Der Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Berliner Beauftragter
für Datenschutz und
Informationsfreiheit

Berlin

Dokumente zu Datenschutz und Informationsfreiheit

2004

Dokumente
zu Datenschutz
und Informationsfreiheit
2004

Impressum

Herausgeber:

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg	**Berliner Beauftragter für Datenschutz und Informationsfreiheit**
Stahnsdorfer Damm 77, Haus 2 14532 Kleinmachnow	An der Urania 4 – 10 10787 Berlin
Telefon: 03 32 03/35 60 Telefax: 03 32 03/3 56 49	Telefon: 0 30/1 38 89-0 Telefax: 0 30/2 15 50 50
E-Mail: Poststelle@LDA.Brandenburg.de	E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.lda.brandenburg.de	Internet: http://www.datenschutz-berlin.de

Druck: Druckerei Conrad GmbH

Stand: Februar 2005

Inhaltsverzeichnis

Vorwort

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum „Großen Lauschangriff“ und seine Auswirkungen haben beide Konferenzen der Datenschutzbeauftragten des Bundes und der Länder, die in diesem Jahr im März und Oktober im Saarland tagten, beschäftigt. Im Mittelpunkt steht die Forderung, das Urteil nicht nur in vollem Umfang umzusetzen, sondern auch vergleichbare Maßnahmen, die tief in die informationelle Selbstbestimmung eingreifen, einer Überprüfung zu unterziehen. In der Herbstsitzung stellte die 68. Konferenz gravierende Datenschutzmängel bei Hartz IV fest und forderte effektive Abhilfe. Wie immer befasste sich die Konferenz mit neuen Informationstechniken, in diesem Jahr insbesondere mit der automatischen Kfz-Kennzeichenerfassung sowie der RFID-Technologie.

Die Europäische Konferenz der Datenschutzbeauftragten fasste nach einer vorbereitenden Diskussion auf der Sitzung im April in Rotterdam im September in Breslau eine Entschließung zur Schaffung eines gemeinsamen Gremiums zur Beratung der Organe der Europäischen Union auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit (Datenschutz in der dritten Säule); die verschiedenen Institutionen (Schengen, Europol, Eurojust, Zollinformationssystem) haben bisher jeweils eigene Datenschutzkontrollorgane, deren Arbeit besser koordiniert werden muss.

Die Art. 29-Datenschutzgruppe, die aus den Datenschutzbehörden der Mitgliedstaaten besteht und die Europäische Kommission berät, hat fast 20 Arbeitspapiere zu den verschiedensten Themen verabschiedet. Die wichtigsten dürften ein Arbeitspapier über genetische Daten, eine Stellungnahme zur Vorratsspeicherung von Telekommunikationsdaten und ein Beschluss über alternative Standardvertragsklauseln sein, die künftig von den Unternehmen ebenfalls genutzt werden können, um beim Datenexport in Drittländer ein angemessenes Datenschutzniveau herzustellen.

Die 26. Internationale Konferenz der Datenschutzbeauftragten im September in Breslau befasste sich mit den Planungen, im Rahmen der Internationalen Standardorganisation ISO einen Rahmenstandard zum Datenschutz zu entwickeln, und wandte sich dagegen, die Normierung in einem Schnellverfahren durchzusetzen. Sie unterstützte aber gleichzeitig die Entwicklung eines effektiven und universell akzeptierten internationalen Standards über Datenschutztechnologien.

Wie in jedem Jahr sind die Arbeitspapiere, die die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation unter Berliner Vorsitz beschlossen hat, vollständig abgedruckt. Die Beschlüsse der Sitzungen im April in Buenos

Aires und im November in Berlin reichen vom Datenschutz bei Kameratelefonen (MMS) über die Risiken drahtloser Netzwerke, die Meinungsäußerungsfreiheit und Persönlichkeitsrechte bei Online-Publikationen bis zu den Lehrplänen zur Internetsicherheit unter Berücksichtigung nationaler, kultureller und rechtlicher Anforderungen.

Die auf der 25. Internationalen Datenschutzkonferenz im September 2003 in Sydney gefasste Resolution zur Verbesserung der Bekanntmachung von Praktiken zum Datenschutz führte zu einer von weltweiten Unternehmen, Anwaltskanzleien, Verbraucherschutzverbänden und Datenschutzbeauftragten getragenen Initiative zur Entwicklung von Datenschutzinformationen, die die Betroffenen sowohl auf kurze, einprägsame Weise („Short Notices"), aber auf Wunsch auch ausführlicher („Layered Notices") über den Zweck der Datenverarbeitung und die Rechte der Betroffenen unterrichten. Das Ergebnis war das auf einer gemeinsamen Sitzung in Berlin im März beschlossene „Berliner Memorandum zu Datenschutzerklärungen", das mittlerweile schon zur Grundlage konkreter Umsetzungen gemacht wurde.

Zur Thematik Informationsfreiheit werden die beiden Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland, der die Landesbeauftragten von Brandenburg, Nordrhein-Westfalen, Schleswig-Holstein und Berlin angehören, dokumentiert: Die Arbeitsgemeinschaft verlangt einen verbesserten Zugang zu den Umweltinformationen sowie die Öffentlichkeit der Sitzungen von Entscheidungsgremien.

Die Internationale Konferenz der Informationsbeauftragten (ICIC), die im April 2003 in Berlin gegründet worden war, fasste auf ihrer zweiten Sitzung im Februar 2004 in Kapstadt zwar keine Entschließung, die Einladung der südafrikanischen Menschenrechtskommission bringt jedoch die Themen zum Ausdruck, die im Mittelpunkt der Konferenz standen.

Der vorliegende Dokumentenband soll zusammen mit den Veröffentlichungen aus den vergangenen Jahren die Fortentwicklung des Datenschutzes nicht nur in Deutschland und Europa, sondern weltweit dokumentieren. Er zeigt, dass die zur Wahrung des Datenschutzes und der Informationsfreiheit berufenen Institutionen keineswegs, wie so oft behauptet, der Entwicklung nachhinken, sondern gestaltend in die Fortentwicklung der Informationsgesellschaft eingreifen.

Dr. Alexander Dix Prof. Dr. Hansjürgen Garstka

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließung vor der 67. Konferenz (vom 13. Februar 2004)

Übermittlung von Flugpassagierdaten an die US-Behörden

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z. B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen. Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke, sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II-System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet (http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm). Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zur Zeit praktiziert wird, muss ausgeschlossen werden.

