Dokumente zum Datenschutz

1998

Impressum

Herausgeber:

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg

Stahnsdorfer Damm 77, Haus 2
14532 Kleinmachnow
Telefon: 03 32 03 / 35 60
Telefax: 03 32 03 / 3 56 49
E-Mail: Poststelle@LDA.Brandenburg.de
Internet: http://www.lda.brandenburg.de

Berliner Datenschutzbeauftragter

Pallasstraße 25/26
10781 Berlin
Telefon: 0 30 / 78 76 88 44
Telefax: 0 30 / 2 16 99 27
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Redaktion, Layout: Volker Brozio, Laima Nicolaus

Druck: Verwaltungsdruckerei Berlin

1. Auflage: März 1999

Inhaltsverzeichnis

Vorwort

Die Kontrolle des Datenschutzes in Deutschland ist gekennzeichnet durch eine außerordentliche Aufspaltung der Zuständigkeiten: Neben dem Bundesbeauftragten für den Datenschutz, der seine Aufgaben gegenüber Bundesgesetzgeber und -behörden wahrnimmt, gibt es für die Landesverwaltungen die Landesbeauftragten für den Datenschutz sowie für den privaten Bereich die Aufsichtsbehörden für den Datenschutz. Trotz dieser Aufsplitterung ist ein effektiver Datenschutz nur dann gesichert, wenn die beteiligten Gremien ihre Arbeit koordinieren; dies ist auch deswegen erforderlich, weil die geringe Ausstattung der Datenschutzbehörden eine Spezialisierung und eine dadurch mögliche Aufgabenverteilung erzwingen. Seit die ersten Dienststellen des Bundes und einiger Landesdatenschutzbeauftragter Ende der 70er Jahre eingerichtet sind, bietet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Forum für die Koordination des Datenschutzes im öffentlichen Bereich. In einer Vielzahl von Beschlüssen und Entschließungen haben sie zur datenschutzgerechten Fortentwicklung der Gesetzgebung, der bürgerfreundlichen Auslegung der bestehenden Gesetze sowie der technisch-organisatorischen Umsetzung des Datenschutzes beigetragen.

Immer mehr Bedeutung gewinnt vor dem Hintergrund der Europäischen Datenschutzrichtlinie und weiterer europarechtlicher Normen mit datenschutzrechtlichem Gehalt auch die Koordination der europäischen Datenschutzbehörden untereinander sowie mit den zuständigen Stellen der Europäischen Kommission. Insbesondere in der aufgrund von Art. 29 der Europäischen Datenschutzrichtlinie gegründeten Gruppe werden Dokumente erarbeitet, die für die Arbeit der nationalen Datenschutzstellen von grundlegender Bedeutung sind.

Schließlich gibt es darüber hinaus weltweite Bemühungen, insbesondere auf dem Gebiet der neuen Techniken wie Internet zu einheitlichen Lösungen zu kommen.

Die Ergebnisse all dieser Koordinierungsgremien werden üblicherweise in den Jahresberichten der Datenschutzbeauftragten abgedruckt, so auch in den Tätigkeitsberichten des Brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie des Berliner Datenschutzbeauftragten. Um den hohen Aufwand mit der parallelen Veröffentlichung der gleichen Texte zu vermindern, haben der Brandenburgische Landesbeauftragte sowie der Berliner Datenschutzbeauftragte beschlossen, künftig diese Texte in einen gemeinsamen Anlagenband aufzunehmen, der gleichzeitig mit dem Tätigkeits- bzw. Jahresbericht erscheint. Diese Form der Veröffentlichung hat zudem den Vorteil, dass eine fortlaufende, von den Berichten getrennte Dokumentation entsteht.

Die gemeinsame Veröffentlichung soll zudem ein Zeichen dafür sein, dass es auch in den weiterhin getrennten Ländern Brandenburg und Berlin Möglichkeiten der Zusammenarbeit gibt, die die Effizienz beider Seiten steigern können.

Dr. Alexander Dix

Prof. Dr. Hansjürgen Garstka

A. Forderungen für einen Politikwechsel zum wirksameren Schutz der Privatsphäre

Datenschutzbeauftragte appellieren an die neue Bundesregierung:

10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre

Die Datenschutzbeauftragten Berlins, Brandenburgs, Bremens, Nordrhein-Westfalens und Schleswig-Holsteins fordern einen Politikwechsel zum Schutz der Privatsphäre.

Deutschland befindet sich auf dem Weg in die Informationsgesellschaft. Niemand kann zuverlässig abschätzen, welche Veränderungen sich aus dieser Entwicklung für Staat und Gesellschaft und für nahezu alle Lebensbereiche der Bürgerinnen und Bürger ergeben. Sicher ist aber, dass ohne Garantien für Datenschutz und Datensicherheit die Informationsgesellschaft nicht zu verantworten ist. Eine Informationsverarbeitung, bei der die Bürgerinnen und Bürger nicht mehr wissen, an welcher Stelle welche Daten über sie gesammelt werden, beeinträchtigt nicht nur ihre eigenen Rechte, sondern ist auch mit dem demokratischen Rechtsstaat unvereinbar.

1. Grundrecht auf Datenschutz

Es ist an der Zeit, das Recht auf informationelle Selbstbestimmung als ausdrückliches Grundrecht auch im Grundgesetz zu verankern. Grundrechte reflektieren das Schutzbedürfnis der Menschen im jeweiligen historischen Zusammenhang.

Unter den Bedingungen der Informationsgesellschaft erlangt der Schutz der Privatsphäre jedes einzelnen Menschen hohe Priorität. Das Grundgesetz sollte sich dazu umso mehr ausdrücklich bekennen, als durch die verfassungsrechtliche Zulassung des Großen Lauschangriffs empfindliche Einschränkungen der Privatsphäre vorgenommen wurden.

FORDERUNG:

In das Grundgesetz ist ein Grundrecht auf Datenschutz aufzunehmen.

2. Datensicherheit

Fragen der Datensicherheit werden in Deutschland bislang vernachlässigt. Das derzeitige Datenschutzrecht verlangt lediglich „angemessene" Datensicherheitsmaßnahmen. Dies genügt nicht. Ohne wirksame Umsetzung auf der technischen Ebene nützen allerdings auch die besten Datenschutzbestimmungen nichts. Die Verhältnisse im Internet zeigen, dass bei der Datensicherheit Nachholbedarf besteht. Auch die Ungewissheit bezüglich des Verhaltens der Computer beim Jahrtausendwechsel am 1. Januar 2000 legen es nahe, Fragen der Ordnungsmäßigkeit der Datenverarbeitung künftig ein anderes Gewicht zu geben. Die Umstellung der Programme auf den Jahrtausendwechsel kostet jetzt Milliarden.

Nicht nur die Interessen der Systembetreiber, sondern auch die der Bürgerinnen und Bürger als Nutzer und Kunden müssen künftig angemessen im Rahmen so genannter „mehrseitiger Sicherheit" berücksichtigt werden.

FORDERUNG:

Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung müssen eine höhere Priorität erhalten.

3. Verschlüsselung

Die Nutzung offener Netze für geschäftliche oder persönliche Zwecke steht und fällt mit der Möglichkeit, die Vertraulichkeit und Unverfälschtheit der ausgetauschten Informationen zu garantieren. Das wichtigste Instrument dazu sind starke Verschlüsselungsverfahren. Die staatliche Politik sollte auf eine Förderung dieser Technik und ihre Verfügbarkeit für jeden einzelnen Bürger gerichtet sein. Überlegungen, das Recht zur Verschlüsselung zugunsten der Sicherheitsbehörden einzuschränken, gehen schon deswegen fehl, weil derartige Regelungen technisch – etwa durch Doppelverschlüsselung oder Steganographie – leicht umgangen werden können. Die Vorstellung, jede elektronische Kommunikation müsse vom Staat überwachbar sein, ist unter den Bedingungen des Internet illusorisch.

FORDERUNG:

Wirksame Verschlüsselungsverfahren müssen gefördert werden; Überlegungen, das Recht auf Kryptographie zu beschränken, müssen eingestellt werden.

4. Modernisierung der Datenschutzgesetze

Die bisherige Datenschutzgesetzgebung muss überprüft und neu gewichtet werden. Das Bundes- und die Landesdatenschutzgesetze basieren auf der Großrechnertechnologie und berücksichtigen nicht die neuen technischen Gegebenheiten. Die ohnehin überfällige Anpassung der Gesetze an die Europäische Datenschutzrichtlinie muss zur umfassenden Modernisierung genutzt werden. Dabei spielen Stichworte wie Verschlankung, Datenschutz durch Technik, Datenschutzaudit, Förderung von Selbstdatenschutz, Datenvermeidung, Anonymisierung und Pseudonymisierung eine entscheidende Rolle.

FORDERUNG:

Die Datenschutzgesetze müssen gründlich modernisiert und effektiviert werden.

5. Bereichsspezifisches Datenschutzrecht

Die bereichsspezifische Datenschutzgesetzgebung kann in der bisherigen Form nicht fortgeführt werden. Es nützt den Bürgerinnen und Bürgern wenig, wenn die Fachgesetze durch immer mehr Vorschriften aufgebläht, zugleich aber in ihrer datenschutzrechtlichen Substanz ausgehöhlt werden.

Jüngstes Beispiel ist die Änderung des Sozialgesetzbuches X, bei der – ohne dass der Sozialdatenschutz in seinem äußeren Zuschnitt verändert wurde – die Sozialbehörden quasi zu Außenstellen der Polizei gemacht wurden. Ähnlich wurde das Ausländerzentralregister als Informationsdrehscheibe und Fahndungsregister für alle deutschen Behörden ausgestaltet. In Zukunft muss im bereichsspezifischen Recht Quali-

tät vor Quantität gehen. Es ist ein Wesensmerkmal des Datenschutzes und des daraus abgeleiteten Zweckbindungsprinzips, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass das, was sie einer Behörde mitteilen, nicht automatisch an alle anderen Behörden weitergegeben werden darf.

FORDERUNG:

Die bereichsspezifische Datenschutzgesetzgebung muss substantielle Rechtsgarantien gewährleisten.

6. Sicherheitsbereich

Im Sicherheitsbereich ist in den vergangenen Jahren bei der Abwägung zwischen Datenschutz und Sicherheitsinteressen fast stets zugunsten letzterer entschieden worden. Die Sicherheitsbehörden verfügen inzwischen über eine derartige Fülle von Befugnissen, dass es schwer geworden ist, den Überblick zu bewahren. Viele rechtsstaatlich problematische, auf die Terrorismusfahndung zugeschnittene Instrumente können jetzt ohne Sicherheitsverlust zurückgenommen werden.

Generell ist bei sensiblen Eingriffsbefugnissen ein Evaluierungsmechanismus einzuführen, der es dem Parlament ermöglicht, nach einer angemessenen Frist die Erforderlichkeit der Eingriffsbefugnisse anhand objektiver Kriterien zu überprüfen.

FORDERUNG:

Die besonders sensiblen Eingriffsbefugnisse im Sicherheitsbereich müssen systematisch auf ihre Effektivität und ihre Grundrechtsverträglichkeit untersucht werden.

Sonderbefugnisse aus der Terrorismusfahndung müssen zurückgenommen werden.

7. Verwaltungsmodernisierung

In nahezu allen Bereichen der Verwaltung laufen umfangreiche Modernisierungsbestrebungen. Häufig sehen sie auch die Straffung der Abläufe, Privatisierung der Aufgabenerfüllung oder jedenfalls zunehmende Einschaltung externer Dienstleister vor. Gegen eine Effektivierung der Verwaltung ist nichts einzuwenden. Wer sie aber nur unter den Aspekten der Beschleunigung und Kosteneinsparung betreibt, wird schnell entdecken, dass rechtsstaatliche Verfahrensgarantien nicht zum Nulltarif zu haben sind.

Verwaltungsleistungen unterscheiden sich von privaten Dienstleistungen wesentlich dadurch, dass sie nicht nur unter marktwirtschaftlichen, sondern gerade unter rechtsstaatlichen Gesichtspunkten erbracht werden. Dazu gehört die Gewährleistung des Datenschutzes. Solange das Datenschutzniveau im Bereich der Privatwirtschaft deutlich niedriger als in der öffentlichen Verwaltung ist, verschlechtert die Privatisierung von Verwaltungsleistungen die Rechtsposition der Bürgerinnen und Bürger.

FORDERUNG:

Datenschutz darf nicht einer rigorosen Verwaltungsmodernisierung zum Opfer fallen.

8. Informationszugang

In der Informationsgesellschaft kommt der Verfügung über die Informationsressourcen herausragende Bedeutung zu. Deshalb gewinnen Informationszugangsrechte in einer demokratischen Gesellschaft immer mehr Gewicht. Nur wenn die Bürgerinnen und Bürger das Recht auf Zugang zu Informationen bei öffentlichen Stellen erhalten,

können sie ihr Gemeinwesen wirksam gestalten. Deutschland kann in dieser Beziehung mit vielen europäischen Nachbarstaaten noch nicht Schritt halten. Auch die Europäische Union hat im Vertrag von Amsterdam allen Bürgerinnen und Bürgern Zugang zu ihren Informationen zugesagt. Es wäre falsch, Datenschutz und Informationszugang gegeneinander ausspielen zu wollen. Beide Prinzipien bedingen und ergänzen einander vielmehr.

FORDERUNG:

Es ist ein allgemeines Informationszugangsrecht einzuführen.

9. Telekommunikation

Das Zusammenwachsen von Computertechnologie und neuen Medien und die zunehmende Allgegenwärtigkeit der Informationstechnik im täglichen Leben führen dazu, dass von den Menschen an den unterschiedlichsten Stellen elektronische Datenspuren hinterlassen werden (Electronic Cash, Nutzung elektronischer Medien, Einsatz von Chipkarten, elektronische Kommunikation). Diese Spuren sind für Sicherheitsbehörden ebenso von Interesse wie für Marketingabteilungen in der Wirtschaft. Die Politik hat die Aufgabe zu verhindern, dass die Bürgerinnen und Bürger durch faktischen Zwang zu gläsernen Menschen werden. Die Multimediagesetzgebung enthält insofern erste Ansätze zur Datenvermeidung. Diese müssen umgesetzt und fortgeschrieben werden. Zugleich hat der Gesetzgeber im Telekommunikationsrecht aufwendige Kontrollinstrumente vorgesehen. So sollen Telekommunikationsanbieter verpflichtet werden, viele Milliarden Mark teure Abhörmöglichkeiten für Sicherheitsbehörden auf eigene Kosten einzurichten, damit jede Nebenstelle abhörbar wird. Der Anspruch der Kontrollierbarkeit jeglicher Telekommunikation kann nicht aufrechterhalten werden.

FORDERUNG:

Das Recht der Bürgerinnen und Bürger auf unüberwachte telekommunikative Selbstbestimmung muss ein zentrales Anliegen der Politik werden.

10. Datenschutz in der Wirtschaft

Neben die Angst vor der Überwachung durch den Staat als „Big Brother“ ist aus guten Gründen die Furcht vor der informationellen Bevormundung durch dessen „Geschwister“ aus der Wirtschaft getreten. Während staatliche Einrichtungen einem relativ strengen Datenschutzregime unterworfen sind, entwickeln sich die privatwirtschaftlich betriebenen personenbezogenen Datenbanken oft fast schon wildwüchsig. Bei Informations-, Finanz- oder sonstigen Dienstleistungsunternehmen oder bei großen Versandhändlern werden Daten über Konsumgewohnheiten, über Bonität und über sonstige, teilweise sehr private Sachverhalte systematisch gesammelt und unter verschiedenen Gesichtspunkten ausgewertet und genutzt. Nicht weniger sensibel sind Datenbanken über Arbeitnehmerinnen und Arbeitnehmer. Das derzeitige Datenschutzrecht gibt den Betroffenen wenig Schutz. Es fehlen konkrete Regelungen und Sanktionen für den Fall des Regelverstoßes. Nicht zuletzt sind die Datenschutzkontrollinstanzen bislang nicht so ausgestattet, dass sie der exponentiell wachsenden Datenverarbeitung in der Wirtschaft gewachsen sind.

FORDERUNG:

Der Datenschutz im privaten Bereich muss rechtlich und organisatorisch ausgebaut werden.

B. Beschlüsse und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Entschließungen der 55. Konferenz am 19./20 März 1998 in Wiesbaden

Datenschutzprobleme der Geldkarte

(Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13. 10. 1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten – sog. White Cards – anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Datenschutz beim digitalen Fernsehen

(Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998)

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fern-

sehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV“ und „Pay TV“) muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;
- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug – etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen – entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

II. Epidemiologie und Datenschutz

Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)

Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Epidemiologie und Datenschutz

(Umlaufbeschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Mai 1998)

Inhaltsübersicht:

Epidemiologie und Datenschutz

Redaktion:

- Wichmann, H. E.;
- Raspe, H. H.;
- Jöckel, K. H.

für die Deutsche Arbeitsgemeinschaft für Epidemiologie;

- Hamm, R.;
- Wellbrock, R.

für den Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Einleitung

Die epidemiologische Forschung zielt nicht auf personenbezogene, sondern auf bevölkerungsbezogene wissenschaftliche Aussagen. Hierbei stützt sie sich jedoch in der Regel auf personenbezogene Daten zum Gesundheitszustand der Probanden, soziodemographische Angaben, Informationen über Risikofaktoren und oftmals medizinische Untersuchungsbefunde und Ergebnisse aus der Analyse biologischer Materialien. Die individuellen Untersuchungsergebnisse werden üblicherweise den Probanden mitgeteilt. Zur Durchführung der Forschungsprojekte werden vielfach Namen und Anschriften zur Kontaktaufnahme benötigt. Darüber hinaus muss eine korrekte Zuordnung von Follow-up-Ergebnissen sowie die Zusammenführung von Daten aus verschiedenen Quellen sichergestellt werden.

Epidemiologie und Datenschutz stehen traditionell im Spannungsfeld des Schutzes der Persönlichkeitsrechte der von der Datenverarbeitung Betroffenen und dem wissenschaftlichen Anliegen, durch das Auswerten von Gesundheitsdaten zu wichtigen und auf andere Weise nicht erreichbaren Kenntnissen zu gelangen.

Im Anschluss an eine Diskussion der datenschutzrechtlichen Fragen zwischen der Deutschen Forschungsgemeinschaft und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben Epidemiologen und Datenschützer versucht, typische Problemfelder zu identifizieren und zu gemeinsamen Lösungsvorschlägen zu kommen. Die folgenden Vorschläge sollen den mit Datenschutzfragen bei epidemiologischen Studien befassten Wissenschaftlern, Datenschützern, Ethikkommissionen, Behörden und Forschungsförderern zur Information und Orientierung dienen, um Probleme zu vermeiden, die durch fehlende Kenntnis der datenschutzrechtlichen Vorschriften, ungeeignet formulierte Einverständniserklärungen oder durch eine falsche oder übervorsichtige Interpretation der Rechtsvorschriften zur Datenübermittlung für Forschungszwecke etc. bedingt sind.

1. Rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten

1.1 Forschung mit anonymisierten Daten

Die datenschutzrechtlichen Bestimmungen finden nur Anwendung, wenn für ein Forschungsprojekt personenbezogene Daten benötigt werden. Forschung mit anonymisierten Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Ob es sich im konkreten Fall um personenbezogene oder um anonymisierte Daten handelt, bedarf allerdings sorgfältiger Prüfung. § 3 Abs. 7 BDSG enthält eine gesetzliche Definition des Anonymisierens. Dieser Definition zufolge ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (sog. „faktische Anonymisierung“). Anonymisierung wird in der wissenschaftlichen bzw. datenschutzrechtlichen Diskussion ganz überwiegend im Sinne einer faktischen Anonymisierung verstanden. Einzelangaben sind z. B. dann keine anonymisierten Daten, wenn beim Forschungs-

institut bzw. beim Forscher lediglich eine organisatorische Trennung der Hilfsmerkmale von den übrigen Daten vorgenommen wurde oder wenn lediglich Name und Adresse der Betroffenen weggelassen wurden und die Betroffenen anhand der weiteren Angaben noch identifizierbar sind. Auch aggregierte Daten können nicht immer als anonymisiert qualifiziert werden. Im Einzelfall muss eine Risikoanalyse unter Berücksichtigung insbesondere des eventuellen Wertes der in Frage stehenden Daten für potentielle Interessenten sowie der dem Empfänger oder den potentiellen Interessenten zur Verfügung stehenden Ressourcen (Zusatzwissen, technische Möglichkeiten der Datenverarbeitung etc.) durchgeführt werden.

In einigen wenigen Bundesländern wird Anonymisierung im Sinne einer absoluten Anonymisierung verstanden, d.h. Einzelangaben werden nur dann als anonym qualifiziert, wenn sie unter keinen Umständen mehr zuzuordnen sind.

1.2 Forschung mit Einwilligung der Betroffenen

Personenbezogene Daten können im Rahmen der epidemiologischen Forschung auf der Basis einer Einwilligung der Betroffenen verarbeitet werden. Nach den datenschutzrechtlichen Regelungen muss die Einwilligung der Betroffenen bestimmte inhaltliche und formale Voraussetzungen erfüllen, damit sie rechtswirksam ist. Insbesondere müssen die Betroffenen über die vorgesehene Verarbeitung ihrer Daten informiert werden (Träger und Leiter des Forschungsprojekts, Zweck des Forschungsvorhabens, Art und Weise der Datenverarbeitung, Personenkreis, der von den personenbezogenen Daten Kenntnis erhält, Zeitpunkt der Löschung der personenbezogenen Daten etc.), damit sie die Tragweite ihrer Entscheidung erkennen können. Die Einwilligung muss in der Regel schriftlich erteilt werden, die gesetzlichen Regelungen sehen jedoch Ausnahmen vor. Ferner ist ein Hinweis erforderlich, dass die Einwilligung freiwillig ist, aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung möglich ist. Einzelheiten sind den jeweils einschlägigen Regelungen zu entnehmen.

Verfügt die Forschungsstelle nicht über die Namen und Adressen der Personen, bei denen Einwilligungen eingeholt werden sollen, und kann sie sich diese Daten aufgrund der rechtlichen Regelungen (z. B. Meldegesetz) nicht beschaffen, so kann die Forschungsstelle die Betroffenen in der Weise kontaktieren, dass sie ihre Anschreiben, Merkblätter etc. in verschlossenen Umschlägen der Stelle übergibt, die über die Daten verfügt, damit letztere auf die Umschläge Namen und Adressen schreibt und die Anschreiben dann versendet. Auf diese Weise wird vermieden, dass die Daten Dritten zur Kenntnis gelangen. Dabei sollte für die Betroffenen in dem Anschreiben eindeutig erkennbar sein, dass ihre geschützten Daten von der Stelle, die über die Daten verfügt, nicht an die forschende Stelle weitergegeben wurden.

