, könnte das Kriterium sein, dass ein Dokument bereits zur Einsicht beantragt wurde. Soweit die Behörde diesem Antrag stattgegeben hat, kann das Dokument automatisch ins Netz gestellt werden, um Informationswünsche Anderer zu erfüllen und den Verwaltungsaufwand mit künftigen Anträgen zu vermeiden.

5. Was bedeutet Informationsfreiheit? Wie stellt man einen Antrag auf Akteneinsicht? Und welche Erfolgsaussichten hätte ein solches Begehren? Um solche Fragen zu beantworten, könnte ein Leitfaden oder die Beantwortung häufig gestellter Fragen (FAQ) auf den Seiten der einzelnen Behörden zur Klärung beitragen.

In der Bundesrepublik setzt die Bundesagentur für Arbeit auf diesem Gebiet erste Maßstäbe, indem sie ehemals „interne“ Weisungen und Dokumente nun im Internet veröffentlicht. Die Bürgerinnen und Bürgern können dadurch behördliche Handlungen besser nachvollziehen und ihr Mitspracherecht leichter wahrnehmen.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder stehen Verwaltungen, die ihr Informationsangebot verbessern möchten, jederzeit gerne für eine Beratung zur Verfügung.

Verbraucherinformation unverzüglich regeln

Das Verbraucherinformationsgesetz ist vorerst gescheitert. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland bedauert, dass dieses Anliegen damit zunächst ungeregelt bleibt. Das verfolgte Ziel, als Konsequenz aus den Lebensmittelskandalen der letzten Zeit die Informationsansprüche der Verbraucherinnen und Verbraucher zu stärken und mehr Transparenz zu schaffen, ist aber aktueller denn je und bedarf weiterhin dringend einer möglichst umfassenden Regelung. Bund und Länder sind deswegen aufgefordert, dieses für einen wirksamen Verbraucherschutz so wichtige Anliegen mit Nachdruck weiterzuverfolgen und gegebenenfalls auch auf Landesebene umzusetzen.