2. Entschließungen der 67. Konferenz vom 25./26. März 2004 in Saarbrücken

Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

– in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

– in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

– in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Radio-Frequency Identification

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre zu Radio-Frequency Identification vom 20. November 2003 (Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a. sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b. wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c. dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d. soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die

mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

3. Entschließungen der 68. Konferenz vom 28./29. Oktober 2004 in Saarbrücken

Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung

der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Beteiligung der GEZ am Adresshandel (8. Rundfunkänderungsstaatsvertrag)

Die für die Rundfunkanstalten zuständigen Datenschutzbeauftragten haben im Rahmen der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu dem 8. Rundfunkänderungsstaatsvertrag nachstehende Feststellung getroffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt dafür eingesetzt, bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland das Prinzip von Datenvermeidung und Datensparsamkeit in stärke-

rem Maße zu berücksichtigen. In der Kritik steht dabei im Besonderen die Beschaffung von jährlich mehreren Millionen Adressen hinter dem Rücken der Betroffenen beim kommerziellen Adresshandel durch die von den Rundfunkanstalten beauftragte Gebühreneinzugszentrale (GEZ), die diese Adressen für flächendeckende Mailing-Aktionen nutzt. Zahlreiche Beschwerden und Anfragen von Bürgerinnen und Bürgern beziehen sich auf diese Praxis der GEZ, die die zuständigen Landesdatenschutzbeauftragten als rechtswidrig bezeichnet haben.

Anstatt gemeinsam mit den Datenschutzbeauftragten datenschutzfreundliche Varianten einer gerechten Finanzierung des öffentlich-rechtlichen Rundfunks ernsthaft zu prüfen, haben die Ministerpräsidenten der Länder mit dem Entwurf eines 8. Rundfunkänderungsstaatsvertrages neben der Erhöhung der Rundfunkgebühren und deren Erstreckung auf Computer weitgehend ohne die gebotene Beteiligung der zuständigen Landesdatenschutzbeauftragten eine weitere Verschlechterung des Datenschutzes beschlossen:

Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der Rundfunkgebührenstaatsvertrag um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und die GEZ personenbezogene Daten unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen.

Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Schließlich haben die Länder gegen das Votum der Datenschutzbeauftragten bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde. Eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel ist jedoch unverhältnismäßig.

Zudem wird durch die ohnehin fragwürdige Befugnis das Ziel der Rundfunkanstalten nicht erreicht. Auch bei einem Inkrafttreten der vorgesehenen Regelung bliebe die Beschaffung von Adressen beim kommerziellen Adresshandel durch die GEZ rechtswidrig, da sich die Erhebung von personenbezogenen Daten bei Dritten ohne Kenntnis der Betroffenen weiterhin nach dem maßgeblichen Landesrecht richtet.

Die Konferenz hat davon Kenntnis genommen.

4. Entschließung nach der 68. Konferenz

Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten. Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz

zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen. Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

II. Europäische Konferenz der Datenschutzbeauftragten vom 14. September 2004 in Breslau

Entschließung zur Schaffung eines gemeinsamen Gremiums zur Beratung der Organe der Europäischen Union auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit (Datenschutz in der dritten Säule)

Der Vertrag über die Europäische Union (EUV) in der Fassung vom 2. Oktober 1997 (Vertrag von Amsterdam) enthält in Titel VI umfassende Bestimmungen über die polizeiliche und justizielle Zusammenarbeit in Strafsachen. Nach dem Vertrag von Nizza soll zudem die Zusammenarbeit der Polizei- und Justizbehörden der EU-Mitgliedstaaten noch weiter intensiviert werden. Dies zählt zu den vordringlichen Aufgaben der Union.

Die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union verkennen nicht die Notwendigkeit einer engeren Zusammenarbeit der Strafverfolgungsbehörden der Mitgliedstaaten mit dem Ziel, den Bürgern der Union ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts zu gewährleisten. Dennoch ist es erforderlich, einen Mittelweg zu finden zwischen diesem Bedürfnis und der Aufrechterhaltung bürgerlicher Freiheitsrechte, einschließlich durch die Charta der Grundrechte der Europäischen Union geschützten Datenschutzrechte.

Es gehört zu den wichtigsten Aufgaben der Datenschutzbeauftragten, die an der Gesetzgebung beteiligten Organe in allen Fragen des Datenschutzes zu beraten, dabei insbesondere auf Risiken für die oben erwähnten Freiheitsrechte hinzuweisen und bürgerfreundliche Lösungen vorzuschlagen. Diese Beratung wird von der Kommission, dem Rat und dem Europäischen Parlament mehr und mehr in Anspruch genommen.

Die Datenschutzbeauftragten kommen dieser Nachfrage selbstverständlich nach bestem Vermögen nach. Sie müssen allerdings darauf hinweisen, dass bisher die organisatorischen Voraussetzungen für die Erfüllung dieser wichtigen Aufgabe fehlen und deshalb eine zeitnahe und europäisch abgestimmte Beratung auf dem gebotenen hohen Qualitätsniveau nicht gesichert ist. Während nämlich die Datenschutzbeauftragten für den Bereich des Binnenmarktes (erste Säule) mit der Arbeitsgruppe nach Art. 29 der Richtlinie 95/46/EG einen geeigneten organisatorischen Rahmen besitzen, der ein (von der Kommission gestelltes) ständiges Sekretariat umfasst und regelmäßige Sitzungen in Brüssel – mit dem erforderlichen Sprachendienst – erlaubt, fehlen diese Voraussetzungen im Bereich der

dritten Säule vollständig. Die im Bereich der dritten Säule bestehenden gemeinsamen Kontrollinstanzen (z. B. bei Europol, Schengen, Eurojust) sind hierfür wegen ihrer eng begrenzten und speziellen Aufgabenstellung nicht geeignet, da zur Sicherung eines einheitlichen Datenschutzstandards für den gesamten Bereich der polizeilichen und justiziellen Zusammenarbeit ein übergeordneter Ansatz erforderlich ist.

Zur Zeit sind die Teilnehmer der Konferenz dabei, ihre Zusammenarbeit in polizeilichen und justiziellen Angelegenheiten zu vertiefen. Deshalb wurde von der Konferenz der Europäischen Datenschutzbehörden eine Polizeiarbeitsgruppe eingesetzt, die die Richtlinien für die Arbeit festlegen soll. Sie untersucht Fälle, die außerhalb des Aufgabengebietes der existierenden Datenschutzbehörden auf EU-Ebene liegen. Außerdem wurde eine weitere Untergruppe der Konferenz gegründet. Dieser Planungsgruppe, die sich unter anderem aus den Vorsitzenden der gemeinsamen Aufsichtsbehörden zusammensetzt (von Europol, Schengen, Zoll und Eurojust), dem Vorsitzenden der Arbeitsgruppe nach Artikel 29 sowie dem Europäischen Datenschutzbeauftragten, obliegt die Entwicklung strategischer Ansätze bei neuen Initiativen. Diese sollen sowohl die Verwendung von persönlichen Daten in der Strafverfolgung als auch den europäischen Aspekt beinhalten.

Dennoch sind zusätzliche strukturelle Maßnahmen notwendig. Angesichts des forcierten Ausbaus der Europäischen Sicherheitsarchitektur in der dritten Säule ist die institutionelle Sicherung einer geregelten Datenschutzberatung durch den Europarat von höchster Priorität. Die Konferenz der Europäischen Datenschutzbeauftragten fordert deshalb den Rat auf, die notwendigen personellen und organisatorischen Maßnahmen umgehend zu ergreifen, damit das Datenschutzgremium noch in diesem Jahr seine wichtige Arbeit im Interesse der Bürger aufnehmen kann. Der Europäische Datenschutzbeauftragte nach Art. 286 Abs. 2 des EG-Vertrags sollte in dem zu schaffenden Gremium mitwirken.