1.3 Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

Das Grundgesetz gewährleistet das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts im Sinne von Artikel 2 i.V.m. Artikel 1 Grundgesetz. Ebenso gewährleistet das Grundgesetz die Freiheit von Wissenschaft und Forschung in Artikel 5 Grundgesetz. Diese beiden Grundrechte können bei Forschungsvorhaben, für die – zumindest vorübergehend – personenbezogene Daten benötigt werden, miteinander in Konflikt geraten. In dieser Situation ist es – wie auch bei anderen Grundrechtskonflikten – in erster Linie Aufgabe des Gesetzgebers, diese potentiellen Konflikte so zu regeln, dass beide Grundrechte möglichst weitgehend realisiert werden können. Der Gesetzgeber muss die rechtlichen Rahmenbedingungen festlegen, unter denen personenbezogene Daten zu Forschungszwecken ohne Einwilligung der Betroffenen verwendet werden dürfen. Dabei sind auch die besonderen Schweigepflichten wie z. B. die ärztliche Schweigepflicht i.S. der Berufsordnung und des § 203 StGB zu beachten. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Einschränkung des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig. Die Verarbeitung personenbezogener Daten muss für den angestrebten Zweck geeignet und notwendig sein und es darf keine Alternative geben, die die Betroffenen weniger belastet (z. B. Anonymisierungs- bzw. Pseudonymisierungsverfahren, Einwilligung der Betroffenen).

Gesetzliche Forschungsregelungen, die das Recht auf informationelle Selbstbestimmung und die Freiheit von Wissenschaft und Forschung in diesem Sinne zuordnen, sind z. B. in Landeskrankenhausgesetzen, Meldegesetzen, im Sozialgesetzbuch X, Krebsregistergesetzen, im Bundesdatenschutzgesetz und in Landesdatenschutzgesetzen enthalten. Entgegen dem allgemeinen Grundsatz der Zweckbindung personenbezogener Daten können nach diesen Regelungen unter bestimmten Voraussetzungen Daten, die zu einem anderen Zweck als wissenschaftlicher Forschung erhoben wurden, zu Forschungszwecken weiterverwendet werden.

2. Forschungsansätze in der Epidemiologie, Datenbedarf und Rechtsgrundlagen der Datenverarbeitung

Die Epidemiologie ist die Lehre von der Verteilung der Krankheiten und ihrer Risikofaktoren in der Bevölkerung. Aussagen epidemiologischer Forschung betreffen nicht das Individuum, sondern eine Bevölkerungsgruppe. Daher werden personenbezogene Daten nur für die Datenerfassung und ggf. spätere Kontaktaufnahmen sowie für die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen benötigt.

Als wichtigste epidemiologische Studientypen sind beispielhaft anzusehen:

- Bei Querschnittserhebungen wird typischerweise einmalig eine Befragung und/oder Untersuchung von Probanden durchgeführt. Diese werden persönlich um ihr Einverständnis gebeten. Die epidemiologische Fragestellung umfasst z. B. die Charakterisierung von Erkrankungshäufigkeiten in der untersuchten Bevölkerungsgruppe oder den Zusammenhang zwischen dem Auftreten von Erkrankungen und Risikofaktoren. Aus datenschutzrechtlicher Sicht sind hier – wie auch bei den anderen Studienformen – die formalen und inhaltlichen Voraussetzungen der Einwilligungserklärung der Betroffenen zu beachten, ferner die jeweils einschlägigen Vorschriften zur Verarbeitung und Nutzung personenbezogener Daten durch die Forschungseinrichtungen (z. B. § 40 BDSG).
- Als zweiter Studientyp ist die Kohortenstudie zu nennen. Hierbei werden – z. B. ausgehend von einer Querschnittstudie – wiederholt Untersuchungen an denselben Probanden durchgeführt. Für diese Follow-up-Untersuchungen ist es erforderlich, personenbezogene Daten zu speichern, Anschriften zu aktualisieren etc. Diese Datenverarbeitung muss von den Einwilligungserklärungen umfasst sein. Als epidemiologische Fragestellungen werden das Auftreten neuer Erkrankungen oder bestimmter Todesursachen im Zusammenhang mit bestimmten Risikofaktoren bearbeitet. Im letzteren Fall ist es zusätzlich erforderlich, über Einwohnermeldeämter und Gesundheitsämter den Vitalstatus sowie im Falle des Ver-

sterbens die Todesursache zu erheben. Als Rechtsgrundlage hierfür kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

- Einen Spezialfall von Kohortenstudien stellen retrospektive Kohortenstudien (mit zurückverlagertem Beginn) dar, die insbesondere im Bereich der Berufsepidemiologie häufig eingesetzt werden. Bei solchen Studien wird typischerweise aufgrund von betrieblichen Unterlagen die Exposition gegenüber bestimmten Arbeitsstoffen am Arbeitsplatz erhoben. Häufig interessiert das Auftreten von Krebserkrankungen oder das Versterben an bestimmten Todesursachen im Zusammenhang mit den beruflichen Expositionen. Hierbei ist es nicht ungewöhnlich, dass die Personen selbst nicht befragt werden, sondern dass ihre Exposition aus den betrieblichen Unterlagen bestimmt wird und die Krebserkrankung oder Todesursache durch Auswertung eines Krebsregisters oder über Einwohnermeldeamt und Gesundheitsamt in Erfahrung gebracht wird. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.
- Als weiterer epidemiologischer Studientyp ist die Fall-Kontroll-Studie zu nennen. Hierbei werden als Fälle Personen mit bestimmten Erkrankungen bezeichnet, die Kontrollpersonen gegenübergestellt werden. Fälle und Kontrollen werden im Hinblick auf in der Vergangenheit liegende Risikofaktoren befragt. Häufig ist es sinnvoll, Fälle aus Registern, z. B. Krebsregistern, einzubeziehen. Als Rechtsgrundlage kommen die gesetzlichen Forschungsregelungen, z. B. in Krebsregistergesetzen, oder die Einwilligung der Betroffenen in Betracht.

3. Typische Problemfelder

3.1 Zweckbindung von personenbezogenen Daten

Problem:

Personenbezogene Daten werden auf der Grundlage einer Einwilligung der Betroffenen oder einer gesetzlichen Forschungsregelung zu einem bestimmten Zweck, d.h. für eine konkrete epidemiologische Studie, erhoben. Aus wissenschaftlicher Sicht kann es allerdings später wichtig werden, diese Daten für die Bearbeitung neuer Fragestellungen zu nutzen, die zum Zeitpunkt der Einwilligungserklärung der Betroffenen bzw. der Übermittlungen der Daten noch nicht bekannt waren und daher in die Angaben zum Zweck der Verwendung der Daten nicht einbezogen wurden. Eine erneute Kontaktierung der Probanden ist häufig nicht möglich oder wäre mit zusätzlichem hohem Aufwand und Kosten verbunden und könnte wegen Umzug, Tod, Desinteresse etc. der Betroffenen auch zu Problemen im Hinblick auf die Repräsentativität der Daten führen.

Lösungsansätze:

- Soweit es sich um anonymisierte Daten handelt, unterliegt eine Zweckänderung der Daten keinen rechtlichen Beschränkungen. Die datenschutzrechtlichen Regelungen sind nicht anzuwenden. Dies gilt entsprechend für die Verwendung biologischer Materialien.
- Es besteht die Möglichkeit, Einwilligungserklärungen so zu formulieren, dass eine eventuelle inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfasst ist. Grundsätzlich muss eine Einwilligungserklärung hinreichend bestimmt sein. Die Anforderungen an die Vollständigkeit und Präzision

der Einwilligungserklärungen können jedoch je nach der konkreten Verarbeitungssituation variieren. Bei der Verarbeitung personenbezogener Daten für eine wissenschaftliche Studie ist eine weitere Formulierung des Zwecks vertretbar und angemessen. Es ist die Entscheidung der Betroffenen, inwieweit sie auch eine Einwilligungserklärung mit einer weiteren Formulierung des Zwecks der Studie unterschreiben, d.h. es handelt sich um eine Frage der Akzeptanz. Die Einwilligungserklärung kann auch verschiedene Varianten der Verwendung der Daten enthalten, über die die Betroffenen entscheiden.

- Bei einer Übermittlung personenbezogener Daten auf der Grundlage einer gesetzlichen Forschungsregelung ist es vertretbar und angemessen, den Zweck der Übermittlung der Daten (d.h. die Darstellung des Forschungsvorhabens) so zu formulieren, dass eventuelle inhaltliche Änderungen bzw. Ausweitungen der Fragestellungen der Studie mit umfasst sind.
- In Betracht kommt auch eine Anwendung der datenschutzrechtlichen Regelungen über die Zweckänderung personenbezogener Daten. Die rechtlichen Voraussetzungen für eine Zweckänderung sind im Einzelfall zu prüfen.
- Verfahrensrechtliche Lösungen wie z. B. Einschaltungen von Ethikkommissionen, Datenschutzbeauftragten etc. kommen im Regelfall nur dann in Betracht, wenn Rechtsvorschriften vorhanden sind, die grundsätzlich eine Zweckänderung der Daten unter bestimmten Voraussetzungen zulassen, denn weder Ethikkommissionen noch Datenschutzbeauftragte können ihre Entscheidung an die Stelle der Entscheidung der Betroffenen setzen.

3.2 Löschung der Daten nach Beendigung des Forschungsvorhabens

Problem:

Es ist offen, in welchem Umfang die Daten nach Beendigung des Forschungsvorhabens gelöscht werden müssen.

Lösungsansätze:

- Soweit die Daten anonymisiert sind, sind die datenschutzrechtlichen Regelungen nicht anzuwenden und die weitere Verarbeitung der Daten unterliegt keinen rechtlichen Beschränkungen.
- Werden personenbezogene Daten verarbeitet, sollte der Zeitpunkt der Löschung der personenbezogenen Daten in dem Text der Einwilligungserklärung bzw. dem Antrag auf Übermittlung der Daten konkret benannt werden. Ist im Einzelfall eine Speicherung anonymisierter Daten für die wissenschaftliche Nachprüfbarkeit der Forschungsergebnisse nach ihrer Publikation nicht ausreichend. so kann eine Speicherung der personenbezogenen Daten für einen bestimmten Zeitraum nach der Publikation der Forschungsergebnisse zur wissenschaftlichen Nachprüfbarkeit der Forschungsergebnisse zulässig sein. Der Zeitpunkt für die Löschung der personenbezogenen Daten sollte in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst konkret benannt werden.

3.3 Weitergabe anonymisierter Daten

Problem:

In einem Forschungsvorhaben erweist es sich als sinnvoll, anonymisierte Daten aus mehreren Studien zu poolen, d.h. zusammenzuführen und gemeinsam statistisch

auszuwerten, weil sich für viele Fragestellungen nur dadurch ausreichend große Fallzahlen erreichen lassen. Auch eine Weitergabe von anonymisierten Daten in Form von Public Use Files kann sinnvoll sein, um die Daten anderen Wissenschaftlern für ihre Forschung zugänglich zu machen.

Lösungsansätze:

- Grundsätzlich können anonymisierte Daten ohne rechtliche Beschränkungen weitergegeben werden. Es muss allerdings im Einzelfall geprüft werden, ob es sich tatsächlich um anonymisierte Daten handelt und ob die Daten auch nach der Zusammenführung mit den Daten aus den anderen Studien noch als anonymisiert qualifiziert werden können. Eine Zusammenführung anonymisierter Daten aus mehreren Studien führt häufig dazu, dass eine Deanonymisierung der Daten noch schwieriger wird. Im Einzelfall kann es jedoch durchaus auch die Konstellation geben, dass anonymisierte Daten durch ihre Zusammenführung mit Daten aus anderen Studien leichter deanonymisiert werden können und dann u.U. als personenbezogen qualifiziert werden müssen. In diesem Fall sind die datenschutzrechtlichen Regelungen zu beachten.
- Eine Übermittlung personenbezogener Daten ist nicht in jedem Fall ausgeschlossen. Es gilt das oben unter 3.1 Gesagte entsprechend.

3.4 Optimale Gestaltung der Einverständniserklärung bzw. des Antrags auf Übermittlung der Daten

Problem:

Einerseits sollten in der Einverständniserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst präzise die zu untersuchende Fragestellung, die Vorgehensweise und die an der Studie beteiligten Institutionen angegeben werden. Andererseits kann es sich im Laufe einer Studie ergeben, dass Kooperationspartner wechseln und sich Fragestellungen erweitern bzw. neue Fragestellungen auftauchen. Wie kann dies in der Einverständniserklärung bzw. in dem Antrag optimal berücksichtigt werden?

Lösungsansätze:

- Die Formulierung des Zwecks der epidemiologischen Studie kann so erfolgen, dass eine evtl. inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mitumfasst ist (vgl. oben 3.1).
- Die Daten verarbeitende Stelle – im Regelfall die Institution (Klinikum, Institut etc.) – muss in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung personenbezogener Daten konkret und verbindlich benannt werden. Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die Verantwortlichkeit für die personenbezogenen Daten dauerhaft klar geregelt ist und der Bürger eindeutig darüber informiert ist, an wen er sich wo bei Auskunftsersuchen, Widerruf seiner Einwilligung etc. wenden kann. Die Namen der Kooperationspartner müssen nur dann konkret aufgeführt werden.
- Im Einzelfall ist es auch möglich, eine Klausel dahingehend aufzunehmen, dass Abweichungen von der angegebenen Vorgehensweise und Erweiterungen der Fragestellungen nur nach Rücksprache mit dem zuständigen Datenschutzbeauftragten bzw. der Ethikkommission erfolgen.

3.5 Verknüpfung personenbezogener Datensätze (record linkage), z. B. bei Kohortenstudien

Problem:

Es soll eine Studie durchgeführt werden, bei der ein Abgleich verschiedener Datenbestände vorgenommen wird, die Betroffenen jedoch zu keinem Zeitpunkt direkt kontaktiert bzw. um Einwilligung gebeten werden. Ein Beispiel hierfür ist eine Studie, bei welcher die Expositionsbedingungen am Arbeitsplatz aus betrieblichen Unterlagen der dort tätigen Arbeitnehmer zusammengestellt werden. Die Erhebung der aufgetretenen Erkrankungen erfolgt über vorhandene Krankheitsregister (z. B. Krebsregister) oder über Einwohnermeldeämter und Gesundheitsämter zur Erhebung des Vitalstatus und der Todesursache.

Lösungsansätze:

- In einzelnen gesetzlichen Regelungen wie z. B. Krebsregistergesetzen ist ein Abgleich verschiedener Datenbestände vorgesehen. Im Übrigen sehen die bundes- bzw. landesrechtlichen Regelungen – mit Unterschieden im Einzelnen – grundsätzlich die Möglichkeit von Datenübermittlungen durch Betriebe, Einwohnermeldeämter, Gesundheitsämter, Krebsregister etc. vor (vgl. z. B. § 28 Abs. 2 Nr. 2 BDSG, Meldegesetze, Gesetze über den öffentlichen Gesundheitsdienst, Krebsregistergesetze, Forschungsregelungen im Bundesdatenschutzgesetz und in den Landesdatenschutzgesetzen). Die rechtlichen Voraussetzungen dieser Übermittlungsbestimmungen müssen im Einzelfall geprüft werden.
- Vor der Durchführung einer Studie sollte der Einsatz eines Treuhänders, d.h. eines vertrauenswürdigen Dritten, geprüft werden, der insbesondere personenbezogene Daten aus verschiedenen Quellen zuordnet, speichert und anonymisiert an die Forschungsinstitution übermittelt. Die Übermittlung personenbezogener Daten an einen Treuhänder bedarf ebenso wie die Übermittlung personenbezogener Daten an die Forschungsinstitution selbst einer Rechtsgrundlage. Der Einsatz eines Treuhänders kann jedoch im Einzelfall den Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung minimieren, indem der Kreis derjenigen Personen, die personenbezogene Daten zur Kenntnis erhalten, reduziert wird und die Datensicherheit umfassender gewährleistet wird. Diese Aspekte haben Relevanz für die in vielen Forschungsregelungen vorgesehene Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens.

3.6 Nutzung der amtlichen Statistik

Problem:

Häufig werden von den statistischen Ämtern des Bundes und der Länder in der Praxis nur Daten übermittelt, bei denen eine Mindestzahl auftretender Konstellationen pro Zelle erfüllt ist. Hierdurch werden bestimmte Aussagen unmöglich gemacht, z. B. die Unterteilung einer Untersuchungsgruppe nach Altersklassen oder nach genaueren diagnostischen Einheiten wie Todesursachen.

Lösungsansätze:

- Die statistischen Ämter des Bundes und der Länder dürfen faktisch anonymisierte Einzelangaben für wissenschaftliche Vorhaben an Hochschulen und

andere Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln, wenn die Empfänger Amtsträger, für den öffentlichen Dienst Verpflichtete oder nach § 16 Abs. 7 Bundesstatistikgesetz Verpflichtete sind (§ 16 Abs. 6 BStatG). Die Daten sind zu löschen, sobald das Vorhaben durchgeführt ist, eine verbindliche Löschungsfrist besteht nicht (§ 16 Abs. 8 BStatG).

- Es besteht die Möglichkeit, aus bereits vorliegenden Individualdaten faktisch anonymisierte Einzelangaben zu bestellen. Von diesem Weg wird jedoch häufig aus Kostengründen Abstand genommen. Für einige Bereiche sind faktisch anonyme Daten auf Vorrat erstellt worden, z. B. aus dem Mikrozensus 1995 und der Einkommens- und Verbrauchsstichprobe 1993. Einzelangaben aus solchen Beständen können gegen geringe Gebühr bezogen werden, die breite Anwendung dieser Verfahren wird aber durch Geldmangel behindert.
- Leichter verfügbar sind statistische Tabellen, die i.a. dadurch anonymisiert sind, dass Felder mit geringen Belegungen so zusammengefasst wurden, dass Zahlen kleiner als 3 nicht mehr auftreten. Dies ist für Forschungszwecke oft hinderlich. Soweit jedoch die Angaben aus Feldern mit zu geringer Belegung nicht mehr erkennen lassen, als nach § 16 Abs. 6 BStG übermittelt werden darf, und auch die weiteren Bedingungen dieser Vorschrift erfüllt werden, bestehen keine datenschutzrechtlichen Bedenken gegen die Übermittlung auch solcher Tabellen mit faktisch anonymisierten Einzelangaben.

3.7 Aufbewahrung von Daten der amtlichen Statistik

Problem:

Die Löschung älterer Datenbestände kann der epidemiologischen Forschung unwiederbringlich Grundlagen entziehen.

Lösungsansätze:

- Abgesehen von den Hilfsmerkmalen (insbesondere Namen und Anschriften) gibt es i. a. keine gesetzlichen Löschungsfristen für statistische Einzelangaben. Die Löschungspraxis richtet sich nach der Einschätzung des zu erwartenden Nutzens aus der weiteren Aufbewahrung im Verhältnis zu deren Kosten. Datenschutzrechtlich zulässig wäre eine weitere Speicherung statistischer Einzelangaben auch für zukünftig erwartete, aber noch nicht im Einzelnen bekannte Zwecke. Vor Löschung der Daten sind diese nach den jeweils geltenden archivrechtlichen Bestimmungen den zuständigen Archiven anzubieten. Zur Dauer der Speicherung der Daten bei den statistischen Ämtern bzw. bei den Archiven sollte aus dem Wissenschaftsbereich der Bedarf dargelegt werden. Die Aufbewahrung der Totenscheine (im Original) richtet sich nach dem jeweiligen Landesrecht.

3.8 Nutzung von Krebsregistern für Fall-Kontroll-Studien

Problem:

Bei Fall-Kontroll-Studien wird häufig ein (möglichst repräsentativer) Zugang zu bestimmten Erkrankungsgruppen benötigt. Dieser kann unter hohen Kosten auf der Grundlage von Einwilligungen der Betroffenen oder gesetzlichen Forschungsregelungen über Krankenhäuser erfolgen, in denen diese Patienten behandelt werden.

Ein effektiverer und vollständigerer Zugang ist aber derjenige über Krankheitsregister (z. B. Krebsregister). Der Zugang über das Register dient dabei nur der Auffindung des Patienten und der Kontaktaufnahme mit ihm, alles Weitere kann durch die Einverständniserklärung der beteiligten Personen abgedeckt werden. Diesen Patienten werden dann Kontrollpersonen aus der Bevölkerung gegenübergestellt, die auf anderem Wege kontaktiert und in die Studie einbezogen werden.

Lösungsansätze:

- Gemäß § 8 des Krebsregistergesetzes des Bundes (KRG) können für Maßnahmen des Gesundheitsschutzes und bei wichtigen und auf andere Weise nicht durchzuführenden, im öffentlichen Interesse stehenden Forschungsaufgaben die zuständigen Behörden der Vertrauensstelle des Krebsregisters die Abgleichung Personen identifizierender Daten mit Daten des Krebsregisters und die Entschlüsselung der erforderlichen verschlüsselten Identitätsdaten und deren Übermittlung im erforderlichen Umfang genehmigen.

  Vor der Übermittlung personenbezogener Daten hat die Vertrauensstelle über den meldenden behandelnden Arzt oder Zahnarzt die schriftliche Einwilligung des Patienten einzuholen. Ist der Patient verstorben, hat die Vertrauensstelle vor der Datenübermittlung die schriftliche Einwilligung des nächsten Angehörigen einzuholen, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.
- Die Länder können in ihren Gesetzen zur Ausführung des Krebsregistergesetzes abweichende Regelungen treffen (§ 13 Abs. 5 Nr. 2 KRG). Einige Länder haben vom Krebsregistergesetz des Bundes abweichende datenschutzrechtliche Modelle (z. B. keine Aufgliederung des Registers in Vertrauensstelle und Registerstelle) gewählt. Im Einzelfall sind die einschlägigen Übermittlungsbestimmungen zu prüfen und zu beachten.

3.9 Datenschutzfragen bei bundesweiten Studien

Problem:

Bei Studien, die in mehreren Bundesländern stattfinden, sind häufig die unterschiedlichen datenschutzrechtlichen Regelungen der Bundesländer zu berücksichtigen.

Lösungsansätze:

- Zur Vereinfachung des Verfahrens kann der Studienleiter den für ihn zuständigen Datenschutzbeauftragten bzw. denjenigen Datenschutzbeauftragten, in dessen Bundesland die zentrale Speicherung der Daten des Forschungsprojekts erfolgen soll, darum bitten, die Stellungnahmen der anderen Datenschutzbeauftragten (soweit von dem konkreten Forschungsprojekt betroffen) zu koordinieren.

III. Entschließungen der 56. Konferenz am 5./6. Oktober 1998 in Wiesbaden

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Dringlichkeit der Datenschutzmodernisierung

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die analysierte Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Fehlende bereichsspezifische Regelungen bei der Justiz

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Derzeit werden in allen Bereichen der Justiz – bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27. 09. 1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,

  namentlich die

  – Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen,

  – Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden;
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen – erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Entwicklungen im Sicherheitsbereich

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

C. Beschlüsse und Arbeitspapiere der Datenschutzbeauftragten der Europäischen Union

Entschließung der Europäischen Konferenz der Datenschutzbeauftragten gegen die Veröffentlichung herabsetzender Informationen im Internet (16./17. September 1998, Santiago de Compostela)

Die unabhängigen Datenschutzbehörden der Europäischen Union zusammen mit denjenigen von Island, Norwegen und der Schweiz, die sich im Anschluss an die 20. Internationale Konferenz in Santiago de Compostela am 16. und 17. September 1998 getroffen haben, sind überzeugt, dass das Internet als ein Mittel dienen kann, die Demokratie zu stärken, indem es den Bürgern erlaubt, besser an öffentlichen Debatten teilzunehmen, und indem es öffentliche Angelegenheiten höhere Publizität verschafft.

Sie machen darauf aufmerksam,

- dass der Gebrauch eines Mittels wie des Internet zur Verbreitung und Sammlung von Informationen und die Folgen, die dies für die Grundwerte hat, die Anerkennung der Notwendigkeit von Garantien erfordern und
- dass derartige Garantien international geschaffen werden müssen, ohne dass damit Hindernisse für die Meinungsfreiheit und das Recht auf Information errichtet werden.

Sie sind der Ansicht, dass auf der Basis der Grundsätze des Schutzes personenbezogener Daten, die in vielen Staaten bereits anerkannt sind und die auch für das Internet gelten, alle Staaten, und insbesondere diejenigen, in denen die Nutzung der neuen Technologien am weitesten verbreitet ist, Maßnahmen zum Schutz personenbezogener Daten ergreifen und verstärken und eine internationale Kooperation fördern müssen, die auf den weltweit anerkannten Werten beruhen und die sicherstellen, dass die steigende Nutzung des Internet keine Folgen hervorbringt, die mit dem Schutz personenbezogener Daten und der Persönlichkeitsrechte nicht vereinbar sind.

Sie weisen insbesondere darauf hin,

- dass Daten, die dafür missbraucht werden könnten, Personen Gefahren auszusetzen oder sie herabzusetzen, auf dem Internet nicht in einer Weise verbreitet werden dürfen, die einen solchen Missbrauch ermöglicht,
- dass effektive rechtliche und technische Maßnahmen entwickelt werden sollten, die es den betroffenen Personen ermöglichen, die Nutzung ihrer personenbezogenen Daten selbst zu bestimmen und zu kontrollieren,
- dass effektive Maßnahmen ergriffen werden sollten, um die Übereinstimmung mit den Prinzipien des Datenschutzes durch alle Beteiligten, die verantwortlich für die Verbreitung oder Sammlung personenbezogener Daten im Internet sind oder die technische Infrastruktur des Internet zur Verfügung stellen, sicherzustellen.

DECLARATION

The independent data protection and privacy authorities of the Member States of the European Union, together with the independent data protection and privacy authorities of Iceland, Norway and Switzerland who met at the end of the 20th annual international conference on data protection in Santiago de Compostela (Spain), on 16 - 17 september 1998 issued the following declaration:

CONVINCED that the Internet can serve as a means of strengthening democracy especially by allowing citizens to participate more widely in public debates and by ensuring greater openness in public affairs;

DRAW ATTENTION to the fact:

- that the use of such a means of distribution and collection of information as the Internet and the consequences which it can have in relation to fundamental principles require the acknowledgment of the need for guarantees, and,
- that such guarantees, without erecting obstacles to the freedom of speech and the right to information, must be internationally established;

TAKE THE VIEW that, on the basis of the principles of personal data protection already well established in many states and applicable to the Internet, all states, and in particular those which make the greatest use of new technologies, must adopt and enforce measures for the protection of personal data and promote international cooperation based on recognised universal principles to ensure that the growing use of the Internet does not produce consequences incompatible with the protection of personal data and privacy,

and HIGHLIGHT:

- that data which can be misused to pose risks for or harrass individuals not be distributed on the Internet in such a way as to permit such misuses;
- that effective legal and technical means be developed to allow data subjects to define and control the use of their personal data,
- that effective means be put in place to ensure compliance with data protection principles by all actors responsible for disseminating or collecting personal data on the Internet or providing the Internet's technical infrastructure.

Arbeitspapier 12 der Gruppe nach Art. 29 der Datenschutzrichtlinie der EU

Übermittlungen personenbezogener Daten an Drittländer:
Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU

Von der Arbeitsgruppe am 24. Juli 1998 angenommen
(WP 12 – GD XV D/5025/98 – DE endgültig)

Inhaltsübersicht:

Einführung

Ziel dieser Arbeitsunterlage ist es, die bislang geleistete Arbeit der nach Artikel 29 der Datenschutzrichtlinie eingesetzten Arbeitsgruppe von EU- Datenschutzbeauftragten

[Siehe

- „Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer – Mögliche Ansätze für eine Bewertung der Angemessenheit“, von der Arbeitsgruppe am 26. Juni 1997 angenommene Diskussionsgrundlage;
- Arbeitsunterlage: „Beurteilung der Selbstkontrolle der Wirtschaft: Wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland?“, von der Arbeitsgruppe am 14. Januar 1998 angenommen;
- Arbeitsunterlage: „Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer“, von der Arbeitsgruppe am 22. April 1998 angenommen]

zu einer allgemeinen Übersicht über ihre Ansichten zu sämtlichen zentralen Fragen zusammenzufassen, die sich aus der Übermittlung personenbezogener Daten in Drittländer im Zusammenhang mit der Anwendung der Datenschutzrichtlinie der EU (95/46/EG) ergeben. Der Aufbau folgt dabei dem System, wie es für internationale Übermittlungen personenbezogener Daten in Artikel 25 und 26 der Richtlinie vorgesehen ist.

In Artikel 25 Absatz 1 ist der Grundsatz aufgeführt, dass die Mitgliedstaaten die Übermittlung in ein Drittland nur gestatten, wenn das betreffende Drittland ein angemessenes Schutzniveau gewährleistet. In Absatz 2 wird darauf verwiesen, dass „die Angemessenheit ... unter Berücksichtigung aller Umstände beurteilt“ wird.

Nach Absatz 6 kann die Kommission feststellen, dass bestimmte Länder ein angemessenes Schutzniveau gewährleisten. Kapitel 1 dieses Papiers ist dieser zentralen Frage des angemessenen Schutzniveaus gewidmet. Zunächst wird erklärt, was unter „angemessen“ zu verstehen ist, und danach ein Rahmen für die Frage vorgestellt, wie die Angemessenheit des Schutzes im konkreten Fall beurteilt werden kann.

In Kapitel 2 und 3 wird dieser Ansatz weiterverfolgt. Kapitel 2 beschäftigt sich mit Übermittlungen in Länder, die das Übereinkommen Nr. 108 des Europarates ratifiziert haben, während Kapitel 3 Fragen im Zusammenhang mit Übermittlungen behandelt, bei denen der Schutz personenbezogener Daten hauptsächlich oder vollständig über Mechanismen der freiwilligen Selbstkontrolle und nicht auf gesetzlichem Wege erfolgt.

Fehlt das angemessene Schutzniveau im Sinne von Artikel 25 Absatz 2, so ist in Artikel 26 Absatz 2 der Richtlinie die Möglichkeit von Ad-hoc-Maßnahmen vorgesehen, die insbesondere vertraglicher Art sein und zur Festlegung angemessener Garantien führen können, auf deren Basis die betreffende Übermittlung erfolgen kann.

In Kapitel 4 des vorliegenden Beitrags werden die Umstände geprüft, unter denen vertragliche Lösungen geeignet erscheinen, und Empfehlungen zur möglichen Form und zum Inhalt dieser Lösungen gegeben.

Kapitel 5 beschäftigt sich mit der dritten und letzten Situation, die in der Richtlinie vorgesehen ist, d. h. bestimmten Fällen nach Artikel 26 Absatz 1, in denen vom Erfordernis des „angemessenen Schutzniveaus“ praktisch abgewichen werden kann. Der genaue Umfang dieser Ausnahmen wird unter Zuhilfenahme von Beispielen von Fällen geprüft, in denen diese Möglichkeit genutzt werden kann bzw. dies nicht möglich erscheint.

Im abschließenden Kapitel 6 finden sich Bemerkungen zu Verfahrensfragen, die sich in Verbindung mit der Beurteilung der Angemessenheit (bzw. des Mangels an Angemessenheit) des Schutzniveaus und der Erzielung eines gemeinschaftsweit einheitlichen Ansatzes zu diesen Fragen ergeben.

Als Anhang sind mehrere anschauliche Fallstudien beigefügt, mit denen demonstriert werden soll, wie der im vorliegenden Dokument beschriebene Ansatz in der Praxis umgesetzt werden könnte.

Kapitel 1:

Bewertung der Angemessenheit des Schutzes

Was ist ein „angemessenes Schutzniveau“?

Sinn und Zweck des Datenschutzes ist es, Personen, deren Daten verarbeitet werden, Schutz zu gewährleisten. Erreicht wird dies durch eine Kombination von dem Betroffenen eingeräumten Rechten und bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt. Die in der Richtlinie 95/46/EG verankerten Pflichten und Rechte orientieren sich an den Festlegungen des Übereinkommens Nr. 108 des Europarates, die sich wiederum kaum von den diesbezüglichen Leitlinien der OECD (1980) oder der UNO (1990) unterscheiden. Dementsprechend kann davon ausgegangen werden, dass zum Inhalt von Datenschutzvorschriften weitgehend Einigkeit besteht, die weit über die fünfzehn Mitgliedstaaten der Gemeinschaft hinausgeht.

Mit Datenschutzvorschriften werden die Rechte des Einzelnen aber nur dann geschützt, wenn sie auch in die Praxis umgesetzt werden. Daher ist nicht nur der Inhalt der für die Übermittlung personenbezogener Daten in Drittländer geltenden Vorschriften, sondern auch das System zu betrachten, mit dem die Durchsetzung der Regeln gesichert werden soll. In Europa ist es bislang so, dass die Datenschutzvorschriften gesetzlich festgeschrieben werden und bei Nichteinhaltung Strafen auferlegt werden können bzw. dem Einzelnen das Recht auf Wiedergutmachung eingeräumt wird. Darüber hinaus sind in derartigen Gesetzen zusätzliche verfahrensrechtliche Mechanismen wie die Einrichtung von Kontrollstellen vorgesehen, denen Überwachungsaufgaben und die Verfolgung von Beschwerden obliegen. Die Verfahrensaspekte spiegeln sich auch in der Richtlinie 95/46/EG wider, die Bestimmungen über Haftung, Sanktionen, Rechtsbehelfe, Kontrollstellen und Meldung bei der Kontrollstelle enthält. Außerhalb der Gemeinschaft sind derartige verfahrensrechtliche Mittel zur Sicherung der Einhaltung der Datenschutzvorschriften weniger üblich. Die Parteien des Übereinkommens Nr. 108 sind zur gesetzlichen Verankerung der Grundsätze des Datenschutzes verpflichtet, doch sind zusätzliche Mechanismen wie eine Kontrollstelle nicht vorgesehen. In den OECD-Leitlinien wird lediglich „ihre Berücksichtigung" in der Landesgesetzgebung angemahnt, und es fehlen verfahrensrechtliche Mittel, mit denen gesichert würde, dass die Leitlinien tatsächlich zu einem wirksamen Schutz des Einzelnen führen. In den später verabschiedeten Leitlinien der UNO sind andererseits Bestimmungen über Kontrolle und Sanktionen enthalten, was zeigt, dass sich weltweit die Erkenntnis durchsetzt, dass auf die ordnungsgemäße Umsetzung von Datenschutzvorschriften nicht verzichtet werden kann.

Vor diesem Hintergrund wird deutlich, dass die Analyse des angemessenen Schutzniveaus ohne die Einbeziehung der beiden folgenden Grundelemente sinnlos ist: Inhalt der geltenden Vorschriften und Mittel zur Sicherung ihrer wirksamen Anwendung.

Geht man von der Richtlinie 95/46/EG aus und berücksichtigt dabei die Bestimmungen weiterer internationaler Dokumente zum Datenschutz, so sollte es möglich sein, für den Datenschutz einen „Kern" von „inhaltlichen" Grundsätzen und „verfahrensrechtlichen" bzw. mit der „Durchsetzung im Zusammenhang stehenden" Erfordernissen herauszuarbeiten, deren Einhaltung als Mindestanforderung an eine Situation gilt, in der von einem angemessenen Schutzniveau gesprochen werden kann. Dabei sollte nicht starr auf bestimmte Mindestanforderungen gepocht werden, denn während die Liste in einem Fall erweitert werden muss, reicht im anderen möglicherweise ein vermindertes Anforderungsspektrum. Bei der Bestimmung der genauen Anforderungen an einen konkreten Fall ist das Ausmaß der Gefahren, die für den Betroffenen der Datenübermittlung entstehen, ein wichtiger Faktor. Doch ungeachtet dieser Einschränkungen ist eine grundlegende Aufstellung von Mindestanforderungen in jedem Fall ein nützlicher Ausgangspunkt für eine Analyse.

i. Inhaltliche Grundsätze

Die folgenden Grundsätze sind unbedingt zu berücksichtigen:

1. Der Grundsatz der Beschränkung der Zweckbestimmung

   Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle [Artikel 13 gestattet eine Einschränkung auf den „Grundsatz der Zweckbestimmung", sofern eine solche Beschränkung für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, ein wichtiges wirtschaftliches oder finanzielles Interesse oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen notwendig ist].

2. Der Grundsatz der Datenqualität und -verhältnismäßigkeit

   Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv sein.

3. Der Grundsatz der Transparenz

   Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland des für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich [Artikel 11 Absatz 2 sieht vor, dass für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, die betroffene Person nicht informiert zu werden braucht, wenn dies unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist].

4. Der Grundsatz der Sicherheit

   Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. Das Recht auf Zugriff, Berichtigung und Widerspruch

   Die betroffene Person muss das Recht haben, eine Kopie aller sie betreffenden Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten haben mit Artikel 13 der Richtlinie im Einklang zu stehen.

6. Beschränkungen der Weiterübermittlung in andere Drittländer

   Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen haben mit Artikel 26 Absatz 1 der Richtlinie im Einklang zu stehen. (Diese Ausnahmen werden in Kapitel 5 untersucht.)

Beispiele weiterer, auf spezifische Arten der Verarbeitung anwendbarer Grundsätze:

1. Sensible Daten

   Sind „sensible" Kategorien von Daten betroffen (die in Artikel 8 der Richtlinie aufgelistet sind [Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die

Arbeitspapiere der Datenschutzbeauftragten der EU

Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben und Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen]), so haben zusätzliche Sicherheitsmaßnahmen wie das Erfordernis zu gelten, dass die betroffene Person ausdrücklich in die Verarbeitung einwilligt.

2. Direktmarketing

   Werden Daten zum Zwecke des Direktmarketings übermittelt, so muss die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu entscheiden.

3. Automatisierte Einzelentscheidung

   Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muss die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der Person zu schützen.

ii. Verfahrensrechtlicher Mechanismus/Durchsetzungsmechanismus

In Europa besteht weitgehend Einigkeit darüber, dass die Datenschutzgrundsätze gesetzlich verankert werden müssen. Im Wesentlichen bestehen auch keine Zweifel über die Notwendigkeit der „externen Kontrolle“ in Form einer unabhängigen Stelle, die Teil eines Systems zur Einhaltung des Datenschutzes ist. In anderen Teilen der Welt hingegen ist dies nicht immer der Fall. Als Grundlage für die Beurteilung der Angemessenheit des vorhandenen Datenschutzniveaus sind zunächst die Ziele des zugrunde liegenden verfahrensrechtlichen Systems für den Datenschutz zu bestimmen; darauf aufbauend ist das Spektrum der verschiedenen in Drittländern bestehenden gerichtlichen und außergerichtlichen verfahrensrechtlichen Mechanismen zu bewerten.

Ein Datenschutzsystem verfolgt im Wesentlichen drei Ziele:

1. Gewährleistung einer guten Befolgungsrate der Vorschriften. (Kein System kann eine 100 %ige Einhaltung garantieren, aber einige sind besser als andere). Ein gutes System zeichnet sich im Allgemeinen dadurch aus, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Wahrnehmung sehr stark bewusst sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso relevant sind natürlich auch Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.

2. Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte. Der Einzelne muss seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muss es eine Art institutionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.

3. Gewährleistung angemessener Entschädigung für die geschädigte Partei bei Verstoß gegen die Bestimmungen. Für dieses Schlüsselelement muss ein System unabhängiger Schlichtung vorhanden sein, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.

Kapitel 2:

Anwendung des Ansatzes auf Länder, die das Übereinkommen Nr. 108 des Europarates ratifiziert haben

Das Übereinkommen Nr. 108 ist neben der Richtlinie das einzige internationale Instrument, das auf dem Gebiet des Datenschutzes bindend ist. Die Mehrzahl der Parteien des Übereinkommens sind auch Mitgliedstaaten der Europäischen Union (die Ratifizierung ist inzwischen durch alle 15 Staaten erfolgt) bzw. Länder wie Norwegen und Island, für die die Richtlinie aufgrund des Abkommens über den Europäischen Wirtschaftsraum ohnehin gilt. Doch auch von Slowenien, Ungarn und der Schweiz ist das Übereinkommen ratifiziert worden, und insbesondere angesichts der Tatsache, dass das Übereinkommen auch Ländern offen steht, die dem Europarat nicht angehören, dürften weitere Drittländer in der Zukunft folgen. Aus diesem Grund ist die Prüfung, ob die Länder, die das Übereinkommen ratifiziert haben, ein angemessenes Schutzniveau im Sinne von Artikel 25 der Richtlinie bieten, nicht nur von rein akademischem Interesse.

Als Ausgangspunkt ist es zunächst günstig, den Wortlaut des Übereinkommens unter dem Aspekt der theoretischen Annahme eines „angemessenen Schutzniveaus“, wie es in Kapitel 1 dieses Dokuments beschrieben ist, zu beleuchten.

Was den Inhalt der Grundprinzipien betrifft, so enthält das Übereinkommen praktisch die ersten fünf der sechs „Mindestanforderungen“. [Hinsichtlich des Grundsatzes der Transparenz mögen gewisse Zweifel bestehen. Artikel 8 Absatz a) des Übereinkommens kann mit der aktiven Pflicht zur Bereitstellung von Informationen, die den Kern von Artikel 10 und 11 der Richtlinie darstellt, kaum gleichgesetzt werden. Im Übrigen sind im Übereinkommen keine konkreten Rechte zur Verwehrung der Verwendung der Daten vorgesehen, wenn diese für Zwecke des Direktmarketings eingesetzt werden sollen. Es fehlen auch Bestimmungen für automatisierte Einzelentscheidungen (Profilerstellung).] Auch das Erfordernis geeigneter Sicherungsmaßnahmen für sensible Daten ist vorgesehen, die als Angemessenheitskriterium für Fälle, in denen derartige Daten vorkommen, angesehen werden können.

Ein Mangel des Inhalts der wesentlichen Vorschriften des Übereinkommens besteht darin, dass für die Übermittlung an Länder, die nicht Vertragsparteien des Übereinkommens sind, Beschränkungen nicht vorgesehen sind. Dies birgt die Gefahr, dass ein dem Übereinkommen Nr. 108 beigetretenes Land bei der Übermittlung von Daten aus der Gemeinschaft in ein weiteres Drittland mit völlig unangemessenem Schutzniveau als „Zwischenstation“ benutzt wird.

Der zweite Aspekt des „angemessenen Schutzniveaus“ betrifft die bestehenden verfahrensrechtlichen Mechanismen, mit denen den Grundprinzipien Geltung verschafft werden soll. Dem Übereinkommen zufolge sind ihre Grundsätze in das innerstaatliche Recht aufzunehmen und geeignete Sanktionen und Rechtsmittel für den Fall der Verletzung festzulegen. Dies müsste für die Gewährleistung eines angemessenen Niveaus der Einhaltung der Vorschriften und der angemessenen Entschädigung für die betroffenen Personen im Falle der Nichteinhaltung der Vorschriften ausreichen (Ziel 1 und 3 eines Systems zur Einhaltung des Datenschutzes). Allerdings verpflichtet das Übereinkommen die Vertragsparteien nicht, institutionelle Mechanismen zur unabhängigen Untersuchung von Beschwerden festzulegen, obwohl die Länder, von denen die Ratifizierung vorgenommen wurde, dies in der Regel getan haben. Dies ist ein Nachteil, da angemessene Unterstützung und Hilfe für die einzelnen betroffenen Personen bei der Wahrnehmung ihrer Rechte (Ziel 2) ohne diese institutionellen Mechanismen möglicherweise nicht garantiert sind.

Diese kurze Analyse lässt den Schluss zu, dass von den meisten Übermittlungen personenbezogener Daten in Länder, von denen das Übereinkommen Nr. 108 ratifiziert worden ist, angenommen werden kann, dass sie gemäß Artikel 25 (1) der Richtlinie unter der Bedingung statthaft sind, dass

- das betreffende Land über geeignete Mechanismen für die Gewährleistung der Einhaltung der Vorschriften, die Unterstützung betroffener Personen und die Möglichkeit einer Entschädigung (beispielsweise eine unabhängige Kontrollstelle mit entsprechenden Befugnissen) verfügt und
- das betreffende Land das Endbestimmungsland der Übermittlung und keine Zwischenstation ist, über die die Daten geleitet werden, es sei denn, es handelt sich um die Weiterübermittlung zurück in die EU oder einen anderen Bestimmungsort mit angemessenem Schutzniveau. [Das Übereinkommen Nr. 108 wird derzeit einer Prüfung unterzogen, in deren Verlauf es zu Änderungen kommen kann, mit denen diese und weitere Schwierigkeiten angesprochen werden.]

Dies ist natürlich eine recht vereinfachte und oberflächliche Prüfung des Übereinkommens. Im Zusammenhang mit konkreten Fällen der Übermittlung von Daten in Länder, die dem Übereinkommen beigetreten sind, dürften neue, an dieser Stelle nicht in Betracht gezogene Probleme auftreten.

Kapitel 3:

Anwendung des Ansatzes auf die Selbstkontrolle der Wirtschaft

Einführung

Entsprechend Artikel 25 Absatz 2 der Datenschutzrichtlinie (95/46/EG) ist die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Nicht nur auf Rechtsvorschriften, sondern insbesondere auf „die dort geltenden Standesregeln und Sicherheitsmaßnahmen" wird Bezug genommen.

Im Text der Richtlinie ist daher festgelegt, dass in dem betreffenden Drittland möglicherweise geltende außergerichtliche Vorschriften berücksichtigt werden, sofern diese Regeln auch eingehalten werden. In diesem Zusammenhang ist auch die Rolle zu betrachten, die die Selbstkontrolle spielt.

Was ist Selbstkontrolle?