Die Konferenz fordert den Rat und die Kommission ebenfalls dazu auf, die rechtlichen Bedingungen für die Harmonisierung der Datenschutzkontrolle innerhalb der dritten Säule zu schaffen, und zwar in enger Zusammenarbeit mit den zuständigen Organisationen.

Der Vorsitzende wird angewiesen, diese Entschließung dem Rat, der Kommission sowie dem Parlament zu übermitteln.

III. Dokumente der Europäischen Union

1. Arbeitspapiere der Artikel 29-Datenschutzgruppe

Arbeitspapier über genetische Daten vom 17. März 2004 (WP 91)

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN –

unter Hinweis auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], insbesondere auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a der Richtlinie,

gestützt auf die Geschäftsordnung der Gruppe[2], insbesondere auf Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. Allgemeine Darlegung der Problematik

Der wissenschaftlich-technische Fortschritt, der in den letzten Jahren auf dem Gebiet der Genforschung stattgefunden hat, wirft neue Fragen bezüglich des Datenschutzes auf und gibt Anlass zur Sorge im Hinblick auf die Bedeutung von genetischen Tests, die Verarbeitung genetischer Daten und die daraus entstehenden Folgen.

Ein fundierter Schutz genetischer Daten kann heute als eine Grundvoraussetzung dafür gelten, dass die Wahrung des Gleichheitsprinzips gewährleistet und das Recht auf Gesundheit in der Praxis verwirklicht werden kann. In sämtlichen internationalen Rechtsvorschriften der jüngsten Zeit wird jegliche Diskriminierung auf der Grundlage genetischer Daten untersagt. Gemäß Artikel 21 der Europäischen Grundrechtecharta ist „jegliche Diskriminierung aufgrund (…) genetischer Merkmale“ untersagt; dieses Verbot ist auch im Übereinkommen des Europarats über Menschenrechte und Biomedizin (Artikel 11) und in der Allgemeinen Erklärung der UNESCO über das menschliche Genom und Menschenrechte (Universal Declaration on Human Genome and Human Rights) enthalten (Artikel 6).

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/index_de.htm

[2] Angenommen von der Arbeitsgruppe auf ihrer dritten Tagung am 11.9.1996.

Die Wirksamkeit dieser Verbote ist an die Existenz strenger Vorschriften gekoppelt, durch die die Möglichkeiten zur Nutzung genetischer Daten begrenzt werden. So ist der Schutz des Rechts auf Gesundheit an die Zusicherung geknüpft, dass keine genetischen Daten an Dritte weitergegeben werden, die diese Daten in diskriminierender und/oder stigmatisierender Weise gegen die betroffene Person verwenden könnten. Aus den USA sind zahlreiche Fälle bekannt, in denen Personen sich bewusst entschieden haben, sich keinen genetischen Untersuchungen zu unterziehen – obwohl diese aus Gründen des Gesundheitsschutzes notwendig waren –, da sie befürchteten, dass Arbeitgeber und Versicherungsunternehmen von den Ergebnissen dieser Untersuchungen Kenntnis erlangen könnten. Hieraus entstand eine intensive öffentliche Debatte und es wurden wichtige Gesetze auf den Weg gebracht. In Abschnitt 2 Ziffer 5 des „Genetic Information Nondiscrimination Act" (Gesetz über das Verbot der Diskriminierung aufgrund genetischer Daten), das vor kurzem vom US-Senat verabschiedet wurde und gegenwärtig durch das US-Repräsentantenhaus überprüft wird, ist ausdrücklich festgehalten, dass „Bundesgesetze über einen landesweiten einheitlichen Grundstandard notwendig sind, um die Öffentlichkeit in vollem Umfang vor Diskriminierung zu schützen und ihre Befürchtungen hinsichtlich des bestehenden Diskriminierungspotenzials zu zerstreuen, so dass die betroffenen Personen die Vorteile genetischer Untersuchungen, Forschungen und neuer Therapien nutzen können." Ausgehend von dieser Feststellung, werden in diesem Gesetz außerordentlich strenge Vorschriften festgelegt, nach denen genetische Informationen weder vom Arbeitgeber noch von Versicherungsunternehmen verwendet werden dürfen.

In ihrer am 13. Juli 2000 veröffentlichten Stellungnahme 6/2000 zum Thema „Menschliches Genom und Privatsphäre" hat die Datenschutzgruppe bereits betont, dass es notwendig ist, im Zuge der Entwicklung neuer Gentechnologien für angemessene Schutzmechanismen zu sorgen, um das Recht auf Schutz der Privatsphäre zu gewährleisten. Die europäischen Datenschutzbehörden haben im September 1998 auf ihrer jährlichen internationalen Konferenz in Santiago de Compostela ihre Sorge über den Plan Islands zum Ausdruck gebracht, Patientendaten aus dem gesamten Land zentral zu erfassen, um sie für die genetische Forschung nutzen zu können. Den isländischen Behörden wurde mit Blick auf die Grundsätze der EU-Datenschutzrichtlinie und insbesondere auf die wichtige Frage der Anonymität empfohlen, das Vorhaben noch einmal zu überdenken. Außerdem wurde betont, dass wirtschaftliche Interessen nicht dazu führen sollten, die Datenbank für ursprünglich nicht vorgesehene Zwecke zu verwenden.

Aufgrund der wachsenden Bedeutung und Sensibilität der Fragen in Verbindung mit dem Schutz genetischer Daten sowie in Anbetracht der laufenden Initiativen auf nationaler und übernationaler Ebene hat die Datenschutzgruppe dieses Thema in ihr Arbeitsprogramm für 2003 aufgenommen.

Auf regulatorischer Ebene ergibt sich innerhalb der EU allem Anschein nach kein einheitliches Bild: Während in einigen Mitgliedstaaten genetische Daten im Datenschutzgesetz ausdrücklich als sensible Daten aufgeführt sind, mit allen damit verbundenen Garantien und Beschränkungen, ist in den meisten Mitgliedstaaten die Verarbeitung genetischer Daten als solche nicht durch eine spezifische Rechtsvorschrift geregelt. Mitunter findet man in den einzelstaatlichen Gesetzen über Patientenrechte entsprechende ergänzende Bestimmungen, und zum Teil ist die Verarbeitung genetischer Daten auch gesetzlich geregelt. Da die nationalen Behörden sich zunehmend der Risiken bewusst sind, die sich aus der Verarbeitung genetischer Daten ergeben, ist in den Mitgliedstaaten ein allgemeiner Trend zu neuen Initiativen auf regulatorischer Ebene absehbar.