Der Begriff „Selbstkontrolle" mag nicht für jeden dieselbe Bedeutung haben. Im Sinne dieser Unterlage beinhaltet ein Selbstkontrollkodex (oder jedes andere Instrument) alle Datenschutzbestimmungen, die auf eine Vielzahl von für die Verarbeitung Verantwortlichen in einer Berufsgruppe oder einem Wirtschaftsbereich Anwendung finden und deren Inhalt ursprünglich von Angehörigen des betreffenden Wirtschaftszweiges oder der betreffenden Berufsgruppe festgelegt wurde.

Diese weit gefasste Definition würde sowohl einen freiwilligen Datenschutzkodex am einen Ende der Skala einschließen, der von einem kleinen Wirtschaftsverband mit nur wenigen Mitgliedern entwickelt wurde, als auch den detaillierten Kodex von Standesregeln am anderen Ende, die für ganze Berufsgruppen wie Ärzte und Bankiers gelten und oft quasigerichtliche Kraft haben.

Ist das für den Kodex verantwortliche Gremium repräsentativ für den Sektor?

Wie aus diesem Kapitel hervorgeht, ist ein wichtiges Kriterium für die Beurteilung des Wertes eines Kodexes das Ausmaß, in dem seine Regeln durchgesetzt werden können. In diesem Zusammenhang ist die Frage, ob der für den Kodex zuständige Verband oder das zuständige Gremium alle Wirtschaftsteilnehmer in einem Sektor repräsentiert oder nur einen kleinen Prozentsatz von ihnen, wahrscheinlich von geringerer Bedeutung als die Stärke des Verbands im Hinblick auf seine Fähigkeit, beispielsweise seinen Mitgliedern wegen Nichterfüllung des Kodexes Sanktionen aufzuerlegen. Daneben gibt es allerdings einige Gründe, die branchen- oder berufsweite Kodizes mit klar abgegrenztem Geltungsbereich zu sehr viel nützlicheren Schutzinstrumenten machen als die, die von kleinen Unternehmensgruppierungen innerhalb von Wirtschaftssektoren entwickelt werden. Zunächst ist es eine Tatsache, dass aus der Sicht des Verbrauchers eine aufgespaltene und durch einige rivalisierende Verbände – mit jeweils eigenem Datenschutzkodex – gekennzeichnete Wirtschaft verwirrend ist. Das Nebeneinanderbestehen unterschiedlicher Kodizes schafft ein allgemeines Bild, dem es für die betroffene Person an Transparenz fehlt. Außerdem können sich insbesondere in Bereichen wie dem Direktmarketing, in denen regelmäßig personenbezogene Daten zwischen verschiedenen Unternehmen desselben Sektors ausgetauscht werden, Situationen ergeben, in denen das Unternehmen, das die personenbezogenen Daten weitergibt, nicht demselben Datenschutzkodex unterliegt wie das Unternehmen, das die Daten erhält. Dies führt hinsichtlich der anwendbaren Regeln zu einem beträchtlichen Maß an Unsicherheit und dürfte auch die Untersuchung und Bearbeitung von Beschwerden einzelner betroffener Personen außerordentlich erschweren.

Beurteilung der Selbstkontrolle – der Ansatz

Angesichts der Vielfalt der Instrumente, die unter den Begriff der Selbstkontrolle fallen, ist klar, dass zwischen den verschiedenen Formen der Selbstkontrolle je nach ihrer tatsächlichen Auswirkung auf das Niveau des Datenschutzes bei der Übermittlung personenbezogener Daten in ein Drittland zu differenzieren ist.

Grundlage für die Bewertung bestehender Datenschutzregeln muss (unabhängig davon, ob sie aufgrund von freiwilliger Selbstkontrolle oder von Vorschriften bestehen) der in Kapitel 1 vorgestellte generelle Ansatz sein. Ein Eckpunkt dieses Ansatzes ist die Prüfung nicht nur des Inhalts des Instruments (es sollte eine Reihe wesentlicher Grundsätze enthalten), sondern auch seine Effizienz im Hinblick auf:

- eine hohe allgemeine Befolgungsrate,
- Unterstützung und Hilfe für die einzelne betroffene Person,
- und, als entscheidenden Faktor, eine angemessene Entschädigung (einschließlich ggf. Schadensersatz).

Beurteilung des Inhalts eines Instruments der Selbstkontrolle

Dies ist eine relativ leichte Aufgabe. Es geht darum, sicherzustellen, dass die erforderlichen, in Kapitel 1 dargelegten inhaltlichen Grundsätze erfüllt sind. Das ist eine objektive Beurteilung. Die Frage ist, was der Kodex enthält, und nicht, wie er erstellt wurde. Die Tatsache, dass ein Wirtschaftszweig oder eine Berufsgruppe selbst die wichtigste Rolle bei der Ausarbeitung des Inhalts des Kodexes gespielt haben, ist an sich nicht relevant, obwohl es natürlich wahrscheinlicher ist, dass der Kodex die erforderlichen wesentlichen Grundsätze des Datenschutzes genauer wiedergibt, wenn die Meinungen der betroffenen Personen und der Verbraucherorganisationen

bei seiner Ausarbeitung berücksichtigt wurden. Die Transparenz des Kodexes ist ein Schlüsselelement; insbesondere sollte der Kodex in allgemein verständlicher Sprache abgefasst sein und konkrete Beispiele enthalten, die seine Bestimmungen veranschaulichen. Darüber hinaus sollte der Kodex die Offenlegung von Daten nicht angeschlossener Unternehmen verbieten, die nicht unter den Kodex fallen, wenn keine anderen angemessenen Schutzmaßnahmen vorgesehen sind.

Beurteilung der Effizienz eines Instruments der Selbstkontrolle

Die Bewertung der Effizienz eines bestimmten Selbstkontrollkodexes oder -instruments ist ein schwierigeres Unterfangen, das die Kenntnis der Mittel und Wege voraussetzt, durch die sichergestellt wird, dass man sich dem Kodex verpflichtet, und mit denen Probleme der Nichtbefolgung behandelt werden. Alle drei funktionellen Kriterien für die Beurteilung der Effizienz des Schutzes müssen erfüllt sein, wenn ein Selbstkontrollkodex bei der Bewertung der Angemessenheit des Schutzes berücksichtigt werden soll.

Gute Befolgungsrate

Ein Wirtschafts- oder Standeskodex wird normalerweise von einem repräsentativen Gremium des betreffenden Wirtschaftszweigs oder der betreffenden Berufsgruppe erstellt und gilt dann für die Mitglieder dieses speziellen repräsentativen Gremiums. Das Niveau der Einhaltung des Kodexes wird wahrscheinlich von der Bekanntheit seiner Existenz und seines Inhaltes unter den Mitgliedern, den zur Sicherstellung der Transparenz des Kodexes für die Verbraucher ergriffenen Schritten, mit denen ermöglicht werden soll, dass die Marktkräfte einen wirksamen Beitrag leisten, der Existenz eines Systems der externen Überprüfung (wie dem Erfordernis einer Überprüfung der Einhaltung in regelmäßigen Abständen) und, was vielleicht am wichtigsten ist, der Art und Durchsetzung von Sanktionen im Fall der Nichtbefolgung abhängen.

Wichtige Fragen sind deshalb:

- Welche Bemühungen des repräsentativen Gremiums sind erforderlich, um sicherzustellen, dass seine Mitglieder den Kodex kennen?
- Fordert das repräsentative Gremium von seinen Mitgliedern Nachweise darüber, dass sie die Bestimmungen des Kodexes umgesetzt haben? Wie oft?
- Ist ein solcher Nachweis von den angeschlossenen Unternehmen selbst vorgesehen oder kommt er von außen (z. B. von einem zugelassenen Wirtschaftsprüfer)?
- Untersucht das repräsentative Gremium mutmaßliche oder vermutete Verstöße gegen den Kodex?
- Ist die Einhaltung des Kodexes eine Voraussetzung für die Mitgliedschaft des repräsentativen Gremiums oder ist sie rein „freiwillig“?
- Welche Formen disziplinarischer Maßnahmen stehen dem repräsentativen Gremium zur Verfügung (Ausschluss u. Ä.), wenn ein Mitglied nachweislich gegen den Kodex verstoßen hat?
- Besteht für eine Person oder ein Unternehmen in der betreffenden Berufsgruppe oder dem betreffenden Wirtschaftszweig auch nach Ausschluss aus dem repräsentativen Gremium die Möglichkeit zur Weiterarbeit?

- Ist die Einhaltung des Kodexes mit anderen Mitteln durchsetzbar, beispielsweise auf gerichtlichem Wege oder durch eine spezielle Stelle? Standesrechtliche Kodizes haben in einigen Ländern Gesetzeskraft. Unter bestimmten Umständen könnte es möglich sein, die Durchsetzung von Branchenkodizes über allgemeine Gesetze zu lauteren Handelspraktiken oder auch zum Wettbewerb zu bewirken.

Bei der Prüfung der vorhandenen Sanktionsarten ist es wichtig, zwischen der „die Situation abstellenden“ Sanktion, die im Fall der Nichterfüllung von einem für die Verarbeitung Verantwortlichen lediglich fordert, seine Praktiken dahingehend zu ändern, dass sie dem Kodex entsprechen, und einer Sanktion, die weitergeht und den für die Verarbeitung Verantwortlichen für die Nichterfüllung tatsächlich bestraft, zu unterscheiden. Nur diese zweite Kategorie der „Strafsanktion“ wirkt sich tatsächlich auf das künftige Verhalten der für die Verarbeitung Verantwortlichen aus, indem sie einen gewissen Anreiz für die Erfüllung des Kodexes bietet.

Fehlen in einem Kodex tatsächlich abschreckende Strafmaßnahmen, so ist dies ein gravierender Nachteil. Ohne derartige Sanktionen ist schwer zu sehen, wie ohne ein striktes System externer Überprüfung (beispielsweise eine öffentliche oder private Stelle, die für die Intervention im Fall der Nichteinhaltung des Kodexes zuständig ist, oder eine zwingende Vorschrift für eine regelmäßige externe Prüfung) ein hohes Niveau allgemeiner Erfüllung erreicht werden kann.

Unterstützung und Hilfe für einzelne betroffene Personen

Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, dass der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben. Diese institutionelle Unterstützung sollte idealerweise neutral, unabhängig und mit den erforderlichen Befugnissen für die Prüfung jeder Beschwerde einer betroffenen Person ausgestattet sein. Im Hinblick auf die Selbstkontrolle ergeben sich in diesem Zusammenhang folgende Fragen:

- Existiert ein System, das die Prüfung von Beschwerden einzelner betroffener Personen ermöglicht?
- Wie erhalten betroffene Personen Kenntnis von diesem System und den Entscheidungen im Einzelfall?
- Entstehen der betroffenen Person Kosten irgendwelcher Art?
- Wer führt die Prüfung durch? Sind die Prüfer mit den erforderlichen Befugnissen ausgestattet?
- Wer entscheidet über eine mutmaßliche Verletzung des Kodexes? Sind diese Personen unabhängig und neutral?

Die Neutralität des Schiedsmanns oder Schiedsrichters bei mutmaßlichen Verletzungen des Kodexes ist ein Schlüsselelement. Eine solche Person oder ein solches Gremium darf zum Verantwortlichen der Verarbeitung in keinem Abhängigkeitsverhältnis stehen. Allerdings reicht dies allein noch nicht aus, um die Neutralität zu gewährleisten. Im Idealfall sollte der Schiedsrichter nicht der betroffenen Berufsgruppe oder dem betroffenen Wirtschaftszweig angehören, weil zwischen dem Verantwortlichen der Verarbeitung, der gegen den Kodex verstoßen haben soll, und den der gleichen Berufsgruppe oder dem gleichen Wirtschaftszweig angehörenden Mitgliedern eindeutig eine Interessengemeinschaft besteht. Die Neutralität des Schiedsgremiums könnte durch die Einbeziehung von Vertretern der Verbraucher neben den Vertretern der Wirtschaft (in gleicher Zahl) gewährleistet werden.

Angemessene Entschädigung

Wenn nachweislich gegen den Selbstkontrollkodex verstoßen wurde, sollten der betroffenen Person Rechtsmittel offen stehen, mit deren Hilfe das Problem behoben werden muss (Berichtigung oder Löschen aller fehlerhaften Daten; Gewährleistung, dass die Verarbeitung für unvereinbare Zweckbestimmungen eingestellt wird); wenn der betroffenen Person Schaden entstanden ist, muss die Zahlung einer angemessenen Entschädigung vorgesehen sein. Dabei ist zu berücksichtigen, dass „Schaden" im Sinne der Datenschutzrichtlinie nicht nur materiellen Schaden und finanziellen Verlust einschließt, sondern darunter auch jeglicher psychischer und moralischer Schaden fällt (im Recht des Vereinigten Königreichs und der USA als „distress" bezeichnet).

Viele der Fragen im Hinblick auf die oben im Abschnitt „Gute Befolgungsrate" aufgelisteten Sanktionen sind hier von Bedeutung. Wie bereits dargelegt wurde, haben Sanktionen eine doppelte Funktion: Den Täter zu bestrafen (und somit die Einhaltung der Regeln durch den Täter und andere zu fördern) und einen Verstoß gegen die Bestimmungen abzustellen. Hier geht es hauptsächlich um die zweite Funktion. Zusätzliche Fragen wären deshalb:

- Lässt sich überprüfen, ob ein Mitglied, das nachweislich gegen den Kodex verstoßen hat, seine Praktiken geändert und das Problem beseitigt hat?
- Können Personen nach dem Kodex eine Entschädigung erhalten und wie?
- Ist der Verstoß gegen den Kodex einem Vertragsverstoß gleichzusetzen oder auf dem Wege des öffentlichen Rechts geltend zu machen (beispielsweise Verbraucherschutz, unlauterer Wettbewerb), und kann das zuständige Gericht auf dieser Grundlage zur Leistung von Schadenersatz verurteilen?

Schlussfolgerungen

- Selbstkontrolle sollte unter Verwendung des objektiven, funktionellen Ansatzes beurteilt werden, der in Kapitel 1 dargelegt wurde.
- Ein Instrument der Selbstkontrolle, das als wirksamer Bestandteil eines „angemessenen Schutzes" anzusehen ist, muss für alle Mitglieder bindend sein, an die personenbezogene Daten übermittelt werden, und angemessene Sicherungsmaßnahmen vorsehen, wenn die Daten an Nichtmitglieder weitergeleitet werden.
- Das Instrument muss transparent sein und den grundlegenden Inhalt aller maßgeblichen Datenschutzgrundsätze enthalten.
- Das Instrument muss über Mechanismen verfügen, die ein gutes allgemeines Befolgungsniveau wirksam gewährleisten. Ein System abschreckender Strafmaßnahmen ist eine Möglichkeit, dies zu erreichen. Zwingende externe Prüfungen sind ein weiteres Mittel.
- Das Instrument muss Unterstützung und Hilfe für einzelne betroffene Personen bieten, die ein Problem im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten haben. Ein leicht zugängliches, neutrales und unabhängiges Gremium zur Anhörung von Beschwerden betroffener Personen und zur Schlichtung bei Verstößen gegen den Kodex muss deshalb eingerichtet werden.
- Das Instrument muss für den Fall der Verletzung von Vorschriften eine angemessene Entschädigung gewährleisten. Die betroffene Person muss die Möglichkeit haben, das Problem zu beseitigen und ggf. Schadensersatz zu erhalten.

Kapitel 4:

Die Rolle der vertraglichen Bestimmungen

1. Einführung

Nach Artikel 25 Absatz 1 der Datenschutzrichtlinie (95/46/EG) gilt der Grundsatz, dass die Übermittlung personenbezogener Daten lediglich erfolgen darf, wenn das Drittland ein angemessenes Schutzniveau gewährleistet. In diesem Kapitel soll die Möglichkeit einer Ausnahme von dem Grundsatz des angemessenen Schutzniveaus nach Artikel 25 geprüft werden, die aufgrund von Artikel 26 Absatz 2 möglich ist. Diese Bestimmung erlaubt einem Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau, „wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet". Weiter wird ausgeführt, dass „diese Garantien sich insbesondere aus entsprechenden Vertragsklauseln ergeben können". Wenn die Kommission nach dem Verfahren des Artikels 31 tätig wird, so befugt Artikel 26 Absatz 4 sie ferner zu beschließen, dass bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Artikel 26 Absatz 2 bieten.

Die Idee der Verwendung von Verträgen als Mittel der Regelung internationaler Übermittlungen personenbezogener Daten ist natürlich nicht erst durch die Richtlinie entstanden. Bereits 1992 waren der Europarat, die Internationale Handelskammer und die Europäische Kommission gemeinsam für eine Studie zu diesem Thema verantwortlich [„Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flow, with Explanatory Memorandum", gemeinsame Studie des Europarates, der Kommission der Europäischen Gemeinschaften und der Internationalen Handelskammer, Straßburg, 2. November 1992]. In jüngerer Zeit haben sich immer mehr Sachverständige und Kommentatoren in Studien und Artikeln zur Verwendung vertraglicher Bestimmungen geäußert – vielleicht, weil sie die ausdrückliche Bezugnahme in der Richtlinie festgestellt haben. Auch in der Praxis werden Verträge weiterhin als ein Mittel zur Behandlung von Datenschutzproblemen eingesetzt, die sich aus der Ausfuhr personenbezogener Daten aus bestimmten EU- Mitgliedstaaten ergeben. Seit Ende der 80er Jahre werden sie in Frankreich häufig verwendet, und in Deutschland fand jüngst das Beispiel der „BahnCard" große Beachtung, da ein Teil des Angebots auf der Einbeziehung der Citibank beruht [vgl. Darstellung dieses Falls durch Alexander Dix auf der Internationalen Konferenz der Datenschutzbeauftragten, September 1996 in Ottawa].

2. Die Verwendung von Verträgen als Grundlage für innergemeinschaftliche Datenflüsse

Vor der Prüfung der Anforderungen an vertragliche Bestimmungen im Rahmen von Datenströmen in Drittländer ist es wichtig, den Unterschied zwischen der Drittlandsituation und der Situation deutlich zu machen, bei der die Daten in der Gemeinschaft bleiben. Im letztgenannten Fall ist der Vertrag der Mechanismus, der verwendet wird, um die Aufteilung der Zuständigkeiten für den Datenschutz zu definieren und zu regeln, wenn mehr als eine Stelle an der fraglichen Datenverarbeitung beteiligt ist. Nach der Richtlinie trägt eine einzige Einheit, d. h. der „für die Verarbeitung Verantwortliche" die Hauptverantwortung für die Erfüllung der wesentlichen Grundsätze des Datenschutzes. Die zweite Einheit, der „Auftragsverarbeiter", ist lediglich für die Datensicherheit zuständig. Von einem „für die Verarbeitung Verantwortlichen" wird gesprochen, wenn eine Person die Entscheidungsbefugnis über die

Zweckbestimmung und die Mittel der Datenverarbeitung besitzt, während der „Auftragsverarbeiter“ lediglich die Stelle ist, die den Datenverarbeitungsdienst physisch erbringt. Die Beziehung zwischen den beiden wird durch Artikel 17 Absatz 3 der Richtlinie geregelt, der Folgendes festlegt:

Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere Folgendes vorgesehen ist:

- der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen,
- die in Absatz 1 genannten Verpflichtungen (die materiellrechtlichen Bestimmungen zur Datensicherheit) gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

Dies baut auf dem allgemeinen Grundsatz nach Artikel 16 auf, dem zufolge Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, sowie der Auftragsverarbeiter selbst personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten dürfen (es sei denn, es bestehen hierzu gesetzliche Verpflichtungen).

Bei der Übermittlung personenbezogener Daten in Drittländer wird normalerweise auch mehr als eine Partei beteiligt sein. Hier ist die betreffende Beziehung eine Beziehung zwischen der die Daten übermittelnden Stelle (dem „Übermittler“) und der Stelle, die die Daten im Drittland entgegennimmt (dem „Empfänger“). Daher sollte der Zweck des Vertrags unter anderem darin bestehen, die Verteilung der Zuständigkeit für die Einhaltung des Datenschutzes auf die beiden Vertragsparteien festzulegen. Der Vertrag muss jedoch noch weiteren Anforderungen entsprechen: Er muss zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, dass der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.

3. Das Ziel einer vertraglichen Lösung

Im Rahmen der Drittlandübermittlungen ist deshalb der Vertrag ein Mittel, um angemessene Garantien durch den für die Verarbeitung Verantwortlichen vorzusehen, wenn Daten aus der Gemeinschaft (und somit außerhalb des durch die Richtlinie und natürlich durch das allgemeine Regelwerk des Gemeinschaftsrechts vorgesehenen Schutzes [Die Wahrnehmung der Datenschutzrechte der Personen wird innerhalb der Gemeinschaft durch das allgemeine Regelwerk erleichtert, beispielsweise das Europäische Übereinkommen über die Übermittlung von Rechtshilfeersuchen »Straßburg 1977«]) in ein Drittland übermittelt werden, in dem kein angemessenes allgemeines Schutzniveau vorhanden ist. Eine Vertragsbestimmung, die diese Funktion erfüllen soll, muss einen befriedigenden Ausgleich für das Fehlen eines allgemein angemessenen Schutzniveaus bieten, indem sie die wesentlichen Elemente des Schutzes enthält, die in einer bestimmten Situation nicht vorhanden sind.

4. Die spezifischen Erfordernisse einer vertraglichen Lösung

Ausgangspunkt für die Bewertung der Bedeutung der „ausreichenden Garantien“ gemäß Artikel 26 Absatz 2 ist der Begriff des „angemessenen Schutzes“, auf den in

Kapitel 1 bereits recht ausführlich eingegangen worden ist. Er umfasst eine Reihe von Grundsätzen des Datenschutzes und drei weitere Voraussetzungen, ohne die diese wirkungslos blieben.

i. Die wesentlichen Datenschutzvorschriften

Das wichtigste Erfordernis der vertraglichen Lösung besteht darin, dass sie auf eine Verpflichtung der an der Übermittlung Beteiligten hinauslaufen muss, sicherzustellen, dass alle in Kapitel 1 dargelegten grundlegenden Bestimmungen des Datenschutzes bei der Verarbeitung von den in das Drittland übermittelten Daten gelten.

Diese Grundsätze sind:

- Der Grundsatz der Beschränkung der Zweckbestimmung
- Der Grundsatz der Datenqualität und -verhältnismäßigkeit
- Der Grundsatz der Transparenz
- Der Grundsatz der Sicherheit
- Die Rechte auf Zugriff, Berichtigung und Widerspruch
- Beschränkungen der Weiterübermittlung an Nichtvertragspartner

  [Weiterübermittlungen personenbezogener Daten vom Empfänger an einen anderen Dritten sind lediglich zulässig, wenn Mittel gefunden werden, den betreffenden Dritten vertraglich zu binden und damit den betroffenen Personen dieselben Garantien des Datenschutzes zu gewährleisten].

In bestimmten Situationen müssen zusätzliche Grundsätze, die sich auf sensible Daten, das Direktmarketing und automatisierte Entscheidungen beziehen, angewandt werden.