Überdies ist festzustellen, dass man auf übernationaler Ebene die Bedingungen für die Durchführung genetischer Tests, die eine Voraussetzung für die nachfolgende Verarbeitung der gewonnenen relevanten Daten bilden, bereits berücksichtigt hat und/oder sich zurzeit damit auseinandersetzt.[3] Das nach wie vor einzige rechtsverbindliche Instrument auf internationaler Ebene ist das 1997 in Oviedo geschlossene Übereinkommen über Menschenrechte und Biomedizin, das seitdem zur Unterzeichnung und Ratifizierung aufliegt.[4] Gemäß dem Übereinkommen ist jede Form der persönlichen Diskriminierung aufgrund des genetischen Profils verboten; prädiktive genetische Tests dürfen nur zu medizinischen Zwecken durchgeführt werden.

Das vorliegende Dokument soll vor allem zeigen, in welchen Bereichen die Verarbeitung genetischer Daten aus Sicht des Datenschutzes Anlass zur Sorge gibt, und dazu beitragen, dass angesichts der gemäß Richtlinie 95/46/EG erlassenen einzelstaatlichen Maßnahmen auf diesem Gebiet ein einheitlicherer Ansatz gefunden wird. Darüber hinaus geht es der Datenschutzgruppe zum gegenwärtigen Zeitpunkt darum, sich gemeinsam über die verschiedenen Fragen bezüglich der Verarbeitung genetischer Daten zu verständigen. Die Genetik betreffende Fragen, die der dritten Säule zuzuordnen sind, werden hier weniger ausführlich behandelt, da sie nicht in den Geltungsbereich der Richtlinie fallen.

---

[3] EUROPARAT
- Arbeitspapier vom 7. Februar 2003 über die Anwendungsmöglichkeiten der Genetik für Gesundheitszwecke. Das Dokument ist zurzeit Gegenstand von Konsultationen und steht in engem Zusammenhang mit den im Übereinkommen über die Biomedizin von 1997 verankerten Grundsätzen.
- Entwurf eines Erläuternden Berichts des Lenkungsausschusses für Bioethik (CDBI) zum Entwurf des Zusatzprotokolls über biomedizinische Forschung vom 22. August 2003 zum Übereinkommen über Menschenrechte und Biomedizin. Der Berichtsentwurf wurde der Parlamentarischen Versammlung vorgelegt, die ihn voraussichtlich Ende Januar 2004 erörtern wird.

UNESCO
- Internationale Erklärung des IBC zum Schutz genetischer Daten, verabschiedet am 16. Oktober 2003.

[4] Eine Übersicht zum Stand der Unterzeichnung und Ratifizierung des Übereinkommens über Menschenrechte und Biomedizin ist unter der folgenden URL-Adresse veröffentlicht:
http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=164&CM=1&DF=

II. Definitionen und Hauptmerkmale genetischer Daten

Definitionen:

Alle Daten, gleich welchen Typs, über die Erbmerkmale einer Person oder über das für diese Merkmale typische Vererbungsmuster innerhalb einer miteinander verwandten Gruppe von Personen *(Europarat, Empfehlung Nr. R(97)5)*.

Alle Arten von Daten über die Erbmerkmale einer Person oder einer Gruppe miteinander verwandter Personen *(Artikel 2 Buchstabe g des luxemburgischen Gesetzes über den Schutz von Personen in Hinblick auf die Verarbeitung personenbezogener Daten vom 2. August 2002)*.

Nicht offenkundige Daten über erbliche Merkmale von Individuen, die durch Nukleinsäureanalyse oder durch andere wissenschaftliche Analysen gewonnen werden *(Internationale Erklärung zum Schutz genetischer Daten, UNESCO)*.

Merkmale:

Genetische Daten beinhalten Merkmale, aufgrund derer diese Daten einen einzigartigen Datenbestand (vor allem im Vergleich zu Gesundheitsdaten) darstellen. Bereits heute bzw. vor allem in Zukunft dürften genetische Daten wissenschaftliche, medizinische und personenbezogene Informationen vermitteln, die für das gesamte Leben eines Menschen von Bedeutung sind. Diese Informationen können sich auch in nachhaltigem Maße über mehrere Generationen hinweg auf die Familie des Betroffenen sowie in bestimmten Fällen auf die gesamte Gruppe auswirken, der die betroffene Person angehört.

Die Identifikationsmöglichkeiten durch den genetischen Fingerabdruck eröffnen ebenfalls einzigartige Möglichkeiten. Genetische Daten vermitteln oft Informationen über mehrere Personen; zugleich wird es durch diese Daten ermöglicht, eine einzige dieser Personen gezielt zu identifizieren. Diese Daten zeigen also die Unverwechselbarkeit der betroffenen Person auf.

Aufgrund dieser Besonderheiten erfordert und rechtfertigt die Verarbeitung genetischer Daten besondere rechtliche Schutzvorkehrungen. Dieses Ziel steht im Mittelpunkt des Arbeitspapiers über genetische Daten.

Allerdings sollte die Menschheit nicht lediglich auf ihre genetischen Merkmale oder auf ihr genetisches Abbild reduziert werden, das sowieso keine letztendliche, allumfassende Erklärung des menschlichen Lebens liefert.

Als eine der ersten Garantien, denen die Verwendung genetischer Daten unterliegt, muss daher vermieden werden, dass diesen Daten eine umfassende Aussagefähigkeit zuerkannt wird.

Genetische Daten weisen also verschiedene besondere Merkmale auf, die sich wie folgt zusammenfassen lassen:

– Genetische Daten stellen einen einzigartigen Datenbestand dar, durch den sich eine bestimmte Person von anderen Personen unterscheidet, allerdings können sie auch Informationen über die Blutsverwandten (die biologische Familie) dieser Person zutage fördern, die auch für Angehörige früherer oder nachfolgender Generationen relevant sind. Darüber hinaus können auch bestimmte Personengruppen (z. B. ethnische Gemeinschaften) durch genetische Daten charakterisiert werden;

– genetische Daten können Aufschluss geben über Verwandtschaftsbeziehungen und Familienverbindungen;

– genetische Daten sind der betreffenden Person selbst häufig völlig unbekannt und existieren unabhängig von dessen persönlichem Willen, da genetische Daten nicht veränderbar sind;

– genetische Daten lassen sich ohne große Schwierigkeiten beschaffen oder aus Rohdatenmaterial gewinnen, auch wenn diese Daten dann mitunter von zweifelhafter Qualität sind;

– angesichts der Entwicklungen in der Forschung besteht die Möglichkeit, dass genetische Daten in Zukunft noch weiter gehende Informationen offenbaren und von einer stetig wachsenden Zahl von Einrichtungen für unterschiedlichste Zwecke verwendet werden.

III. Anwendbarkeit der Richtlinie 95/46/EG

Gemäß Artikel 2 Buchstabe a der Richtlinie bezeichnet der Begriff „*‚personenbezogene Daten' alle Informationen über eine bestimmbare natürliche Person (betroffene Person); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.*"

Es besteht kein Zweifel, dass der Informationsgehalt genetischer Daten in dieser Definition Berücksichtigung findet. So ist der Bezug auf eine konkrete Person, d. h. die Tatsache, dass es sich um eine bestimmte oder um eine bestimmbare Person handelt, in den meisten Fällen klar. In einigen Fällen ist dies jedoch weniger eindeutig, wie etwa bei der Entnahme von DNA-Proben an einem bestimmten Ort – z. B. bei der Spurensicherung am Tatort eines Verbrechens. Derartige Proben können aber insofern eine Quelle personenbezogener Daten darstellen, als die

Möglichkeit bestünde, die DNA-Proben einer bestimmten Person zuzuordnen, insbesondere dann, wenn ihre Herkunft durch einen gerichtsmedizinischen Nachweis bestätigt wurde. Bei der Regelung des Umgangs mit genetischen Daten sollte deshalb auch der rechtliche Status der DNA-Proben Berücksichtigung finden.

Gemäß Artikel 8 Absatz 1 der Richtlinie zählen zu den Kategorien personenbezogener Daten, die aufgrund ihrer Sensibilität ein höheres Maß an Schutz verlangen, auch „Daten über die Gesundheit". Genetische Daten, die ja in gewisser Weise detailliert Auskunft über die körperliche Disposition eines Menschen und dessen Gesundheitszustand geben, könnte man deshalb den „Daten über die Gesundheit" zuordnen. Anhand genetischer Daten lassen sich jedoch auch spezifische Formen aus einem breiten Spektrum physischer Merkmale beschreiben. Wird auf diese Weise z. B. die Haarfarbe einer Person bestimmt, dann dürfte man diese genetischen Informationen nicht als direkt die Gesundheit betreffende Daten betrachten. Da aber die genetischen Daten in diesem Zusammenhang z. B. dazu beitragen können, die ethnische Herkunft einer Person zu ermitteln, sollte man sie ebenfalls als Daten im Sinne von Artikel 8 Absatz 1 ansehen.

In Anbetracht des ganz singulären Charakters genetischer Daten und ihrer Verknüpfung mit Informationen, die Aufschluss geben können über den Gesundheitszustand oder die ethnische Herkunft einer Person, sollten sie als besonders sensible Daten im Sinne von Artikel 8 Absatz 1 der Richtlinie behandelt werden und deshalb einem stärkeren Schutz unterliegen, wie er in der Richtlinie und in den nationalen Gesetzen zu ihrer Umsetzung vorgesehen ist.

Gemäß Artikel 8 Absatz 3 der Richtlinie besteht die Besonderheit sensibler Daten darin, dass sie nur unter außergewöhnlichen Umständen, d. h. „wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist", und nur unter ganz bestimmten Voraussetzungen verarbeitet werden dürfen. So ist die Verarbeitung von Daten, die die Gesundheit betreffen, nur dann zulässig, wenn sie durch ärztliches Personal, das der Schweigepflicht unterliegt, oder durch sonstige Personen erfolgt, für die eine dieser Schweigepflicht entsprechende Geheimhaltungspflicht gilt. Es spricht einiges dafür, dass genetische Daten verarbeitet werden könnten, wenn einer der oben genannten außergewöhnlichen Umstände vorliegt.

Gemäß Artikel 6 der Richtlinie dürfen personenbezogene Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden (Grundsatz der Zweckbestimmung). Außerdem müssen personenbezogene Daten den Zwecken entsprechen, für die sie erhoben und weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen (Grundsatz der Verhältnismäßigkeit).

Angesichts der Komplexität und Sensibilität genetischer Informationen besteht eine große Gefahr, dass sie von dem für die Verarbeitung Verantwortlichen oder von Dritten für verschiedene Zwecke missbraucht und/oder wiederverwendet werden. Das Risiko einer Wiederverwendung könnte z. B. dann eintreten, wenn bereits gewonnene genetische Informationen genutzt werden oder wenn das zugrunde liegende Material einer zusätzlichen Analyse unterzogen wird (z. B. durch Entnahme von Blutproben). Die Richtlinie verbietet eine Weiterverarbeitung von Daten, die mit dem Zweck der Datenerhebung unvereinbar ist. Ausgenommen von diesem Verbot ist jedoch die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken, sofern die Mitgliedstaaten geeignete Garantien vorsehen.

Ferner ist die Wahrung der Verhältnismäßigkeit und der Rechtmäßigkeit zu bewerten; dabei sind die Risiken für den Schutz der Grundrechte und Grundfreiheiten des Einzelnen zu berücksichtigen, vor allem die Frage, ob der beabsichtigte Zweck nicht auch auf eine weniger in die Rechte des Betroffenen eingreifende Weise zu erreichen ist. Genetische Daten dürfen nur dann verwendet werden, wenn sie ihrem Zweck entsprechen, dafür erheblich sind und nicht darüber hinausgehen. Das setzt voraus, dass an die Notwendigkeit und die Verhältnismäßigkeit der verarbeiteten Daten strenge Maßstäbe angelegt werden. (Beispiel: Die spanische Datenschutzbehörde beanstandete die Einrichtung einer Genprobenbank zur Identifizierung von Neugeborenen durch DNA-Tests, mit der man verhindern wollte, dass Säuglinge vertauscht und der falschen Mutter zugeordnet werden. Nach Ansicht der Datenschutzbehörde stellte die Einrichtung der Genprobenbank einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit dar, da man den gleichen Zweck ganz sicher auch mit anderen Mitteln hätte erreichen können, wie z. B. mit einer Kennzeichnung durch Armbänder oder mit Hilfe von Fußabdrücken.) Fast alle bisherigen Entscheidungen der Datenschutzbehörden zur Verarbeitung genetischer Daten stellen vornehmlich auf das Kriterium der Verhältnismäßigkeit ab.

Die Wahrung des Grundsatzes der Zweckbestimmung und des Grundsatzes der Verhältnismäßigkeit setzt eine eindeutige Bestimmung des Zwecks voraus, für den genetische Daten erhoben und weiterverarbeitet werden. Um eine zweckfremde Wiederverwendung zu vermeiden, ist es unerlässlich, dass die Zwecke der Verarbeitung genetischer Daten klar definiert sind.

Gemäß Artikel 10 der Richtlinie ist eine Person, bei der die sie betreffenden Daten direkt erhoben werden, berechtigt, vom für die Verarbeitung Verantwortlichen (oder seinem Vertreter) entsprechende Informationen zu erhalten. Gemäß Artikel 11 der Richtlinie hat die betroffene Person auch dann das Recht, Informationen vom für die Verarbeitung Verantwortlichen (oder seinem Vertreter) zu erhalten, wenn die Daten nicht bei ihr selbst erhoben wurden. Aufgrund der Sensibilität genetischer Daten ist das Recht auf Information insbesondere dann rele-

vant, wenn es um die Verarbeitung dieser Daten geht. In Fällen, die unter die in Artikel 8 Absatz 3 vorgesehene Ausnahmeregelung fallen, könnte sich für das dort erwähnte ärztliche Personal insofern eine Zwangslage ergeben, als einerseits die ärztliche Schweigepflicht gilt und andererseits auch die in Artikel 11 vorgeschriebene Informationspflicht zur Anwendung kommt. (Ein solcher Fall tritt z. B. dann ein, wenn das genetische Material, aus dem Informationen gewonnen werden, von Verwandten stammt.)