Der Vertrag sollte detailliert darlegen, wie der Empfänger der Datenübermittlung diese Grundsätze anzuwenden hat (d. h. Spezifizierung der Zweckbestimmungen, der Datenkategorien, Begrenzung der Speicherzeit, Sicherheitsmaßnahmen usw.). In anderen Fällen, wenn beispielsweise der Schutz in einem Drittland durch ein allgemeines Datenschutzgesetz vorgesehen ist, das der Richtlinie ähnelt, sind wahrscheinlich andere Mechanismen vorhanden, aus denen hervorgeht, auf welche Art und Weise die Datenschutzvorschriften in der Praxis Anwendung finden (Verhaltenskodexe, Notifizierung, beratende Funktion der Aufsichtsbehörde). Da dies bei vertraglichen Beziehungen nicht der Fall ist, kommt der Festlegung der Einzelheiten besondere Bedeutung zu, wenn die Übermittlung auf der Grundlage eines Vertrags erfolgt.

ii. Den wesentlichen Vorschriften Geltung verschaffen

In Kapitel 1 sind für die Beurteilung der Effizienz eines Datenschutzsystems drei Kriterien dargelegt. Dabei handelt es sich um die Fähigkeit des Systems:

- eine gute Befolgungsrate der Vorschriften zu bewirken,
- Unterstützung und Hilfe für die einzelne betroffene Person bei der Wahrnehmung ihrer Rechte zu sichern
- und – als besonders wichtiges Element – für eine angemessene Entschädigung des Geschädigten im Falle der Nichteinhaltung von Vorschriften zu sorgen.

Dieselben Kriterien müssen bei der Beurteilung der Effizienz einer vertraglichen Lösung gelten. Dies ist natürlich eine große, wenn auch zu bewältigende Herausforderung. Es geht darum, Mittel und Wege zu finden, um das Fehlen von Aufsichts- und Durchsetzungsmechanismen auszugleichen und der betroffenen Person, die vielleicht kein Vertragspartner ist, Hilfe, Unterstützung und letztendlich Entschädigung zu gewähren.

Jede dieser Fragen muss in allen Einzelheiten geprüft werden. Zur Erleichterung der Analyse werden sie hier in umgekehrter Reihenfolge behandelt.

Entschädigung für eine betroffene Person

Einer betroffenen Person mit Hilfe eines zwischen „Datenübermittler" und „Datenempfänger" abzuschließenden Vertrages die Möglichkeit des Rechtsbehelfs einzuräumen (d. h. das Recht auf eine durch einen unabhängigen Schiedsrichter beurteilte Beschwerde und gegebenenfalls das Recht auf eine Entschädigung) ist keine einfache Frage. Viel wird von der Art des gewählten Vertragsrechts sowie von dem auf den Vertrag anwendbaren einzelstaatlichen Recht abhängen. Normalerweise dürfte das anwendbare Recht das des Mitgliedstaats sein, in dem die übermittelnde Partei niedergelassen ist. Das Vertragsrecht einiger Mitgliedstaaten erlaubt die Begründung von Rechten Dritter, die in anderen Mitgliedstaaten nicht möglich ist.

Es gilt die allgemeine Regel, dass die Rechtssicherheit für die betroffene Person umso größer ist, je mehr der Empfänger im Hinblick auf seine Freiheit beschränkt ist, die Zweckbestimmungen, Mittel und Bedingungen zu wählen, unter denen er die übermittelten Daten verarbeitet. Da es ja hier um Fälle unangemessenen allgemeinen Schutzes geht, bestünde die beste Lösung darin, im Vertrag festzulegen, dass der Empfänger der Übermittlung im Hinblick auf die übermittelten Daten oder die Art und Weise, in der diese anschließend verarbeitet werden, keine eigene Entscheidungsbefugnis hat. Der Empfänger hat in diesem Fall allein nach Anweisung des Übermittlers zu handeln. So verbleibt beispielsweise die Entscheidungskompetenz über die Daten auch dann, wenn die Daten nach außerhalb der Europäischen Union übermittelt wurden, bei der Stelle, die die Übermittlung vorgenommen und ihren Sitz in der Gemeinschaft hat. Der Übermittler bleibt somit der für die Verarbeitung Verantwortliche, während der Empfänger lediglich ein Verarbeiter mit einem Subunternehmervertrag ist. Da die Aufsicht über die Daten durch eine in einem Mitgliedstaat der EU niedergelassene Aufsichtsbehörde ausgeübt wird, gilt das Recht des betreffenden Mitgliedstaats für die in dem Drittland erfolgte Verarbeitung weiter [aufgrund von Artikel 4 Absatz 1 Buchstabe a) der Richtlinie 95/46/EG]. Darüber hinaus ist der für die Verarbeitung Verantwortliche weiterhin nach dem Recht des Mitgliedstaats für jeden Schaden haftbar, der in Folge einer unzulässigen Verarbeitung entstanden ist [vgl. Artikel 23 der Richtlinie 95/46/EG].

Diese Art der Übereinkunft ist der nicht unähnlich, die bei der interterritorialen Vereinbarung gefunden wurde, mit der der zuvor erwähnte Fall von BahnCard und Citibank gelöst wurde. In der vertraglichen Vereinbarung sind dabei insbesondere im Hinblick auf die Datensicherheit detaillierte Festlegungen für die Datenverarbeitung getroffen worden, die alle anderen Nutzungen der Daten durch den Empfänger der Übermittlung ausschließen. Damit wurde gesichert, dass für die im Drittland erfolgende Datenverarbeitung deutsches Recht gilt und den betroffenen Personen Rechtsbehelfe offen stehen. [Obwohl für diesen Fall ein Gesetz galt, das vor der Richtlinie erlassen worden war, fand das Gesetz selbst nicht automatisch Anwendung auf alle Verarbeitungen, die durch einen in Deutschland niedergelassenen Verantwortlichen für die Datenverarbeitung kontrolliert wurden. Die Rechtsbehelfe für die betroffene Person wurden durch die Möglichkeit des deutschen Vertragsrechts geschaffen, Rechte Dritter zu begründen.]

Natürlich wird es Fälle geben, in denen eine solche Lösung nicht möglich ist. Möglicherweise erbringt der Empfänger der Übermittlung nicht nur einen reinen Datenverarbeitungsdienst für den Verantwortlichen mit Sitz in der Europäischen Union, sondern hat die Daten beispielsweise für eine Verwendung zum eigenen Nutzen oder für eigene Zwecke gemietet oder erworben. Unter diesen Umständen muss der Empfänger über einen gewissen Handlungsspielraum verfügen, um die Daten nach seinem Belieben zu verarbeiten, wodurch er selbst zu einem Verantwortlichen für die Daten wird.

In einem derartigen Fall kann man sich nicht auf die ständige automatische Anwendbarkeit der Rechtsvorschriften eines Mitgliedstaats und die fortgesetzte Schadenshaftung des Übermittlers der Daten stützen. Andere, komplexere Mechanismen müssen gefunden werden, um der betroffenen Person angemessene Rechtsbehelfe an die Hand zu geben. Wie bereits erwähnt, ist es in einigen Rechtssystemen für Dritte möglich, Vertragsrechte geltend zu machen, so dass dies genutzt werden könnte, um über einen offenen, veröffentlichten Vertrag zwischen Übermittler und Empfänger Rechte für betroffene Personen zu begründen. Die Position dieser Personen würde weiter gestärkt, wenn sich im Rahmen des Vertrages die Parteien selbst zu einer Art verbindlichen Schlichtung für den Fall verpflichten, dass die Vertragserfüllung durch eine betroffene Person angefochten wird. In den Selbstkontrollkodizes einiger Branchen sind derartige Schlichtungsmechanismen enthalten, und die Verwendung von Verträgen in Verbindung mit derartigen Kodexen wäre sicherlich nutzbringend.

Eine weitere Möglichkeit besteht darin, dass der Übermittler zum Zeitpunkt des Eingangs der ersten Daten der betroffenen Person eine gesonderte vertragliche Vereinbarung mit ihr abschließt und darin festlegt, dass er (der Übermittler) für jeden Schaden oder jede Notlage haftbar bleibt, die dadurch entsteht, dass der Empfänger einer Datenübermittlung das vereinbarte Paket an Grundprinzipien des Datenschutzes nicht einhält. Auf diese Weise verfügt die betroffene Person gegenüber dem Übermittler bei Verstößen durch den Empfänger über Rechtsmittel. Es ist dann Sache des Übermittlers, Maßnahmen wegen Vertragsbruchs gegen den Empfänger einzuleiten und etwaige Schadensersatzleistungen, zu deren Zahlung an die betroffene Person er genötigt war, anschließend von diesem zurückzufordern.

Diese ausgeklügelte dreiseitige Lösung ist vielleicht machbarer, als dies scheinen mag. Der Vertrag mit der betroffenen Person könnte Teil der Allgemeinen Geschäftsbedingungen werden, zu denen beispielsweise eine Bank oder ein Reisebüro ihren Kunden Dienstleistungen anbietet. Sie hat den Vorteil der Transparenz: Die betroffene Person wird über ihre Rechte voll informiert.

Schließlich könnte als Alternative zum Vertragsabschluss mit der betroffenen Person auch vorgesehen werden, dass ein Mitgliedstaat für Schäden, die infolge der Handlungen des Empfängers der Übermittlung entstehen, eine fortgesetzte Haftpflicht der für die Verarbeitung Verantwortlichen, die Daten nach außerhalb der Gemeinschaft übermitteln, gesetzlich niederlegt.

Unterstützung und Hilfe für betroffene Personen

Eine der Hauptschwierigkeiten betroffener Personen, deren Daten in den Bereich einer ausländischen Rechtsprechung übermittelt werden, ist das Problem, dass sie nicht in der Lage sind, die Ursache des betreffenden Problems, mit dem sie zu

kämpfen haben, zu finden, und deshalb nicht beurteilen können, ob die Vorschriften für den Datenschutz korrekt befolgt wurden oder ob Gründe für eine rechtliche Anfechtung bestehen. [Auch wenn einer betroffenen Person Rechte durch einen Vertrag gewährt werden, wird sie oft nicht beurteilen können, ob ein Vertragsbruch vorliegt, und wenn, durch wen. Dafür ist ein Untersuchungsverfahren außerhalb der formellen zivilrechtlichen Verfahren erforderlich.] Deshalb muss für ein angemessenes Schutzniveau eine Art institutioneller Mechanismus vorhanden sein, der eine unabhängige Untersuchung von Beschwerden ermöglicht.

Die Überwachungs- und Untersuchungsfunktion der Kontrollstelle eines Mitgliedstaats beschränkt sich auf die Datenverarbeitung, die im Hoheitsgebiet des Mitgliedstaats erfolgt [siehe Artikel 28 Absatz 1 der Richtlinie 95/46/EG]. Werden Daten in einen anderen Mitgliedstaat übermittelt, so gewährleistet ein System der gegenseitigen Unterstützung der Kontrollstellen, dass jede Beschwerde einer betroffenen Person in dem ersten Mitgliedstaat ordnungsgemäß bearbeitet wird. Erfolgt die Übermittlung in ein Drittland, besteht in den meisten Fällen eine solche Garantie nicht. Damit stellt sich die Frage, welche Art Ausgleichsmechanismus festgelegt werden kann, wenn die Datenübermittlung auf der Grundlage eines Vertrags erfolgt.

Eine Möglichkeit bestünde darin, die Aufnahme einer Vertragsklausel zu fordern, die der Kontrollstelle des Mitgliedstaats, in dem der Übermittler der Daten niedergelassen ist, ein Recht auf Einsichtnahme in die von dem Verarbeiter im Drittland vorgenommene Verarbeitung garantiert. Diese Einsichtnahme könnte in der Praxis durch einen gegebenenfalls von der Kontrollstelle ernannten Vertreter vorgenommen werden (beispielsweise eine spezialisierte Buchprüferfirma). Bei diesem Ansatz besteht allerdings das Problem, dass die Kontrollstelle im Allgemeinen keine Vertragspartei ist [die französische Delegation könnte sich Situationen vorstellen, in denen die Kontrollstelle Vertragspartner ist] und bei der Forderung nach Zugang der Vertrag somit in einigen Rechtssystemen nicht geltend gemacht werden kann. Eine andere Möglichkeit wäre eine gesetzliche Verpflichtung des Empfängers im Drittland unmittelbar gegenüber der entsprechenden Kontrollstelle des EU-Mitgliedstaats, mit der der Empfänger der Daten einwilligt, der Kontrollstelle oder einem benannten Vertreter im Fall einer vermuteten Nichterfüllung der Grundsätze des Datenschutzes den Zugang zu erlauben. Zu dieser Verpflichtung könnte auch gehören, dass die an der Datenübermittlung Beteiligten die Kontrollstelle über jede Beschwerde unterrichten, die sie von einer betroffenen Person erhalten. Bei einer derartigen Vereinbarung wäre die Existenz einer solchen Verpflichtung eine Voraussetzung, die erfüllt sein müsste, bevor die Datenübermittlung stattfinden kann.

Unabhängig von der gewählten Lösung bleiben große Zweifel im Hinblick auf die Frage bestehen, ob es zweckmäßig, praktikabel oder hinsichtlich der Ressourcen für eine Kontrollstelle eines EU-Mitgliedstaats auch wirklich machbar ist, die Zuständigkeit für eine Untersuchung und Überprüfung der Datenverarbeitung zu übernehmen, die in einem Drittland erfolgt.

Gewährleistung einer hohen Befolgungsrate

Auch wenn keine Beschwerde oder kein Problem einer betroffenen Person vorliegt, muss man darauf vertrauen können, dass die Vertragsparteien den Vertrag tatsächlich erfüllen. Das Problem bei der vertraglichen Lösung ist die Schwierigkeit, Sanktionen für die Nichterfüllung festzulegen, die so abschreckend sind, dass von ihnen die für das Herstellen dieses Vertrauens erforderliche Wirkung ausgeht. Auch in Fällen, in denen eine tatsächliche Kontrolle über die Daten weiterhin von innerhalb der Gemeinschaft ausgeübt wird, droht dem Empfänger der Übermittlung möglicherweise keine direkte Strafe, wenn er Daten in Zuwiderhandlung gegen den Vertrag verarbeitet. Stattdessen bliebe die Haftung bei dem in der Gemeinschaft niedergelassenen Übermittler der Daten, der dann mögliche Verluste in einer gesonderten Rechtshandlung gegen den Empfänger eintreiben müsste. Eine solche indirekte Haftung ist möglicherweise nicht ausreichend, um den Empfänger zu veranlassen, den Vertrag in allen Einzelheiten zu erfüllen.

Angesichts dessen wird es wahrscheinlich in den meisten Fällen notwendig sein, eine vertragliche Lösung durch zumindest die Möglichkeit einer Art externer Überprüfung der Verarbeitungstätigkeiten des Empfängers zu ergänzen, z. B. ein Audit durch ein zuständiges Gremium oder ein spezialisiertes Prüfungsunternehmen.

5. Das Problem des vorrangigen Rechts

Eine besondere Schwierigkeit beim vertraglichen Ansatz ist die Möglichkeit, dass die allgemeinen Rechtsvorschriften des Drittlands den Empfänger einer Datenübermittlung verpflichten, unter bestimmten Umständen personenbezogene Daten gegenüber dem Staat offen zu legen (Polizei, Gerichte oder Steuerbehörden), und dass derartige gesetzliche Erfordernisse meist Vorrang vor Verträgen haben, bei denen der Verarbeiter Vertragspartei ist. [Das Ausmaß der staatlichen Befugnis zur Forderung der Offenlegung von Informationen ist ebenfalls ein Punkt, der bei der allgemeinen Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland zu berücksichtigen ist.] Für Verarbeiter in der Gemeinschaft ist diese Möglichkeit in Artikel 16 der Richtlinie angesprochen, dem zufolge Auftragsverarbeiter personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten dürfen, es sei denn, es bestehen gesetzliche Verpflichtungen. Nach der Richtlinie müssen sich allerdings derartige Offenlegungen (die naturgemäß für Zweckbestimmungen erfolgen, die mit denen unvereinbar sind, für die die Daten erfasst wurden) auf solche beschränken, die in demokratischen Gesellschaften aus einem der Gründe der öffentlichen Sicherheit nach Artikel 13 Absatz 1 der Richtlinie erforderlich sind. Artikel 6 des Vertrags von Amsterdam garantiert die Einhaltung der in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten enthaltenen Grundrechte. In Drittländern mag es ähnliche Beschränkungen der Möglichkeiten des Staates, die Bereitstellung personenbezogener Daten von Unternehmen und anderen in ihrem Hoheitsgebiet tätigen Organisationen zu fordern, nicht immer geben.

Es gibt keine einfache Möglichkeit, diese Schwierigkeit zu überwinden. Damit wird lediglich illustriert, welche Grenzen der vertragliche Ansatz hat. In einigen Fällen ist ein Vertrag ein zu schwaches Instrument, um angemessene Garantien für den Datenschutz zu bieten, und Übermittlungen in bestimmte Länder sollten nicht genehmigt werden.

6. Praktische Erwägungen zur Verwendung von Verträgen

Aus der vorstehenden Analyse geht hervor, dass für jeden einzelnen Fall der Datenübermittlung eine detaillierte, den jeweiligen Erfordernissen angepasste Lösung gefunden werden muss. Diese Notwendigkeit der Festlegung von Einzelheiten im Hinblick auf die genauen Zweckbestimmungen und die Voraussetzungen, unter denen die übermittelten Daten verarbeitet werden, schließt die Möglichkeit der Erstellung eines Mustervertrags nicht aus, macht es aber erforderlich, jeden auf diesen Mustervertrag aufbauenden Vertrag entsprechend den besonderen Umständen des Einzelfalls zu ergänzen.

Die Analyse hat zudem ergeben, dass besondere praktische Probleme bei der Untersuchung der Nichterfüllung eines Vertrags bestehen, wenn die Verarbeitung außerhalb der Europäischen Union erfolgt und von dem betreffenden Drittland keine Kontrollstelle vorgesehen ist. Diese beiden Erwägungen laufen darauf hinaus, dass es Situationen geben wird, in denen eine vertragliche Lösung geeignet ist, und andere, in denen ein Vertrag die erforderlichen „angemessenen Sicherheiten" in keiner Weise garantieren kann.

Die notwendige detaillierte Anpassung von Verträgen an die Besonderheiten der jeweiligen Übermittlung impliziert, dass ein Vertrag besonders für Situationen geeignet ist, in denen ähnliche Datenübermittlungen wiederholt vorgenommen werden. Die Schwierigkeiten bei der Überwachung bedeuten, dass eine vertragliche Lösung dann äußerst effizient sein kann, wenn es sich bei den Vertragsparteien um bedeutende Wirtschaftsteilnehmer handelt, die bereits öffentlicher Prüfung und Regelung unterworfen sind [im Fall von Citibank und „BahnCard" arbeitete der Berliner Datenschutzbeauftragte mit den amerikanischen Bankaufsichtsbehörden zusammen]. Große internationale Netze, wie sie für Kreditkartengeschäfte und Flugbuchungen bestehen, weisen diese beiden Merkmale auf und stellen somit Situationen dar, für die Verträge sehr gut geeignet erscheinen. Unter diesen Umständen könnten sie sogar noch durch multilaterale Vereinbarungen ergänzt werden, von denen eine größere Rechtssicherheit ausgeht.

Auch wenn die an der Übermittlung Beteiligten ein und derselben Unternehmensgruppe angehören oder Tochtergesellschaften sind, dürfte aufgrund der engen Bindungen zwischen dem Empfänger im Drittland und der Einheit mit Sitz in der Gemeinschaft eine weitaus größere Möglichkeit zur Untersuchung der Nichterfüllung des Vertrags bestehen. Unternehmensinterne Übermittlungen sind deshalb ein weiterer Bereich, in dem es ein deutliches Potential für die Entwicklung effizienter vertraglicher Lösungen gibt.

Wichtige Schlussfolgerungen und Empfehlungen

- Verträge werden in der Gemeinschaft als Mittel zur Festlegung der Aufteilung der Zuständigkeit für die Erfüllung des Datenschutzes zwischen dem für die Verarbeitung Verantwortlichen und einem beauftragten Auftragsverarbeiter verwendet. Erfolgt bei Datenflüssen in Drittländer der Abschluss eines Vertrages, so muss dieser weiteren Anforderungen entsprechen: Er muss zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, dass der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.
- Die Grundlage für die Beurteilung der Angemessenheit der Sicherheitsmaßnahmen aufgrund einer vertraglichen Lösung entspricht der Grundlage für die Beurteilung der Angemessenheit des allgemeinen Schutzniveaus in einem Drittland. Eine vertragliche Lösung muss die wichtigsten Grundsätze des Datenschutzes und die Mittel umfassen, mit denen die Grundsätze durchgesetzt werden können.
- Im Vertrag sind die Zweckbestimmungen, die Mittel und Bedingungen, unter denen die Verarbeitung der übermittelten Daten zu erfolgen hat, genau festzulegen. Dies gilt auch für die Art und Weise, in der die grundlegenden Prinzipien des Datenschutzes anzuwenden sind. Die Rechtssicherheit für die betroffene Person ist umso größer, je mehr der Vertrag den Empfänger in seiner Freiheit beschränkt, die Daten ohne Kontrolle von außen im eigenen Namen zu verarbeiten. Der Vertrag sollte deshalb möglichst als ein Mittel verwendet werden, mit dem die die Daten übermittelnde Stelle die Entscheidungsbefugnis über die in dem Drittland erfolgende Verarbeitung behält.
- Verfügt der Empfänger im Hinblick auf die Verarbeitung der übermittelten Daten in gewissem Maße über eigene Entscheidungsgewalt, so ist die Situation nicht so eindeutig, und ein einfacher Vertrag zwischen den an der Übermittlung Beteiligten reicht dann möglicherweise als Grundlage für die Wahrnehmung der Rechte durch Betroffene nicht aus. Vielleicht wird ein Mechanismus benötigt, auf dessen Grundlage der übermittelnde Beteiligte in der Gemeinschaft für alle Schäden haftbar bleibt, die sich aus der in dem Drittland erfolgten Verarbeitung ergeben können.
- Weiterübermittlungen an Gremien oder Organisationen, die nicht durch den Vertrag gebunden sind, sollten vertraglich explizit ausgeschlossen werden, sofern es nicht möglich ist, derartige beteiligte Dritte vertraglich auf die Einhaltung derselben Datenschutzgrundsätze zu verpflichten.
- Das Vertrauen in die Befolgung der Grundsätze des Datenschutzes nach der Übermittlung von Daten wird gestärkt, wenn die Einhaltung des Datenschutzes durch den Empfänger der Übermittlung einer externen Überprüfung beispielsweise durch ein spezialisiertes Audit-Unternehmen oder ein Normungs-/Zertifizierungs-Gremium unterworfen ist.
- Im Fall eines Problems einer betroffenen Person, das sich vielleicht aus einem Verstoß gegen die vertraglich garantierten Datenschutzbestimmungen ergibt, stellt sich das allgemeine Problem der Sicherstellung der ordnungsgemäßen Prüfung der Beschwerde einer betroffenen Person. Bei der Durchführung einer solchen Prüfung durch die Kontrollstellen des EU-Mitgliedstaats wird es zu praktischen Problemen kommen.
- Vertragliche Lösungen sind wahrscheinlich am besten für große internationale Netze (Kreditkartengeschäfte, Flugbuchungen) geeignet, die durch große Mengen sich wiederholender Datenübermittlungen gleicher Art und eine relativ kleine Anzahl bedeutender Wirtschaftsteilnehmer in Branchen charakterisiert sind, die bereits in wesentlichem Umfang öffentlicher Prüfung und Regelung unterworfen sind. Unternehmensinterne Datenübermittlungen zwischen verschiedenen Zweigniederlassungen derselben Unternehmensgruppe sind ein weiterer Bereich, in dem es ein beträchtliches Potential für die Verwendung von Verträgen gibt.
- Länder, in denen beim Informationszugang die Befugnisse der staatlichen Behörden über das hinausgehen, was durch die weltweit angenommenen Normen des Schutzes der Menschenrechte erlaubt ist, sind keine sicheren Bestimmungsorte für Übermittlungen auf der Grundlage von Vertragsklauseln.