IV. Zwecke, für die genetische Daten erhoben und verarbeitet werden können, und diesbezügliche Fragestellungen

Da genetische Daten hinsichtlich ihres Wesens und ihrer Merkmale Besonderheiten aufweisen und ihre Verwendung erhebliche Folgen für das Leben des Einzelnen und seiner Familienangehörigen haben kann, ist es sehr wichtig, die Zwecke zu bestimmen, für die diese Daten verarbeitet werden können.

- **Gesundheitsfürsorge/medizinische Behandlung**

Genetische Tests haben sich in der Gesundheitsdiagnostik bereits sehr gut bewährt. Wenn erkannt wird, wie die Genetik jeden einzelnen Aspekt der Gesundheit beeinflusst, dann bieten sich viel wirksamere Möglichkeiten, um Krankheiten zu behandeln, zu heilen und sogar vorzubeugen. Die Erhebung genetischer Daten zur Verbesserung der Gesundheitsfürsorge wird als der wichtigste legitime Zweck für ihre Weiterverarbeitung angesehen.

Diagnostische Gentests dienen zur Klärung der Ursachen einer Krankheit, die bereits klinisch manifest ist. Genetische Untersuchungen zu Diagnosezwecken können entweder anstelle der konventionellen Diagnostik oder in Ergänzung dazu durchgeführt werden. Außerdem können diagnostische Tests im Hinblick auf die Gesundheit anderer Familienmitglieder auch eine prädiktive Komponente beinhalten.

Prädiktive genetische Tests sollen genetische Veränderungen deutlich machen, die bei der getesteten Person zu einem späteren Zeitpunkt höchstwahrscheinlich zu einer Erkrankung führen werden. Ein besonderes Problem bei der prädiktiven Diagnostik besteht darin, dass man selbst dann, wenn sich die nachweislich mit bestimmten Krankheiten zusammenhängenden genetischen Veränderungen identifizieren lassen, häufig nicht mit Sicherheit vorhersagen kann, ob und wann bei der betreffenden Person später mit einer konkreten Erkrankung zu rechnen ist.

In beiden Fällen sollte die betroffene Person über die Notwendigkeit dieser Tests ordnungsgemäß unterrichtet werden und in die Tests sowie in die Verarbeitung der genetischen Daten **ausdrücklich einwilligen** (Artikel 8 Absatz 2 Buchstabe a). Von besonderer Bedeutung im Bereich der genetischen Untersuchung ist die **informierte Einwilligung**, da die Informationen, die die Personen über

sich selbst erhalten, ernsthafte Implikationen haben könnten. **Freie Einwilligung** sollte bedeuten, dass eine Person nicht zu einem genetischen Test gezwungen wird, wenn sie sich nicht ausdrücklich dazu bereiterklärt.

Recht auf Wissen/auf Zugang zu den genetischen Informationen für die biologischen Familienangehörigen der betroffenen Person:

Recht auf Wissen: Eines der grundlegenden Merkmale genetischer Daten besteht darin, dass damit ein Individuum von anderen Personen abgegrenzt wird und dass diese Daten – bzw. die Merkmale, auf die sich diese Daten beziehen – strukturell auch bei sämtlichen Mitgliedern der gleichen biologischen Gruppe anzutreffen sind, wogegen andere Mechanismen, durch die Gemeinsamkeiten bei personenbezogenen Daten auftreten, vom Willen der betroffenen Personen, sozialen Gebräuchen oder rechtlichen Vorschriften abhängig sind.

Da die Ergebnisse von Gentests erhebliche Auswirkungen bzw. Folgen für die biologischen Familienangehörigen mit sich bringen können, wirft dies unter datenschutzrechtlichen Aspekten auch Fragen hinsichtlich der Informationen auf, die an diese Familienangehörigen weitergegeben werden dürfen.

Aus dem Europäischen Übereinkommen über Biomedizin sowie aus der Allgemeinen Erklärung der UNESCO über das menschliche Genom lässt sich ablesen, dass das Konzept für den Schutz der Vertraulichkeit der Daten sich auf ein individuumsbezogenes Konzept stützt. Ein völlig andersartiges Konzept wird durch andere, nicht minder bedeutende Instrumente verfolgt, in denen deutlicher auf die Bedeutung abgehoben wird, die genetischen Daten heute zugeschrieben wird, so in der Empfehlung Nr. R(97)5 des Europarats, in der Executive Order von Präsident Clinton vom 8. Februar 2000 („To Prohibit Discrimination in Federal Employment Based on Genetic Information – Verbot der Diskriminierung aufgrund genetischer Informationen an staatlichen Arbeitsplätzen"), im „Statement on DNA Sampling" („Erklärung zur Entnahme von DNA-Proben") des Hugo Ethics Committee, in der Internationalen Erklärung der UNESCO zum Schutz genetischer Daten aus dem Jahr 2003 sowie im „Genetic Information Non-discrimination Act" („Gesetz über das Verbot der Diskriminierung aufgrund genetischer Daten").[5]

[5] In der Empfehlung des Europarats werden genetische Daten als Daten beliebiger Art definiert, welche die „Erbeigenschaften einer Person oder die Vererbungsmuster derartiger Merkmale innerhalb einer verwandten Gruppe von Einzelpersonen betreffen". Nach der „Executive Order" umfassen „geschützte genetische Informationen" auch Informationen über „das Auftreten einer Erkrankung, eines medizinischen Befunds oder einer Krankheit bei Familienangehörigen der betroffenen Person" (siehe Abschnitt 2(e)C). Das Hugo Ethics Committee spricht die Empfehlung aus, dass „besondere Berücksichtigung dem Zugang durch nächste Verwandte" zukommen sollte, wobei besondere Bedeutung der Rolle der Verwandten dahingehend zugeschrieben wird, dass die Vernichtung der gesammelten Daten davon abhängig gemacht wird, dass diese am Zugang zu diesen Daten nicht interessiert sind. In der Internationalen Erklärung zum Schutz genetischer Daten wird darauf verwiesen, dass derartigen Informationen aufgrund ihrer „besonderen Auswirkungen auf die Familie" eine „besondere Bedeutung" zukomme. Im „Genetic Information Nondiscrimination Act" ist festgelegt, dass „der Begriff ‚genetische Informationen' als Informationen über (i) die Gentestergebnisse einer Einzelperson; (ii) die Gentestergebnisse der Familienangehörigen der Einzelperson" zu verstehen ist (siehe Section 101(6) und an anderer Stelle).

Angesichts dieses besonders sensiblen Themas gilt es, eine Balance zwischen dem Recht der betroffenen Person auf Nichtweitergabe ihrer genetischen Daten und den möglicherweise schwer wiegenden Folgen einer Weitergabe und Verwendung dieser Daten für die biologischen Familienangehörigen dieser Person zu finden.

Aufgrund der besonderen Beschaffenheit genetischer Daten müssen bestimmte Aspekte der hierfür geltenden Rechtsvorschriften über die rein individuumsbezogene Perspektive hinaus betrachtet werden – wobei der Zugang blutsverwandter Angehöriger der gleichen biologischen Gruppe zu diesen Daten besondere Berücksichtigung finden muss. Diese Fragen betreffen insbesondere die möglicherweise bestehende Pflicht einer Person, ihre genetischen Daten einem Blutsverwandten gegenüber offenzulegen, soweit diese Daten zur Wahrung von dessen Gesundheit von Bedeutung sind, sowie die Wahrnehmung des Rechts auf Nichtwissen innerhalb dieser Gruppe.

In diesem Zusammenhang stellt sich auch die Frage, ob genetische Daten ausschließlich Eigentum der betreffenden Einzelperson sind, bei der sie erhoben wurden, und ob die Familienangehörigen selbst dann ein Recht auf Zugang zu diesen Daten haben, wenn die Zustimmung der betreffenden Einzelperson verweigert wird.

Soweit die genetischen Daten für die Familie relevant sind, lässt sich der Standpunkt vertreten, dass es sich um „gemeinsame“ Informationen handelt und die Familienangehörigen ein Recht auf Zugang zu Daten haben, die für ihre eigene Gesundheit und ihr weiteres Leben von Bedeutung sind.

Die genauen rechtlichen Folgen dieser Auseinandersetzung sind noch nicht ganz klar. Es sind mindestens zwei Szenarien vorstellbar. Das eine Szenario besagt, dass auch weitere Familienangehörige als „betroffene Personen“ mit allen hieraus resultierenden Rechten betrachtet werden könnten. Eine weitere Überlegung sieht vor, dass die übrigen Familienangehörigen ein Recht auf anders geartete Informationen haben, das sich aus dem Umstand ergibt, dass ihre persönlichen Interessen unmittelbar davon betroffen sind. Bei beiden Szenarien wären jedoch noch weitere Überlegungen und Bedingungen zu berücksichtigen, um die verschiedenen Konflikte einzubeziehen, die sich auf absehbare Weise aus den unterschiedlichen Ansprüchen der Familienangehörigen ergeben, entweder Zugang zu den Informationen zu erhalten oder aber diese Informationen vertraulich zu behandeln.

In diesem Zusammenhang ist ein Fallbeispiel aus Italien bekannt, wo im Jahr 1999 durch die italienische Datenschutzbehörde (Garante per la protezione dei dati personali) eine Entscheidung getroffen wurde, nach der der Antragstellerin die Möglichkeit zum Zugang zu den genetischen Daten ihres Vaters eingeräumt

wurde, obwohl dazu keine Einwilligung des Vaters vorlag. Dem Antrag wurde stattgegeben, wobei das Recht des Vaters auf Schutz der Privatsphäre gegenüber dem Recht der Antragstellerin auf Gesundheit – d. h. auf „geistiges und körperliches Wohlbefinden" – zurückzustehen hatte.[6]

Man könnte also sagen, dass damit eine neue, rechtlich relevante gesellschaftliche Gruppe entstanden ist, nämlich die biologische Gruppe, die Gruppe der Blutsverwandten im – technisch betrachteten – Gegensatz zur Gruppe der eigenen Familie. Dieser Gruppe gehören Familienmitglieder wie der eigene Ehepartner oder Stiefkinder nicht an, wohl aber Personen außerhalb des – rechtlichen oder faktischen – Familienverbands, so z. B. Samenspender oder Frauen, die bei der Geburt ihres Kindes das eigene Kind nicht anerkannten und die Weitergabe der eigenen personenbezogenen Daten verweigerten, wobei dieses Recht in bestimmten Rechtssystemen auch anerkannt wird. Die letzteren Personengruppen gewährte Anonymität wirft eine weitere Frage auf, die in der Regel dadurch gelöst wird, dass personenbezogene Daten, die für Gentests erforderlich sind, ausschließlich einem Arzt zugänglich gemacht werden dürfen, dabei die Identität der betreffenden Person aber nicht offengelegt wird.

Angesichts der Komplexität der vorstehend angesprochenen Fragestellungen vertritt die Datenschutzgruppe die Auffassung, dass in der gegenwärtigen Phase einer fallweisen Entscheidung Vorrang bei der Frage eingeräumt werden sollte, wie mögliche Konflikte zwischen den Interessen der betroffenen Personen und den Interessen ihrer biologischen Familie beigelegt werden können.

Recht auf Nichtwissen: Das betrifft Fälle, in denen die in Frage stehende Person über die Ergebnisse der genetischen Tests nicht informiert werden will und auch keine weiteren Auskünfte wünscht (also nicht erfahren möchte, ob sie Träger eines defekten Gens ist oder mit dem Ausbruch einer Krankheit rechnen muss). Von besonderem Belang ist dies dann, wenn es sich um eine sehr ernste Krankheit handelt und es bislang keine wissenschaftlichen Präventions- oder Behandlungsmöglichkeiten gibt. Das Gleiche gilt für die Familienangehörigen, die ein Recht auf Nichtwissen geltend machen wollen, weil sie die Testergebnisse für ein Mitglied ihrer Familie bezüglich einer vorhandenen oder nichtvorhandenen ernsthaften genetischen Funktionsstörung – insbesondere dann, wenn es keine Präventions- oder Behandlungsmöglichkeiten gibt – lieber nicht erfahren möchten und stattdessen ein Leben bevorzugen, das nicht getrübt ist vom Wissen um eine derartige Veranlagung.

[6] Die Antragstellerin hatte die Herausgabe der Daten beantragt, um sich einem Gentest zu unterziehen und auf der Grundlage aller Informationen eine Entscheidung in der Frage ihrer Fortpflanzung zu treffen – und zwar unter Würdigung der Risiken der Vererbung einer Erbkrankheit, an der ihr Vater litt, auf eventuelle Nachkommen. Die von der Garante erteilte Genehmigung wurde auf der Grundlage der besonderen Merkmale genetischer Daten getroffen, die von einer Generation auf die nächste vererbt werden und damit das gemeinsame Erbe mehrerer Personen darstellen; die Empfehlung des Europarats wurde in der Entscheidung, die im Amtsblatt der Garante veröffentlicht wurde, ausdrücklich erwähnt (Cittadini e società dell'informazione 1999, Nr. 8, S. 13–15).

(Fallbeispiel: Die CNIL hält es für unangemessen, Familienangehörige von Trägern eines Gens, das eine unheilbare Krankheit auslösen kann, regelmäßig zu informieren und sie dadurch ständig in Sorge zu versetzen; dies hätte für sie keinen unmittelbaren Nutzen, da eine wirksame Behandlung in naher Zukunft nicht möglich ist.)