Kapitel 5:

Ausnahmen von der Anforderung der Angemessenheit

In Artikel 26 Absatz 1 der Richtlinie ist eine begrenzte Zahl von Fällen aufgeführt, in denen Ausnahmen vom Erfordernis der Angemessenheit für Übermittlungen in Drittländer zulässig sind. Diese enggefassten Ausnahmen betreffen überwiegend Fälle, in denen die Risiken für die betroffene Person relativ gering sind oder in denen andere Interessen (Wahrung eines wichtigen öffentlichen Interesses oder des

Arbeitspapiere der Datenschutzbeauftragten der EU

Interesses der betroffenen Person selbst) Vorrang vor dem Recht der betroffenen Person auf den Schutz der Privatsphäre genießen. Als Ausnahmen von der allgemeinen Regel müssen sie restriktiv ausgelegt werden. Zudem können die Mitgliedstaaten im innerstaatlichen Recht festlegen, dass die Ausnahmen in bestimmten Fällen nicht gelten. Dies trifft beispielsweise zu, wenn besonders schutzbedürftige Gruppen wie Arbeitnehmer oder Patienten zu schützen sind.

Bei der ersten Ausnahme muss die betroffene Person ihre Einwilligung ohne jeden Zweifel gegeben haben. Es sei darauf verwiesen, dass entsprechend der Definition in Artikel 2 Buchstabe h) der Richtlinie die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben worden sein muss. Das Erfordernis der Kenntnis der Sachlage ist insofern besonders wichtig, als damit verlangt wird, dass die betroffene Person über das konkrete Risiko der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau ordnungsgemäß in Kenntnis gesetzt werden muss. Geschieht dies nicht, so darf die Ausnahme nicht angewandt werden. Da die Einwilligung ohne jeden Zweifel erfolgen muss, führt jeglicher Zweifel daran, ob die Einwilligung tatsächlich gegeben worden ist, ebenfalls dazu, dass die Ausnahmeregelung nicht gilt. Damit würde auch in einer Vielzahl von Fällen, in denen die Einwilligung unterstellt wird (weil die betreffende Person beispielsweise auf die Übermittlung aufmerksam gemacht wurde und keinen Einwand dagegen erhoben hat), die Ausnahmeregelung nicht greifen. Von Nutzen dürfte die Regelung dann sein, wenn der Übermittler in direktem Kontakt mit der betroffenen Person steht, die erforderlichen Informationen problemlos mitgeteilt werden können und die Einwilligung ohne jeden Zweifel erlangt wird. Dies ist z. B. bei Übermittlungen im Rahmen eines Versicherungsschutzes häufig der Fall.

Die zweite und die dritte Ausnahme beziehen sich auf Übermittlungen, die erforderlich sind 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) oder zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll. Diese Ausnahmen erscheinen zunächst recht weitgefasst, doch wie die im Folgenden erörterte vierte und fünfte Ausnahme wird ihre Anwendung in der Praxis durch das Kriterium der Erforderlichkeit eingeschränkt: Die übermittelten Daten müssen ausnahmslos für die Erfüllung des Vertrages erforderlich sein. Werden also zusätzliche, nicht zu den wesentlichen Angaben zählende Daten übermittelt oder dient die Übermittlung nicht der Erfüllung des Vertrages, sondern einer anderen Zweckbestimmung (z. B. Nachfassmarketing), gilt die Ausnahme nicht. Was die vorvertraglichen Maßnahmen betrifft, so können dies nur von der betroffenen Person initiierte Situationen sein (wie die Anforderung von Informationen zu einem speziellen Dienst) und nicht solche, die sich aus den Marketingkonzepten der für die Verarbeitung Verantwortlichen herleiten.

Ungeachtet dieser Vorbehalte werden die zweite und die dritte Ausnahme nicht ohne Wirkung bleiben. So dürften sie etwa bei Übermittlungen für die Buchung eines Flugtickets für einen Passagier oder bei Übermittlungen personenbezogener Daten im Zusammenhang mit dem grenzüberschreitenden Zahlungsverkehr oder der Zahlung per Kreditkarte häufig angewandt werden. Die Ausnahmeregelung für Verträge „im Interesse der betroffenen Person“ (Artikel 26 Absatz 1 Buchstabe c) deckt speziell auch die Übermittlung von Daten an den Empfänger von Bankzahlungen ab, der, obwohl betroffene Person, meist keine Vertragspartei des Verantwortlichen ist, der die Übermittlung vornimmt.

Zur vierten Ausnahme gehören zwei Komponenten, von denen sich die erste auf Übermittlungen bezieht, die für die Wahrung eines wichtigen öffentlichen Interesses erforderlich oder gesetzlich vorgeschrieben sind. Hierzu mögen bestimmte begrenzte Übermittlungen zwischen öffentlichen Verwaltungen zählen, obwohl Vorsicht geboten ist, damit diese Bestimmung nicht zu weit ausgelegt wird. Dabei reicht ein einfaches öffentliches Interesse nicht aus, sondern es muss sich um ein wichtiges öffentliches Interesse handeln. Aus Punkt 58 geht hervor, dass die Datenübermittlung zwischen Steuer oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind, generell abgedeckt ist. Auch Übermittlungen zwischen den Kontrollstellen im Finanzdienstleistungssektor können unter diese Ausnahmeregelung fallen. Die zweite Komponente betrifft Übermittlungen, die im Rahmen internationaler Rechtsstreitigkeiten oder Gerichtsverfahren vorgenommen werden, und speziell Übermittlungen, die für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich sind.

Die fünfte Ausnahme bezieht sich auf Übermittlungen im Interesse der Wahrung lebenswichtiger Interessen der betroffenen Person. Ein einleuchtendes Beispiel wäre hier die dringende Übermittlung von medizinischen Unterlagen in ein Drittland, in dem ein zuvor in der EU behandelter Tourist in einen Unfall verwickelt ist oder sich eine gefährliche Erkrankung zugezogen hat. Allerdings wird in Punkt 31 der Richtlinie das „lebenswichtige Interesse“ recht eng als „für das Leben der betroffenen Person wesentliches Interesse“ ausgelegt. Ein Interesse aus finanziellen, eigentumsbezogenen oder familiären Gründen wäre im Normalfall ausgeschlossen.

Die sechste und letzte Ausnahme betrifft die Übermittlung aus einem Register, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind. Hinter dieser Ausnahme steht die Absicht, dass in Fällen, in denen ein Register in einem Mitgliedstaat zur Einsichtnahme durch die Öffentlichkeit oder Personen, die ein berechtigtes Interesse nachweisen können, offen steht, die Tatsache, dass die zur Einsichtnahme berechtigte Person in einem Drittland ansässig ist und der Vorgang der Einsichtnahme ohne Datenübermittlung unmöglich ist, die Übermittlung der Informationen nicht verhindert. Entsprechend Punkt 58 ist die Übermittlung der Gesamtheit oder ganzer Kategorien der im Register enthaltenen Daten nicht gestattet. Aufgrund dieser Einschränkungen darf diese Ausnahmebestimmung nicht als allgemeine Ausnahme für die Übermittlung der Daten aus öffentlichen Registern angesehen werden. So kann beispielsweise kein Zweifel darüber bestehen, dass die massenhafte Übermittlung von Daten aus öffentlichen Registern für kommerzielle Zwecke oder die Erfassung ganzer Bestände öffentlich zugänglicher Daten zum Zwecke der Erarbeitung von Profilen bestimmter Personen von den Ausnahmebestimmungen nicht abgedeckt sind.

Kapitel 6:

Verfahrensfragen

In Artikel 25 ist ein auf dem Einzelfall beruhendes Konzept vorgesehen, bei dem die Beurteilung der Angemessenheit sich auf die einzelne Datenübermittlung oder eine Kategorie von Datenübermittlungen bezieht. Dennoch ist natürlich klar, dass angesichts der enormen Anzahl der täglich aus der Gemeinschaft übermittelten personenbezogenen Daten und der zahllosen Akteure, die an den Übermittlungen beteiligt sind, kein Mitgliedstaat imstande ist, jeden einzelnen Fall im Detail zu prüfen,

welches System er für die Umsetzung von Artikel 25 auch wählt. [Von den Mitgliedstaaten können zur Erfüllung der Pflichten gemäß Artikel 25 unterschiedliche Verwaltungsverfahren festgelegt werden. Dazu gehört die direkte Verpflichtung des für die Verarbeitung Verantwortlichen ebenso wie die Einrichtung von Systemen zur vorherigen Genehmigung oder zur ExPost-Prüfung der Fakten durch die Kontrollstelle.] Dies heißt natürlich nicht, dass überhaupt keine Fälle einer gründlichen Kontrolle unterzogen werden, sondern dass Mechanismen zu entwickeln sind, mit denen der Entscheidungsprozess für eine große Anzahl von Fällen gestrafft wird, so dass die Entscheidung oder zumindest eine vorläufige Entscheidung ohne unnötige Verzögerung oder übermäßigen Aufwand getroffen werden kann.

Eine solche Rationalisierung ist unabhängig davon notwendig, wer die Entscheidung trifft – der für die Verarbeitung Verantwortliche, die Kontrollstelle oder eine sonstige vom Mitgliedstaat festgelegte Stelle.

i. Anwendung von Artikel 25 Absatz 6 der Richtlinie

Ein Beitrag zu einem rationelleren Verfahren bestünde, wie in der Richtlinie vorgesehen, in der Feststellung, dass bestimmte Drittländer ein angemessenes Schutzniveau gewährleisten. Derartige Feststellungen dienten „nur der Orientierung“ und würden daher Fälle unberührt lassen, in denen es zu besonderen Schwierigkeiten kommt. Doch zumindest würde das Problem praktisch angegangen.

Mit einer solchen Feststellung würde insbesondere für die Wirtschaftsteilnehmer ein Grad von Sicherheit hinsichtlich der Länder geboten, bei denen allgemein von der Gewährleistung eines „angemessenen“ Schutzniveaus ausgegangen werden kann. Zudem würde für Drittländer, die sich noch im Prozess der Entwicklung und Verbesserung der eigenen Schutzsysteme befinden, ein klarer und öffentlicher Anreiz gegeben. Würden obendrein mehrere solcher Feststellungen auf Gemeinschaftsebene getroffen, so wäre dies ein Beitrag zur Festlegung eines einheitlichen Ansatzes in dieser Frage, und es würde verhindert, dass von den Mitgliedstaaten bzw. den Datenschutzstellen unterschiedliche und womöglich einander widersprechende „weiße Listen“ erstellt werden.

Dieser Ansatz birgt natürlich auch Schwierigkeiten. An erster Stelle ist dabei der Aspekt zu nennen, dass viele Drittländer über keinen für alle Wirtschaftszweige einheitlich geltenden Schutz verfügen. So gibt es in vielen Staaten Datenschutzbestimmungen für den öffentlichen Sektor, jedoch nicht für die Privatwirtschaft. In einigen Ländern, beispielsweise in den USA, bestehen besondere Gesetze für bestimmte Bereiche (Meldung von Kreditaufnahmen, Unterlagen über die Ausleihe von Videos im Fall der USA), für andere hingegen nicht. Zusätzliche Schwierigkeiten existieren in Ländern mit Föderalstruktur wie den USA, Kanada und Australien, wo sich die Bestimmungen vielfach von Bundesstaat zu Bundesstaat unterscheiden. Wie die Bilanz zeigt, ist es derzeit nicht wahrscheinlich, dass bei vielen Drittländern generell von der Gewährleistung eines angemessenen Schutzniveaus ausgegangen werden kann. Dabei wäre die Aktion dem Anliegen, den für die Verarbeitung Verantwortlichen größere Sicherheit zu bieten, umso weniger dienlich, je kleiner die Anzahl der Länder, für die sich eine positive Feststellung treffen ließe. Weiterhin besteht die Gefahr, dass einige Drittländer die Versagung der Feststellung, dass sie ein angemessenes Schutzniveau bieten, als politische Provokation oder zumindest als politisch diskriminierend ansehen, da die Versagung der Feststellung ebenso durch das Versäumnis, die Bedingungen in dem Land überhaupt zu prüfen, wie im Ergebnis der Beurteilung des Datenschutzsystems zustande gekommen sein kann.

Nach sorgfältiger Abwägung dieser unterschiedlichen Argumente ist die Arbeitsgruppe dessen ungeachtet der Ansicht, dass es nützlich wäre, Arbeiten auf den Weg zu bringen, um die Lage zu erfassen und Feststellungen entsprechend Artikel 25 Absatz 6 zu treffen. Dabei würde es sich um einen kontinuierlichen Prozess handeln, der nicht in einer endgültigen Liste mündet, sondern in einer Liste, die in Abhängigkeit von den Entwicklungen ständig ergänzt und überarbeitet würde. Die positive Feststellung sollte dabei grundsätzlich nicht auf Länder mit horizontalen Datenschutzgesetzen beschränkt sein, sondern auch einzelne Sektoren innerhalb eines Landes umfassen, in denen das Datenschutzniveau angemessen ist, obwohl dies in anderen Sektoren desselben Landes nicht der Fall ist.

Es sei darauf verwiesen, dass der nach Artikel 29 eingesetzten Datenschutzgruppe im Zusammenhang mit Entscheidungen zu einer bestimmten Datenübermittlung oder bei der Feststellung der „Angemessenheit“ gemäß Artikel 25 Absatz 6 keine spezielle Rolle zufällt, da in beiden Fällen das in Artikel 31 genannte Ausschussverfahren zur Anwendung kommt. Eine der speziellen Aufgaben der Datenschutzgruppe nach Artikel 29 besteht jedoch darin, gegenüber der Kommission zum Schutzniveau in der Gemeinschaft und in Drittländern Stellung zu nehmen (siehe Artikel 30 Absatz 1 Buchstabe b). Somit gehören zum Zuständigkeitsbereich der Gruppe nach Artikel 29 durchaus auch die Beurteilung der Lage in bestimmten Drittländern und die Erarbeitung einer vorläufigen Position zum jeweiligen Schutzniveau. Um nicht wirkungslos zu bleiben, sind positive Feststellungen entsprechend Artikel 25 Absatz 6 möglichst breit bekannt zu machen. Wird andererseits festgestellt, dass ein Land nicht über ein angemessenes Schutzniveau verfügt, so bedeutet dies nicht unbedingt, dass es auf eine „schwarze Liste“ gesetzt werden müsste. Gegenüber der Öffentlichkeit müsste erklärt werden, dass es gegenwärtig nicht möglich ist, für das betreffende Land eine allgemeine Orientierung zu geben.

ii. Risikoanalyse konkreter Übermittlungen

Obwohl die Anwendung von Artikel 25 Absatz 6, wie sie hier beschrieben wurde, im Entscheidungsprozess bezüglich einer großen Anzahl von Datenübermittlungen eine wertvolle Hilfe ist, wird es häufig vorkommen, dass für das betreffende Land (ganz oder partiell) eine positive Feststellung nicht möglich ist. Die Art und Weise, in der die Mitgliedstaaten mit diesen Fällen umgehen, hängt davon ab, wie Artikel 25 von ihnen in einzelstaatliches Recht (siehe Fußnote auf der vorherigen Seite) umgesetzt wurde. Ist der Kontrollstelle eine konkrete Handlungsweise vorgegeben, d. h. Datenübermittlungen noch vor der eigentlichen Übermittlung zu genehmigen oder Prüfungen ex post facto im Nachgang vorzunehmen, dürfte es schon allein von der Menge der Übermittlungen her notwendig sein, für die Kontrollstelle ein System der Aufgabenschwerpunkte festzulegen. Ein solches System könnte aus einem vereinbarten Bündel bestimmter Kriterien bestehen, anhand derer eine Übermittlung oder Kategorie von Datenübermittlungen aufgrund der Tatsache, dass sie für die Privatsphäre des Einzelnen eine besondere Gefahr darstellen, als prioritär eingestuft werden könnte.

Selbstverständlich würde sich damit nichts an der Verpflichtung jedes einzelnen Mitgliedstaats ändern, dafür zu sorgen, dass nur solche Übermittlungen zulässig sind, bei denen der Drittstaat ein angemessenes Schutzniveau gewährleistet. Es bestünde also eine Orientierung in der Frage, welche Fälle der Datenübermittlung als „vorrangige Fälle“ für eine Prüfung oder sogar eine Untersuchung anzusehen sind. Damit würden auch die zur Verfügung stehenden Mittel in Richtung jener Übermittlungen gelenkt, die in puncto Schutz der betroffenen Personen besonderen Anlass zur Besorgnis geben.

Die Arbeitsgruppe ist der Ansicht, dass bei den folgenden Kategorien von Datenübermittlungen für den Schutz der Privatsphäre ein besonderes Risiko besteht und sie daher spezieller Aufmerksamkeit bedürfen:

- Übermittlungen, bei denen auch sensible Kategorien von Datenübermittlungen entsprechend der Definition von Artikel 8 der Richtlinie weitergegeben werden;
- Übermittlungen, mit denen die Gefahr finanzieller Schädigung verbunden ist (z. B. Kreditkartenzahlung über das Internet);
- Übermittlungen, mit denen eine Gefahr für die persönliche Sicherheit verbunden ist;
- Übermittlungen zum Zwecke einer Entscheidung von erheblicher Bedeutung für die betreffende Person (z. B. Entscheidung über die Einstellung oder Beförderung, über eine Darlehensgewährung usw.);
- Übermittlungen, mit denen der Betreffende ernsthaft in eine peinliche Lage gebracht werden kann oder sein Ruf beschädigt wird;
- Übermittlungen mit dem Ergebnis bestimmter Aktionen, die in bedeutendem Maße ein Eindringen in das Privatleben darstellen, z. B. unerwünschte Telefonanrufe;
- Wiederholte Übermittlungen großer Datenbestände (wie über Fernmeldenetze, das Internet u. Ä. verarbeitete Transaktionsdaten);
- Übermittlungen, bei denen unter Verwendung neuer Technologien Daten gesammelt werden und dies auf besonders verborgene oder heimliche Art geschieht (z. B. Internet-Cookies).

iii. Standardvertragsklauseln

Wie bereits in Kapitel 4 ausführlich dargestellt, ist in der Richtlinie die Möglichkeit vorgesehen, dass in den Fällen, in denen das Schutzniveau nicht angemessen ist, der für die Verarbeitung Verantwortliche durch Vertragsabschluss angemessene Sicherheitsmaßnahmen herbeiführen kann. Nach Artikel 26 Absatz 2 der Richtlinie können die Mitgliedstaaten Übermittlungen auf der Grundlage von Vertragsklauseln genehmigen, wobei die Kommission anschließend von dieser Entscheidung in Kenntnis gesetzt werden muss. Bestehen gegen die Genehmigung Einwände, so kann die Kommission die Entscheidung entsprechend dem in Artikel 31 bestimmten Ausschussverfahren aufheben oder bestätigen. Doch kann die Kommission nicht nur hinsichtlich der Genehmigungen durch die Mitgliedstaaten tätig werden, sondern darf nach Artikel 26 Absatz 4 der Richtlinie auch darüber befinden, ob bestimmte Standardvertragsklauseln ausreichende Garantien bieten, wobei sie auch hier nach dem Ausschussverfahren von Artikel 31 vorgehen muss. Diese Feststellungen sind dann für die Mitgliedstaaten bindend.

Angesichts der nicht zu übersehenden Kompliziertheit vertraglicher Lösungen und der damit verbundenen Schwierigkeiten besteht zweifellos das Erfordernis, den für die Verarbeitung Verantwortlichen, die auf diese Weise mit Verträgen zu arbeiten beabsichtigen, eine abgestimmte Orientierung an die Hand zu geben. Auf der Ebene der Mitgliedstaaten tragen wahrscheinlich die zuständigen staatlichen Stellen ein Großteil der Verantwortung für diese Orientierung, insbesondere im Zusammenhang mit Genehmigungen entsprechend Artikel 26 Absatz 2. Die Behörden der Mitgliedstaaten und die Kommission sollten zusammenarbeiten und ihre Ansichten zu den ihnen vorgelegten Vertragsklauseln austauschen. Für vorgeschlagene Standard-

vertragsklauseln, die den Behörden der Mitgliedstaaten oder direkt der Kommission vorgelegt werden, sollte ein Verfahren entwickelt werden, mit dem gewährleistet wird, dass diese Klauseln im Interesse der Verhinderung des Entstehens voneinander abweichender einzelstaatlicher Praktiken auch von der Arbeitsgruppe geprüft werden. Bei Entscheidungen gemäß Artikel 26 Absatz 4 könnte sich die Kommission damit auf den Rat der entsprechenden Sachverständigen stützen.

Anhang und Beispiele:

Artikel 25 und 26 der Richtlinie und ihre praktische Auswirkung auf die Übermittlung personenbezogener Daten in Drittländer

Einführung

Im Hauptteil dieser Arbeitsunterlage wird ein allgemeiner Ansatz für die Problematik der Datenübermittlung in Drittländer dargelegt und dabei auf Folgendes eingegangen:

- Einschätzung des angemessenen Schutzniveaus im Sinne von Artikel 25 der Datenschutzrichtlinie
- Einschätzung alternativer Möglichkeiten zur Herbeiführung angemessener Garantien mittels vertraglicher Lösungen, wie sie in Artikel 26 Absatz 2 vorgesehen sind;
- Einschätzung der Ausnahmen vom Erfordernis des angemessenen Schutzniveaus entsprechend Artikel 26 Absatz 1.

Die Darlegung der Probleme wäre jedoch unvollständig ohne eine Beschreibung der Art und Weise, wie sich der allgemeine Ansatz dann tatsächlich auf die Übermittlung personenbezogener Daten auswirkt. In diesem Anhang werden daher einige realistische (wenn auch fiktive) Fallbeispiele für die Übermittlung von Daten so geprüft, wie dies aller Wahrscheinlichkeit mit dem In-Kraft-Treten der einzelstaatlichen Gesetze zur Umsetzung der Richtlinie geschehen soll.

Es werden drei Fälle vorgestellt, bei denen im ersten Schritt jeweils zu bewerten ist, ob das Schutzniveau im Bestimmungsland aufgrund der geltenden Gesetze oder der bestehenden freiwilligen Selbstkontrolle im Privatsektor als angemessen gelten kann. Ist dies nicht der Fall, so besteht der zweite Schritt darin, unter den in Artikel 26 Absatz 1 (Ausnahmen) und 2 (vertragliche Lösung) angebotenen Möglichkeiten eine Lösung für das Problem zu ermitteln. Der dritte Schritt, die Verhinderung der Übermittlung, darf nur dann getan werden, wenn keine der Lösungen geeignet ist.

FALL 1:

Datenübermittlung zur Feststellung der Kreditwürdigkeit

Ein Bürger der Gemeinschaft möchte in Land A außerhalb der EG ein Ferienhaus kaufen und stellt bei einem Kreditinstitut in jenem Land einen Kreditantrag. Vom Kreditinstitut wird daraufhin eine Auskunftei mit einer entsprechenden Recherche beauftragt. Der Auskunftei liegt zu der betreffenden Person keine Akte vor, doch lässt sie sich alle Angaben über die bisherige Kreditaufnahme dieser Person von ihrer „Schwesterauskunftei“ im Vereinigten Königreich übermitteln. Bei Land A handelt es sich um ein fortgeschrittenes Industrieland mit seit langem bestehenden und stabilen demokratischen Institutionen. Das Justizsystem ist voll ausgebaut und arbeitet effektiv. Es handelt sich um einen föderal verfassten Staat.

ERSTER SCHRITT:
EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

Der für die Verarbeitung Verantwortliche unterliegt einem Bundesgesetz, das Vorschriften zu personenbezogenen Informationen zum Zwecke der Einschätzung von Kreditvergaberisiken enthält. Der für die Verarbeitung Verantwortliche behauptet zudem, eigene, öffentlich bekannt gemachte Datenschutznormen zu befolgen. Es ist keines der Gesetze der Teilstaaten anwendbar, und ein branchenweiter Selbstkontrollkodex besteht nicht.

Bewertung des Inhalts der anwendbaren Vorschriften

Zunächst sei vermerkt, dass die Mitteilung der im Vereinigten Königreich ansässigen Auskunftei wie jede andere Mitteilung an einen für die Verarbeitung Verantwortlichen im Vereinigten Königreich oder einem anderen Mitgliedstaat den normalen Anforderungen des Rechts des Vereinigten Königreichs unterworfen wäre, mit denen alle Artikel der Richtlinie mit Ausnahme der Artikel 25 und 26 umgesetzt werden. Dies ist deshalb so wichtig, weil sich dadurch die Prüfung der Rechtmäßigkeit der Mitteilung selbst erübrigt. Im Mittelpunkt der Aufmerksamkeit steht daher der Schutz der in das Land A übermittelten Daten.

Bei der Bewertung des Inhalts der Vorschriften sollte logischerweise mit der Bundesgesetzgebung begonnen werden. Werden hier Lücken festgestellt, so sind zunächst die „weniger strengen" Datenschutznormen des Unternehmens zu betrachten, um herauszufinden, ob die Lücken damit ausgefüllt werden. Danach wird eine Aufstellung zu den als notwendig erachteten inhaltlichen Punkten erarbeitet, und es wird beurteilt, ob die erforderlichen inhaltlichen Punkte im Gesetz oder in den Datenschutznormen des Unternehmens enthalten sind.

Der Grundsatz der Beschränkung der Zweckbestimmung kann in diesem Zusammenhang nur die Anforderung betreffen, dass die Sekundärnutzung und -offenlegung der übermittelten Daten mit der Zweckbestimmung, für die die Übermittlung erfolgte, nicht unvereinbar sein dürfen. Die Aufnahme der Daten in eine auf dem freien Markt zu verkaufende oder zu vermietende Versandliste dürfte ebenso als unvereinbar eingestuft werden wie die Offenlegung der Daten gegenüber potentiellen Arbeitgebern oder an der Solvenz der betroffenen Person interessierten Geschäftspartnern. Offenlegung der Daten gegenüber Kreditgebern (Banken, Kreditkartenunternehmen) könnte hingegen als vereinbar angesehen werden. Im hier geschilderten Fall ist im Bundesgesetz tatsächlich eine begrenzte Anzahl von Zweckbestimmungen festgelegt, bei denen die personenbezogenen Kreditinformationen legal offen gelegt werden können. Zu den Zweckbestimmungen gehören „Beschäftigung" und „rechtmäßige geschäftliche Erfordernisse im Zusammenhang mit einer geschäftlichen Transaktion, an der die betroffene Person beteiligt ist". Im letztgenannten Fall umfasst dies bestimmte Nutzungen der Daten für Marketingzwecke, die auch das Marketing von Waren oder anderen Leistungen als Kredite durch Dritte einschließen. Daraus ergibt sich, dass die Zweckbestimmung durch das Bundesgesetz nicht ausreichend begrenzt wird und das Schutzniveau in diesem Punkt nicht ausreicht. Auch die zum Schutz der Privatsphäre vom Unternehmen für sich festgelegten Datenschutznormen tragen nicht zur Verbesserung der Lage bei.

Nach dem Grundsatz der Transparenz müssten der betroffenen Person die Identität der Auskunftei in Land A und mögliche neue Zweckbestimmungen, für die die Daten verarbeitet werden sollen, mitgeteilt werden. Die Art und Weise, in der dies

geschieht, sollte der Vorgehensweise in Artikel 11 der Richtlinie vergleichbar sein. Im vorliegenden Fall kennt das Bundesgesetz keine speziellen Transparenzvorschriften, die unmittelbar die Auskunftei betreffen würden. Allerdings muss der Kreditgeber in Land A die betroffene Person davon in Kenntnis setzen, dass er sich zwecks Kreditinformationen an eine Auskunftei wenden wird, deren Namen und Anschrift er jedoch nicht zu nennen braucht. Für die betroffene Person ist also rechtlich nicht garantiert, dass sie darüber informiert wird, dass ihre Daten durch die betreffende Auskunftei verarbeitet werden. Da die Auskunftei mit der betroffenen Person nicht in direktem Kontakt steht, erschiene die Pflicht der Auskunftei zur Kontaktaufnahme mit der betroffenen Person mit dem speziellen Ziel ihrer Unterrichtung als „unverhältnismäßiger Aufwand" im Sinne von Artikel 11 der Richtlinie. Das Schutzniveau in Bezug auf Transparenz ist also offensichtlich ausreichend.

Der Grundsatz der Datenqualität und -verhältnismäßigkeit umfasst mehrere unterschiedliche Elemente. Im Bundesgesetz ist keine Einschränkung für die Sammlung und Verarbeitung unnötiger Daten vorgesehen. Zur Dauer der Datenspeicherung bestehen Vorschriften, mit denen die Verbreitung veralteter Informationen (mehr als zehn Jahre zurückliegende Urteile in Konkursverfahren) verhindert wird, was praktisch zur Löschung dieser Informationen führt. Zwar besteht rechtlich keine Auflage zur Führung korrekter Daten, doch stellt eine betroffene Person, die auf Antrag Zugang zu der sie betreffenden Kreditauskunft bekommen hat, einen Teil der Informationen in Frage, so sind als nichtzutreffend nachweisbare Daten zu löschen. Erneut scheint das Schutzniveau nicht in vollem Umfang angemessen, und auch die Datenschutznormen des Unternehmens gehen über die Regelungen im Bundesgesetz nicht hinaus.

Der Grundsatz der Sicherheit spiegelt sich im Bundesgesetz in dem Erfordernis wider, geeignete Maßnahmen gegen die unrechtmäßige Datenoffenlegung zu ergreifen. Aus den Datenschutznormen des Unternehmens geht hervor, dass zur Verhinderung des unberechtigten Zugriffs auf die Kreditinformationen und ihrer Manipulation ein strenges Kontrollsystem besteht. Hierzu werden sowohl technische Mittel (Passwörter usw.) eingesetzt als auch die Mitarbeiter entsprechend unterwiesen, wobei eine Verletzung dieser Pflicht zu disziplinarischen Maßnahmen führen kann. Damit wäre ein angemessenes Sicherheitsniveau gewährleistet.

Das Recht auf Zugriff und Berichtigung ist bundesrechtlich geregelt und mit dem Recht, wie es diesbezüglich in der Richtlinie besteht, vergleichbar. Wurde einer betroffenen Person der Kredit verwehrt, so ist die Einsichtnahme in die Auskunft kostenlos. Es besteht kein Recht auf Widerspruch, doch kann ein Betroffener Beschwerde bei der zuständigen Bundesbehörde einreichen oder Klage vor Gericht (siehe unten) erheben, wenn seine nach dem Bundesgesetz bestehenden Rechte verletzt wurden.

Sensible Daten zum Gesundheitszustand der betroffenen Person sind Teil der übermittelten Daten. Im Bundesgesetz sind strengere Vorschriften für die Verarbeitung von Informationen im Zusammenhang mit strafrechtlichen Verurteilungen sowie zu Geschlecht, Rasse, ethnischer Herkunft, Alter und Familienstand enthalten, nicht jedoch zu Informationen über den Gesundheitszustand. In den Datenschutznormen der Auskunftei ist jedoch festgelegt, dass bei Kreditauskünften keine Gesundheitsdaten weitergegeben werden, sondern nur bei Überprüfungen im Zusammenhang mit einer beabsichtigten Einstellung oder dem Abschluss einer Versicherung. In diesen beiden Fällen wird die Verwendung dieser Daten durch die betroffene Person auf den dazu erforderlichen Vordrucken genehmigt. Hier bestünde also für die in diesem Beispiel vorkommenden Gesundheitsdaten ein in der Sache verstärkter Schutz, auch wenn dieser Schutz vom Gesetz nicht vorgesehen ist.

Die Verwendung der Daten für Zwecke des Direktmarketing durch die Auskunftei (und die Offenlegung der Daten gegenüber anderen zu diesem Zweck) ist in diesem Zusammenhang ein wichtiger Punkt. Einer solchen Verwendung steht rechtlich nichts wirklich im Wege, und es gibt kein rechtliches Erfordernis, aus dem heraus dies verwehrt werden kann. Damit ist das Schutzniveau in diesem Punkt eindeutig unangemessen, da insbesondere in diesem Fall die Daten nicht nur durch die Auskunftei (zum Versand von Mailings an Kreditinstitute) verwendet werden, sondern auch gegenüber Dritten für das Vermarkten sowohl von finanztechnischen Produkten als auch branchenfremden Produkten wie Rasenmähern und Urlaubsangeboten offen gelegt werden.

Wie es scheint, kann angesichts der Zweckbestimmung der Übermittlung eine automatisierte Entscheidung darüber getroffen werden, ob der betroffenen Person ein Kredit gewährt werden soll. Für die betroffene Person müssen daher zusätzliche Garantien bestehen. Im Bundesgesetz gibt es Bestimmungen, mit denen die betroffene Person in der Auskunft enthaltene Informationen anfechten und der Auskunft erforderlichenfalls Erklärungen beifügen kann, aber es sind keine Regelungen vorgesehen, nach denen eine auf falschen oder unvollständigen Informationen beruhende Entscheidung angefochten, überprüft und, sollten sich die Einwände als berechtigt erweisen, geändert werden kann. Mit diesem Mechanismus können an einer Auskunft zwar Änderungen vorgenommen werden, um Probleme in der Zukunft zu vermeiden, doch wird das Problem einer bereits getroffenen Kreditentscheidung damit nicht unbedingt angesprochen. Dieser rückwirkende Rechtsschutz ist nicht ausreichend, da nicht vorhanden.

Beschränkungen der Weiterübermittlung der Daten an ein weiteres Drittland oder an Organisationen in anderen, den Vorschriften im Bundesgesetz nicht unterstellten Sektoren in Land A: Weder im Bundesgesetz noch in den Datenschutznormen des Unternehmens ist Derartiges vorgesehen.

Anwendungsbereich des Bundesgesetzes und der Datenschutznormen des Unternehmens: In einem weiteren Kontrollgang ist sicherzustellen, dass sowohl das Bundesgesetz als auch die Datenschutznormen des Unternehmens für die Daten aller betroffenen Personen und nicht nur für die Daten der Staatsangehörigen oder Bürger des Landes A gelten. Im vorliegenden Fall besteht eine solche Beschränkung des Anwendungsbereichs nicht.

Bewertung der Wirksamkeit des Schutzes

Das betreffende Bundesgesetz ist geltendes Recht, und nach seinen Bestimmungen ist auch eine öffentliche Stelle mit bestimmten externen Überwachungsbefugnissen eingerichtet worden. Zur Durchsetzung ihrer Rechte können die betroffenen Personen den Rechtsweg einschlagen. Allerdings ist die öffentliche Stelle nicht eindeutig dazu verpflichtet, sämtlichen Beschwerden von betroffenen Personen nachzugehen, und einigen Kommentatoren zufolge hat sie sich bei der Durchsetzung des Rechts auch nicht immer durch besondere Aktivität ausgezeichnet. Klagen vor Gericht zur Wiedergutmachung sind für die betroffenen Personen kostspielig und häufig auch zeitaufwendig – dies besonders dann, wenn die betroffene Person in einem anderen Land wohnt als in dem, wo das Gerichtsverfahren stattfindet.

Die Datenschutznormen des Unternehmens enthalten keinen eigenständigen Mechanismus, mit dem Betroffene ihre Rechte durchsetzen können, doch sind disziplinarische Strafen für Mitarbeiter vorgesehen, die die Grundsätze verletzen. Mehrere Beschäftigte sind bereits wegen entsprechender Vergehen disziplinarisch zur Verantwortung gezogen worden.

Die Kombination von gesetzlichen Regelungen und unternehmensinternen Datenschutznormen muss anhand der für die verfahrensrechtlichen Mechanismen festgelegten „Ziele“ bewertet werden. Im vorliegenden Fall könnten folgende Schlüsselfragen geprüft werden:

- Allgemein hohes Einhaltungsniveau

  Für das Unternehmen besteht der Hauptanreiz zur Einhaltung der eigenen Datenschutznormen in der Gefahr eines negativen Echos in der Presse, sollte festgestellt werden, dass es sich nicht an die eigenen Vorgaben hält. Zudem werden den Mitarbeitern des Unternehmens für den Fall der Verletzung der Sicherheitsvorschriften disziplinarische Maßnahmen angedroht. Indes reichen diese Mechanismen allein wahrscheinlich nicht aus, um die Einhaltung der Datenschutznormen in der Praxis zu gewährleisten. Diese Schlussfolgerung würde anders ausfallen, wenn:

  1. die Datenschutznormen des Unternehmens ihren Ausdruck in einem branchenweiten, vom Fachverband erarbeiten Verhaltenskodex gefunden hätten, nach dessen Bestimmungen ein Unternehmen, das gegen den Kodex verstößt, sofort aus dem Fachverband ausgeschlossen würde oder
  2. es nach einem allgemeinen Rechtsgrundsatz möglich wäre, von einer staatlichen Stelle gegen Unternehmen, die die eigenen veröffentlichten Datenschutznormen verletzen, wegen „unlauterer und betrügerischer“ Geschäftspraktiken strafrechtlich vorzugehen.

  Was das Bundesgesetz angeht, so wird die Einhaltung dadurch gefördert, dass vom Betroffenen im Falle der Nichteinhaltung Klage erhoben werden kann. Die Aussicht, vor Gericht auf der Anklagebank zu sitzen, dürfte auf den für die Verarbeitung Verantwortlichen einen gewissen abschreckenden Effekt ausüben. Allerdings ist die Wahrscheinlichkeit einer direkten externen Prüfung der Datenverarbeitungsverfahren sehr gering, da die staatliche Stelle erst reagiert, wenn sie beispielsweise durch den Beschwerdeführer oder die Presse darauf aufmerksam gemacht wird.

- Unterstützung und Hilfe für einzelne betroffene Personen

  Es ist eindeutig so, dass eine staatliche Stelle vorhanden ist, bei der betroffene Personen Beschwerde gegen die für sie erstellten Kreditauskünfte einlegen können. Die Kosten der Untersuchungen im Zusammenhang mit der Beschwerde braucht die betroffene Person nicht zu tragen.

- Angemessene Entschädigung

  Zwar hat im Falle der Verletzung der recht eng gefassten Regelungen im Bundesgesetz die betroffene Person die Möglichkeit, eine Wiedergutmachung auf dem Gerichtswege durchzusetzen, doch ist dies ein relativ kostspieliges Unterfangen, und häufig fehlt es hierbei an Unterstützung durch die staatliche Stelle. Das Gericht kann den für die Verarbeitung Verantwortlichen zur Leistung von Schadenersatz verurteilen (sofern es der Meinung ist, dass eine Schädigung erfolgte) und ihn anweisen, die Datenverarbeitungsverfahren und den Inhalt der betreffenden Kreditkartei zu ändern. Für die Verletzung der lediglich in den internen Datenschutznormen festgelegten Datenschutzgrundsätze ist eine solche Entschädigung nicht möglich.

Der Urteilsspruch

1. Etliche der Datenschutzgrundsätze, die im Diskussionspapier als „Kerngrundsätze" herausgearbeitet wurden, finden sich in der einen oder anderen Form im für die Kreditkartei geltenden Bundesgesetz, während andere in den Datenschutznormen des Unternehmens verankert sind. Doch auch wenn beide zusammen betrachtet werden, kann nicht behauptet werden, dass sämtliche „Kerngrundsätze" vorkommen. Selbst bei denen, die vorhanden sind (z. B. der Grundsatz der Beschränkung der Zweckbestimmung), sind einige nur in relativ abgeschwächter Form anzutreffen.
2. Hier ergibt sich als allgemeineres Problem die Frage, ob die Datenschutznormen des Unternehmens überhaupt als ausreichend wirksamer Mechanismus in Betracht gezogen werden können. Werden die Datenschutznormen nicht dadurch untermauert und durchsetzbarer gemacht, dass dem Fachverband oder einer staatlichen Stelle die Befugnis zur externen Kontrolle übertragen wird, so sind die Bestimmungen dieser Normen größtenteils nicht durchsetzbar und brauchen daher nicht berücksichtigt zu werden.
3. Auch wenn die zur Durchsetzung des Bundesrechts eingerichtete öffentliche Stelle nicht ganz mit denselben Befugnissen ausgestattet ist wie die typische Datenschutzbehörde in Europa, so bietet sich durch das Gesetz eine gewisse Rechtssicherheit, was insbesondere auf das gut funktionierende Rechtssystem und die „Prozesskultur" in Land A zurückzuführen ist. Das Gesetz enthält klar formulierte Vorschriften zum möglicherweise wichtigsten aller Datenschutzgrundsätze, dem Recht auf Zugriff und Berichtigung, und es grenzt die Zweckbestimmung der Datenverarbeitung in gewissem Maße ein.

Schlussfolgerung

Das Schutzniveau ist unangemessen, da das Gesetz zu wenige der „Kerngrundsätze" beinhaltet, und die unternehmensinternen Datenschutznormen sind für sich allein genommen kein wirksames Mittel zur Gewährleistung von Schutz. Der Urteilsspruch könnte auf Angemessenheit lauten, wenn das Gesetz in Richtung solcher Grundsätze wie Transparenz und Schutz von Daten zum Gesundheitszustand ausgebaut oder die unternehmensinternen Datenschutznormen mit Hilfe einer der vorgeschlagenen Methoden wirksamer gestaltet werden (d. h. Einhaltung als Voraussetzung für die Mitgliedschaft im Fachverband oder Bevollmächtigung einer staatlichen Stelle zur strafrechtlichen Verfolgung des Unternehmens wegen irreführender und betrügerischer Geschäftspraktiken im Falle der Verletzung der eigenen Datenschutznormen).

ZWEITER SCHRITT:
LÖSUNGSSUCHE

Von den in Artikel 26 Absatz 1 genannten möglichen Ausnahmen kommt nur der die Einwilligung der betroffenen Person betreffende Buchstabe a) in Frage. Die in Buchstabe b) geregelte Ausnahme im Interesse der Erfüllung eines Vertrags ist nicht anwendbar, da zwischen der übermittelnden Partei, der im Vereinigten Königreich ansässigen Auskunftei, und der betroffenen Person kein Vertragsverhältnis besteht. Auch kann schwerlich darauf verwiesen werden, dass die Übermittlung zur Erfüllung eines Vertrags „im Interesse der betroffenen Person" erforderlich sei, wie dies für die Ausnahme in Buchstabe c) geregelt ist.

Mit der Einwilligung durch die betroffene Person würde für das Problem jedoch eine relativ unkomplizierte Lösung gefunden. Die Einwilligung könnte entweder direkt durch die im Vereinigten Königreich ansässige Auskunftei oder in ihrem Auftrag durch das Kreditinstitut in Land A erlangt werden, das hierzu die betroffene Person auf dem Kreditantragsformular um Einwilligung ersuchen könnte. Unabhängig vom gewählten Verfahren sollte die betroffene Person von den konkreten Gefahren in Kenntnis gesetzt werden, die mit der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau verbunden sind.

Solange Übermittlungen dieser Art noch relativ selten sind, besteht die zweckmäßigste Methode wahrscheinlich darin, die Einwilligung jeweils einzeln einzuholen. Kommt es jedoch zu einem systematischeren weltweiten Datenaustausch mit Auskunfteien, so können andere Vorkehrungen, wie vertragliche Lösungen oder ein internationaler Verhaltenskodex, getroffen werden.

FALL 2:

Übermittlung sensibler Daten in der Luftfahrt

Ein portugiesischer Bürger bucht in einem Lissabonner Reisebüro einen Flug an Bord einer Maschine einer in Land B ansässigen Luftfahrtgesellschaft. Dabei wird u. a. erfasst, dass der Bürger behindert ist und einen Rollstuhl benutzt. Die Daten werden in ein internationales Computerreservierungssystem eingegeben und von dort durch die Fluggesellschaft in ihre Passagierdatenbank in Land B heruntergeladen, in der sie auf unbegrenzte Zeit gespeichert werden. Von der Fluggesellschaft werden die Daten abgesehen von internen Planungszwecken dazu verwendet, die Dienstleistung für den Passagier bei künftigen Flügen mit dieser Fluggesellschaft zu verbessern. [Dieser Fall weist gewisse Ähnlichkeiten mit einem tatsächlich geschehenen Fall auf, der schwedischem Recht unterliegt und in den amerikanische Fluggesellschaften und die Lufthansa verwickelt sind. Gegenwärtig läuft das Berufungsverfahren.]

ERSTER SCHRITT:
EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

In Bezug auf die Daten in der Datenbank der Fluggesellschaft in Land B bestehen keine Datenschutzbestimmungen, obwohl es für Daten in Computerreservierungssystemen einen internationalen Verhaltenskodex gibt.

Bewertung des Inhalts der anwendbaren Vorschriften

Es sind keine Vorschriften anwendbar.

Bewertung der Wirksamkeit des Schutzes

Nicht zutreffend.

Der Urteilsspruch

Das Schutzniveau in Land B ist insbesondere angesichts der Sensibilität der Daten nicht angemessen.

ZWEITER SCHRITT:

LÖSUNGSSUCHE

Die Übermittlung der Daten an das Computerreservierungssystem und ihre Verwendung durch die Fluggesellschaft zum Zwecke der Erbringung der entsprechenden Dienstleistung für den behinderten Passagier im Zusammenhang mit dem betreffenden Flug stellt eine Übermittlung dar, die für die Erfüllung des Vertrags zwischen dem Passagier und der Fluggesellschaft (Artikel 26 Absatz 1 Buchstabe b)) erforderlich ist. Für den weiteren Verbleib der Daten (einschließlich sensibler Daten zum Gesundheitszustand der betroffenen Person) in der Datenbank der Fluggesellschaft ist dies jedoch kein Grund. Folglich muss die Übermittlung der Daten an die Fluggesellschaft von einer anderen Ausnahmeregelung abgedeckt sein.

Wie in Fall 1 wäre die Einwilligung der betroffenen Person die beste Lösung. Sie könnte vom Reisebüro in Lissabon im Namen der Fluggesellschaft eingeholt werden. Dabei sollten der betroffenen Person die mit der Speicherung der Daten in Land B verbundenen Risiken ebenso mitgeteilt werden wie die Tatsache, dass die Übermittlung und die Speicherung der Daten in der Datenbank der Fluggesellschaft aus Gründen, die mit dem gebuchten Flug in Verbindung stehen, nicht erforderlich sind.

FALL 3:

Übermittlung von Daten für Marketinglisten

Ein Unternehmen in den Niederlanden ist auf die Erstellung von Versandlisten spezialisiert. Unter Verwendung der Vielzahl unterschiedlicher Quellen, die es in den Niederlanden für öffentliche Informationen gibt, sowie von Kundenverzeichnissen von anderen niederländischen Unternehmen entstehen Listen, in denen Personen aufgeführt sind, die einem bestimmten sozio-ökonomischen Profil entsprechen. Verkauft werden diese Listen an die Kunden dieser Firma nicht nur in den Niederlanden und der EU, sondern auch in zahlreichen Drittländern. Die Empfängerunternehmen nutzen die Listen (in denen die Postanschrift, die Telefonnummer und häufig auch die E-mail-Adresse angegeben sind), um mit den in den Listen aufgeführten Personen in Kontakt zu treten und ihnen die unterschiedlichsten Erzeugnisse und Dienstleistungen zu verkaufen. Sehr viele der auf den Listen genannten Personen haben bei der niederländischen Datenschutzbehörde Beschwerde gegen die Marketingangebote eingelegt.

Die geltenden Vorschriften

Einige der Unternehmen, die die Versandlisten der niederländischen Firma kaufen, sind in Ländern ansässig, in denen allgemeine gesetzliche Datenschutzvorschriften gelten, die das Recht der betroffenen Personen beinhalten, die Entgegennahme von Marketingangeboten zu verwehren. Andere befinden sich in Ländern ohne derartige gesetzliche Regelungen, sind jedoch Mitglied von Selbstkontrollvereinigungen, von denen Datenschutzkodizes erarbeitet worden sind. Weitere Firmen unterliegen überhaupt keinen Datenschutzvorschriften.

Bewertung des Inhalts der anwendbaren Vorschriften

In diesem Fall müssten zahllose Gesetze und Kodizes bewertet werden. Bleibt die in den Niederlanden ansässige Firma ihrem Grundsatz treu, ihre Listen an Unternehmen in jedem beliebigen Land der Welt zu verkaufen bzw. zu vermieten, so kommt es zwangsläufig zu Situationen, in denen das Schutzniveau nicht angemessen ist.

ZWEITER SCHRITT:

LÖSUNGSSUCHE

Im vorliegenden Beispiel wäre es für die niederländische Firma kaum möglich, die Einwilligung jeder einzelnen Person zur Aufnahme in die Versandlisten zu erlangen, da die Daten aus öffentlichen Quellen stammen und ohne direkten Kontakt mit der betroffenen Person erfasst wurden. Es ist daher nicht wahrscheinlich, dass hier eine der Ausnahmen von Artikel 26 Absatz 1 greift.

Der niederländischen Firma stehen zwei Möglichkeiten offen, die sie alternativ oder im Verbund nutzen kann. Zum einen könnte sie den Handel mit den Versandlisten auf Unternehmen in Ländern begrenzen, in denen aufgrund von gesetzlichen Regelungen bzw. entsprechenden Instrumenten der freiwilligen Selbstkontrolle eindeutig feststeht, dass ein angemessenes Schutzniveau gewährleistet ist. Bei der Entscheidung könnte sich die Firma an möglicherweise bestehenden „weißen Listen“ orientieren.

Als zweite Möglichkeit könnten von allen Kunden (oder zumindest von den Kunden in Ländern mit unangemessenem“ Schutzniveau) vertragliche Verpflichtungen hinsichtlich der übermittelten Daten gefordert werden. Bei den vertraglichen Regelungen sollten die in Kapitel 4 des Haupttextes gegebenen Hinweise befolgt werden. Insbesondere sollte dabei gesichert werden, dass die niederländische Firma gemäß niederländischem Recht für alle Verletzungen der Datenschutzgrundsätze seitens der Empfängerunternehmen der übermittelten Versandlisten haftbar bleibt.

Mit einer solchen vertraglichen Lösung würde bei ordnungsgemäßer Umsetzung ein Beitrag zur Überwindung des Handelshemmnisses geleistet, das das Fehlen eines angemessenen Schutzniveaus in bestimmten Drittländern darstellt.

Geschehen zu Brüssel, 24. Juli 1998

Für die Arbeitsgruppe

Der Vorsitzende

P. J. HUSTINX

D. Beschlüsse der International Working Group on Data Protection in Telecommunications

Gemeinsamer Standpunkt zu Datenschutz bei Suchmaschinen im Internet

angenommen auf der 23. Sitzung in Hong Kong SAR, China

15. April 1998

– 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 in den letzten Jahren immer beliebter geworden.

Mit diesen Suchmaschinen kann man auch nach personenbezogenen Daten suchen. Als Ergebnis erhält man ein Profil der Aktivitäten der gesuchten Person auf dem 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.

Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit 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. Darüber hinaus könnte die geplante Einführung von Filterprogrammen für Datenschutzzwecke zu weiteren Gefährdungen führen, falls die Datenschutzpräferenzen, die vom Benutzer in diesen Programmen festgelegt werden, von Suchmaschinen überwacht werden. Die Arbeitsgruppe empfiehlt daher, dass jedes Filterprogramm so konstruiert sein muss, dass die Datenschutzpräferenzen der Nutzer nicht durch die Betreiber von Websites oder Dritten überwacht und aufgezeichnet werden können.

Schließlich erinnert die Arbeitsgruppe im Hinblick auf übermittelte oder veröffentlichte personenbezogene Daten an zwei Prinzipien, auf die sich ihr gemeinsamer Standpunkt stützt:

- auch personenbezogene Daten, die der Nutzer freiwillig veröffentlicht hat, unterliegen den für sie geltenden Schutzbestimmungen;
- der Einzelne sollte in jedem Fall und zu jedem Zeitpunkt das Recht haben, der Veröffentlichung seiner personenbezogenen Daten in einem Internet-Angebot zu widersprechen. Er oder sie sollte das Recht haben zu verlangen, dass der Zweck respektiert wird, für den die Daten veröffentlicht worden sind.

Empfehlungen

Die Arbeitsgruppe hat bereits in der Vergangenheit auf die mit der Nutzung des Internets verbundenen Datenschutzprobleme hingewiesen und Empfehlungen zu Möglichkeiten, diese Probleme zu lösen, ausgesprochen. Die Regulierungsbehörden

könnten das Angebot von Suchmaschinen auf die Suche nach Namen beschränken und die Abfrage von ausufernden und komplexen Suchprofilen verbieten. Allerdings dürfte es aufgrund der internationalen Struktur des Internets unmöglich sein, das Netz umfassend durch gesetzliche Maßnahmen zu regulieren.

Die Nutzer des Internets können gleichzeitig auch Informationsanbieter sein. Sie sollten sich darüber im Klaren sein, dass jedes personenbezogene Datum, das sie auf dem Netz publizieren (z. B. bei der Einrichtung ihrer eigenen Homepage, einem bei den großen Online-Diensteanbietern üblichen Angebot), von Dritten für die Erstellung eines Profils genutzt werden kann. Die Nutzer sollten die Möglichkeit haben, die Nutzung ihrer Daten auf bestimmte Zwecke zu beschränken.

Darüber hinaus können mit Suchmaschinen auch Nachrichten, die in News Groups eingestellt worden sind, durchsucht werden, womit den Profilen weitere Informationen darüber hinzugefügt werden können, wer welche Meinung über welchen Sachverhalt geäußert hat. Eine Möglichkeit, diese Gefährdung der Privatsphäre zu minimieren, könnte in der Nutzung von Pseudonymen bei der Teilnahme an News-Diensten bestehen. Daher sollten Diensteanbieter und Softwarehersteller im Internet ihren Nutzern solche Pseudonymdienste anbieten. Die Nutzung solcher Dienste könnte auch die Bedrohung für die Privatsphäre des Nutzers minimieren, da die Erstellung eines Profils über seine oder ihre Interessen dann unmöglich wäre. Gleichzeitig sollten die Nutzer auf das Risiko aufmerksam gemacht werden, das sie eingehen, wenn sie an News-Diensten unter ihrer echten E-mail-Adresse oder sogar ihrem wirklichen Namen teilnehmen.

Die Nutzer sollten darüber hinaus in die Lage versetzt werden, Teile ihrer eigenen Informationsangebote auf dem Netz gegen die Überwachung durch Suchmaschinen zu schützen. Dies kann durch das Setzen einer „no-robots"-Option in ihrem Website-Programm erreicht werden. Allerdings setzt die Wirksamkeit dieser Einrichtung voraus, dass sie von den Anbietern von Suchmaschinen beachtet wird.

In dem Vertrag oder der Übereinkunft, die zwischen dem Betreiber einer Suchmaschine und dem Benutzer geschlossen wird, sollte festgelegt werden, dass der Betreiber sich an die Richtlinie zum Schutz personenbezogener Daten der Europäischen Union hält. Aussagen wie: „Der Betreiber der Suchmaschine wird keine Informationen über den Suchvorgang oder den Benutzer der Suchmaschine speichern. Nach Beendigung der Suche bleiben keine Daten gespeichert" sollten in den Vertrag aufgenommen und umgesetzt werden.

Im Hinblick auf die Notwendigkeit, die Konformität von Suchmaschinen mit den grundlegenden Prinzipien des Datenschutzes herzustellen, ist eine Möglichkeit zur Kontrolle erforderlich. Die genauen Methoden dafür (z. B. Auditing, Evaluierung, Zertifizierung) sollten in einer Studie untersucht werden, die unterschiedliche Situationen berücksichtigt.

Zum Schutz der Privatsphäre der Benutzer ist der umfassende Einsatz von datenschutzfreundlichen Technologien erforderlich, wo dies möglich ist. Auf Wunsch des Benutzers muss ein technisches Mittel zum Schutz seiner Identität verfügbar sein, das vollständige Anonymität während der Suche ermöglicht. Der Austausch von Daten muss in technischer Hinsicht dem Prinzip der Angemessenheit entsprechen, wie es in den Leitlinien der OECD von 1980 und der Richtlinie der Europäischen Union von 1995 festgelegt ist.

Um eine Analyse des Datenverkehrs zu verhindern, sollten konventionelle Sicherheitsmaßnahmen wie die permanente Übertragung zufällig generierter Zeichenfolgen angewandt werden.

Gemeinsamer Standpunkt im Hinblick auf Invert-Suche in Teilnehmerverzeichnissen

angenommen bei der 23. Sitzung in Hong Kong SAR, China

15. April 1998

– Übersetzung –

Inverse Verzeichnisse werden durch Verarbeitung personenbezogener Daten aus Teilnehmerverzeichnissen erzeugt. Die Nutzung inverser Verzeichnisse zur Erlangung der Identität und der Adresse einer Person aufgrund einer Telefon- oder Telefax-Nummer oder einer E-mail-Adresse kann erhebliche negative Auswirkungen auf den Datenschutz haben und sollte daher spezifischen Regelungen zum Schutz des Persönlichkeitsrechts unterliegen.

In einigen Staaten existieren Regelungen, die den auf ihrem Territorium ansässigen Anbietern von Telekommunikation das Angebot von inversen Verzeichnissen verbieten. In diesem Zusammenhang stellen die Teilnehmer an der Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 14. und 15. April 1998 in Hong Kong fest, dass

- die Existenz inverser Verzeichnisse ohne spezielle Schutzvorschriften zur Gefährdung des Datenschutzes im Rahmen privater Beziehungen zwischen Personen führen kann;
- die kommerzielle Nutzung inverser Verzeichnisse möglicherweise schädliche Konsequenzen für Personen haben kann, die ausschließlich ihre Telefonnummer angeben wollten, insbesondere im Zusammenhang mit Kleinanzeigen in Zeitungen;
- der Zweck eines inversen Verzeichnisses nicht identisch mit dem Zweck eines Telefonverzeichnisses ist; mit einem Telefonverzeichnis ist es möglich, die Telefonnummer einer bekannten Person auf Grundlage ihres Namens und eines geographischen Kriteriums zu erhalten, während der Zweck eines inversen Verzeichnisses in der Suche nach der Identität und der Adresse von Teilnehmern besteht, bei denen nur die Telefonnummer bekannt ist;
- Teilnehmer das Recht haben müssen, nicht in Telefonverzeichnisse aufgenommen zu werden oder der kommerziellen Nutzung ihrer Daten zu widersprechen, wie dies bereits in der Gemeinsamen Erklärung der Arbeitsgruppe bei ihrer Sitzung in Berlin im Jahre 1989 dargelegt wurde. Dass eine Person, der nur die Telefonnummer des Teilnehmers bekannt ist, dessen Adresse und Identität durch Nutzung eines inversen Verzeichnisdienstes erhält, sollte nur mit Einwilligung des Teilnehmers möglich sein;
- obwohl das Umsortieren in ein inverses Verzeichnis in manchen Fällen legitimen Interessen dienen kann, wie dem Schutz von Menschenleben oder der öffentlichen Sicherheit, die regelmäßige Bekanntgabe der Identität und der Adresse eines Teilnehmers auf der Basis seiner Telefonnummer eine unzulässige Erhebung von Informationen darstellt, wenn die Teilnehmer der Bekanntgabe ihrer Daten durch einen solchen Dienst nicht im Vorhinein widersprechen konnten;
- auch die Verarbeitung von Abrechnungsdaten, Einzelverbindungsnachweisen oder der Anzeige der Nummer des Anrufenden im Hinblick auf die Möglichkeit zur Invert-Suche oder von inversen Verzeichnissen analysiert werden muss.

Sie stimmen darin überein, dass, wo inverse Verzeichnisse nicht durch Gesetz verboten sind,

- diese Dienste eine ausdrückliche freiwillige Einwilligung erfordern. Wenigstens ein Widerspruchsrecht und das Recht auf Auskunft, die generell von existierenden nationalen und internationalen Regelungen über den Schutz personenbezogener Daten anerkannt sind, sollten garantiert werden;
- es in jedem Fall notwendig ist, den Teilnehmern bei der Datenerhebung ein Recht auf Information durch die Anbieter von Telefon- oder E-mail-Diensten über die Existenz von Diensten zur Invert-Suche einzuräumen. Falls die ausdrückliche Einwilligung nicht erforderlich ist, müssen die Teilnehmer das Recht zum Widerspruch haben und auf dieses Recht hingewiesen werden.

Gemeinsamer Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation

angenommen bei der 23. Sitzung in Hong Kong SAR, China

15. April 1998

– Übersetzung –

1. Während der Einzelne die vertrauliche Behandlung seiner privaten Kommunikation erwarten können muss, können andere öffentliche Interessen in bestimmten Fällen das Abhören durch die zuständigen Behörden rechtfertigen.

2. Das Abhören sollte nur unter besonderen Umständen erlaubt sein, wo es aufgrund schwerer Verbrechen gerechtfertigt ist, und angemessenen Schutzmaßnahmen unterliegen – wie der richterlichen Anordnung, der Benachrichtigung der Betroffenen, Beschränkungen der Nutzung und Anforderungen an die Vernichtung von Tonbändern und Protokollen. (Dieses Papier behandelt weder diese Angelegenheiten noch Fälle, in denen das Abhören möglicherweise für den technischen Betrieb von Netzen oder Zwecke der Regulierungsbehörden erforderlich ist.)

3. Das autorisierte Abhören muss notwendigerweise ohne das vorherige Wissen der Betroffenen ausgeführt werden. Allerdings sollten zur Einhaltung der Prinzipien der Offenheit, der Transparenz und der Verantwortlichkeit Mechanismen geschaffen werden, um die Öffentlichkeit zu versichern, dass die Möglichkeit zum Abhören gesetzmäßig, angemessen und verhältnismäßig genutzt wird.

4. Solche Mechanismen sollten einschließen:
   - das Führen von Protokollen
   - Überwachung und Kontrolle
   - regelmäßige öffentliche Berichterstattung.

5. *Protokollierung:*
   Behörden, die Abhörmaßnahmen durchführen, sollten angemessene Protokolle zum Nachweis der gesetzlichen Befugnis und der Rechtmäßigkeit jeder Abhörmaßnahme führen. Die Verpflichtung zur Führung von Protokollen könnte auch auf die beteiligten Anbieter von Telekommunikationsdiensten ausgedehnt werden.

6. *Überwachung und Kontrolle:*
   Einer Einrichtung, die unabhängig von der untersuchenden Behörde ist, sollte die Aufgabe zugewiesen werden, die Einhaltung der Abhörgesetze zu überprüfen; sie sollte die notwendigen Befugnisse, Möglichkeiten und Ressourcen haben, Untersuchungen durchzuführen.

7. *Öffentliche Berichterstattung:*
   In regelmäßigen Abständen sollten Übersichten öffentlich zugänglich gemacht werden, die den Umfang und die Merkmale von Abhöraktivitäten dokumentieren, um so den gesamten Grad des Eindringens in die Privatsphäre anzuzeigen. Berichte können Statistiken enthalten über:

   - die Anzahl der angeordneten Abhörmaßnahmen und ihre Dauer
   - die Anzahl der abgelehnten Anträge auf eine Abhörmaßnahme
   - Genehmigungen mit besonderen Merkmalen oder Bedingungen (wie z. B. die Befugnis, private Grundstücke zu betreten)
   - die Anzahl der abgehörten Kommunikationsvorgänge und der identifizierten Einzelpersonen
   - die Art der verschiedenen abgehörten Kommunikationsdienste (wie Telefon, Fax, E-mail, Pager und Sprachbox-Dienste)
   - generelle Klassifizierungen von Orten, an denen Abhörmaßnahmen durchgeführt wurden (z. B. Geschäftsräume, Privatwohnungen, Fahrzeuge)
   - die Art der untersuchten Straftaten
   - die Resultate und die Effektivität von Abhörmaßnahmen, wie z. B. Fälle, in denen keine Hinweise für Verstöße gefunden wurden, in denen Anklage erhoben wurde und in denen Abhörprotokolle als Beweismittel verwendet wurden und ein Schuldspruch erreicht wurde
   - die Kosten von Abhörmaßnahmen.

   Die Informationen in den Berichten sollten in klarer und verständlicher Weise gefasst sein; sie sollten Trends und besondere Eigenschaften von Abhöraktivitäten während des Berichtszeitraums enthalten.

Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb

angenommen bei der 23. Sitzung in Hong Kong SAR, China

15. April 1998

– Übersetzung –

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation unterstützt jegliche Bemühungen zur Entwicklung von Technologien, die den Schutz der Privatsphäre der Benutzer im WorldWideWeb verbessern helfen.

Unter diesem Gesichtspunkt hat die Arbeitsgruppe mit besonderem Interesse auf ihrer 22. Sitzung in Berlin am 2. September 1997 und der 23. Sitzung in Hong Kong am 14. April 1998 von dem Platform for Privacy Preferences Project (P3P) Kenntnis genommen, das gegenwärtig durch das WorldWideWeb-Konsortium durchgeführt wird.

Obwohl noch eine Reihe von technischen Details zu klären ist, einschließlich des Ausmaßes, in dem Punkte wie Datensicherheit, Qualität der Daten, Speicherungsdauer sowie Auskunft und Berichtigung von Daten behandelt werden sollen, möchte die Arbeitsgruppe die folgenden grundlegenden Bedingungen darlegen, die von jeder technischen Plattform für den Datenschutz im WorldWideWeb mit dem Ziel der Verhinderung einer systematischen Sammlung personenbezogener Daten berücksichtigt werden sollten:

1. Technologie allein kann nicht die Lösung zur Sicherstellung des Datenschutzes im Web sein. Sie muss innerhalb eines regulatorischen Rahmens angewandt werden (dieser kann sowohl in gesetzlichen Regelungen als auch in Verträgen und Verhaltensregeln bestehen, die gleichartige Garantien im Hinblick auf ihre Durchsetzung bieten, einschließlich Sanktionen, eines effektiven und unabhängigen Überwachungssystems und Rechtsschutzes für den Einzelnen).
2. Jeder Nutzer sollte die Möglichkeit haben, das Web anonym zu benutzen. Das betrifft auch das Herunterladen öffentlich zugänglicher Informationen. Personenbezogene Informationen sollten in diesem Fall nur für den Zeitraum verarbeitet werden, in dem der Nutzer die Website liest, mit Ausnahme der Verbindungsdaten, soweit diese für Sicherheitszwecke erforderlich sind.
3. Bevor personenbezogene Daten, insbesondere solche, die durch den Benutzer offenbart wurden, durch den Anbieter einer Website verarbeitet werden, ist eine informierte Einwilligung des Benutzers erforderlich. Darüber hinaus sollten einige unabdingbare Grundregeln in die Standardkonfiguration der technischen Plattform eingebaut werden. Personenbezogene Daten dürfen nicht in einem automatischen Verfahren zu einer Website ohne vorherige Information des Betroffenen übertragen werden, der stets die Möglichkeit haben sollte, die Übertragung zu verhindern.
4. Die Implementierung des P3P-Projekts wird von entscheidender Bedeutung sein und sollte genau beobachtet werden.