Beratung: Die Durchführung genetischer Tests wirft unweigerlich gewisse ethische und rechtliche Fragen auf. In dieser Hinsicht ist es sehr wichtig, dass die betroffenen Personen gut informiert sind, bevor sie eine Entscheidung treffen. Es könnten deshalb in bestimmten Fällen außergewöhnliche Bedingungen vorliegen, wie etwa für eine Frühberatung (z. B. für Paare, die sich vor dem Entschluss, ein Kind zu bekommen, einem Gentest unterziehen wollen). Dieser nicht unbedeutende Aspekt soll hier aber nicht näher erörtert werden.

- **Beschäftigung**

Vom Standpunkt des Arbeitgebers könnte die Verarbeitung genetischer Daten bereits vor der Einstellung von Mitarbeitern von Nutzen sein, da sich mit Hilfe dieser Daten besser feststellen lässt, welche Bewerber für eine bestimmte Tätigkeit nicht tauglich sind, z. B. aufgrund einer angegebenen Krankheit, oder ein relativ hohes Krankheitsrisiko haben, so dass diese Bewerber dann nicht eingestellt werden. Dem Arbeitnehmer können genetische Tests darüber Auskunft geben, ob er sich für eine spezielle Tätigkeit eignet und mit welchen Schutzmaßnahmen sich Verbesserungen am Arbeitsplatz erzielen lassen.

Die Datenschutzgruppe hatte Gelegenheit, die Verarbeitung genetischer Daten im Arbeitsumfeld auf der Grundlage des Konsultationspapiers über einen „gemeinschaftlichen Rahmen für den Schutz personenbezogener Daten von Arbeitnehmern im Arbeitsumfeld“ zu prüfen. In ihrer abschließenden Stellungnahme vom 24. September 2003 brachte die Datenschutzgruppe zum Ausdruck, dass die Verarbeitung genetischer Daten im Beschäftigungsbereich prinzipiell verboten werden sollte. Sie sollte nur dann zulässig sein, wenn wirklich außergewöhnliche Umstände vorliegen, auch unter Berücksichtigung des diesbezüglichen Verbots, das in einigen Mitgliedstaaten bereits in Kraft ist.

Wie bereits in der Stellungnahme der Europäischen Gruppe für Ethik in Naturwissenschaften und Neuen Technologien vom Juli 2003 zu den ethischen Aspekten von Gentests am Arbeitsplatz ausgeführt, „gibt es bislang keinerlei Beweise für die Relevanz und Reliabilität der bestehenden Gentests im Zusammenhang mit Beschäftigungsfragen. Ihre Aussagekraft ist nach wie vor zweifelhaft.“ Daher darf keinesfalls gestattet werden, dass Einzelpersonen auf der Grundlage von Informationen diskriminiert werden, die unter dem prädiktiven Gesichtspunkt in den meisten Fällen nicht als endgültig betrachtet werden sollten, denn einerseits hängt ihre Wirkung von dem Zusammenspiel mit anderen Faktoren ab, die z. B.

das Umfeld betreffen, und andererseits handelt es sich hier um probabilistische Informationen.

- **Versicherungen**

Die Datenschutzgruppe ist der Ansicht, dass die Verarbeitung genetischer Daten im Bereich der Versicherungen zum gegenwärtigen Zeitpunkt prinzipiell verboten werden sollte; sie sollte nur dann zulässig sein, wenn wirklich außergewöhnliche Umstände vorliegen, die per Gesetz eindeutig festgelegt sind. So könnte die Verwendung genetischer Daten im Versicherungsgewerbe beispielsweise dazu führen, dass ein Versicherungsantragssteller oder dessen Familienangehörige aufgrund des genetischen Profils diskriminiert werden. In einigen Fällen ist auch nicht auszuschließen, dass Versicherungsantragsteller infolge eines für sie ungünstigen Befundes aus einem Gentest exorbitante Versicherungsprämien zahlen müssen oder wegen einer möglichen Krankheit, die vielleicht niemals eintreten wird, sogar als nicht versicherbar gelten. Die von der Datenschutzgruppe vertretene Auffassung steht im Einklang mit der mehrheitlichen Position jener Mitgliedstaaten, in denen die Verarbeitung genetischer Daten im Bereich der Versicherungen keinen legitimen Zweck darstellt.

- **Medizinische und naturwissenschaftliche Forschung**

In den letzten Jahren sind große Mengen an genetischen Daten für Forschungszwecke erfasst und gespeichert worden. Dies dient hauptsächlich dazu, nach der Erforschung der DNA in der Genwissenschaft weitere Erkenntnisse über das menschliche Genom zu gewinnen und das Anwendungspotenzial in der Medizin zu vergrößern. Forschungsdatenbanken oder so genannte Biobanken haben sich für die Weiterentwicklung des Gesundheitswesens als äußerst hilfreich erwiesen.

Dennoch könnte die Einrichtung großer Genforschungsdatenbanken aus Sicht des Datenschutzes Anlass zur Sorge geben. Fragen in Bezug auf a) die Weiterverarbeitung der Daten zu Zwecken, an die zum Zeitpunkt ihrer Erhebung noch gar nicht zu denken war, b) die Speicherungsdauer für genetische Daten und c) die geeigneten Sicherheitsmaßnahmen sollten eingehend geprüft werden.

Biobanken sind ein Feld für fortlaufende Studien. Sind sie erst einmal eingerichtet, haben diese Datenbanken potenziell ein breit gefächertes Anwendungs- oder Nachfragespektrum. Es ist sogar festzustellen, dass die Anwendungsmöglichkeiten in der Forschung gegenüber einigen ursprünglich vorgesehenen Verwendungszwecken größtenteils nur eine sekundäre Rolle spielen. Da es in der Genetik vielschichtige Möglichkeiten der Forschungsfinanzierung gibt, wäre eine Vorhersage über das künftige Entwicklungstempo der Forschung in diesem Bereich zum gegenwärtigen Zeitpunkt unrealistisch.

Eine Möglichkeit, die Sicht des Datenschutzes in diese Problematik einzubeziehen, könnte darin bestehen, Vorschriften für entsprechende Anonymisierungsverfahren zu entwickeln.

Während eines bestimmten Zeitraums und zu Zwecken der Forschung scheint es jedenfalls notwendig zu sein, dass das Forschungspersonal in der Lage ist, die Daten mit der Person, von der sie stammen, in Verbindung zu bringen (um z. B. die Entwicklung einer Krankheit, die Reaktion auf eine Behandlung usw. beurteilen zu können). Außerdem lässt sich gespeicherte DNA nachweislich einer ganz bestimmten Person zuordnen – vorausgesetzt, es liegen in gewissem Umfang weitere Informationen vor; eine direkte, personenbezogene Speicherung ist jedoch nicht möglich. Eine von der dänischen Regierung eingesetzte Arbeitsgruppe, die die Notwendigkeit weiterer Gesetzesvorschläge in Dänemark beurteilen sollte, hat den Begriff *Biobank* definiert als *eine strukturierte Sammlung humanbiologischen Materials, die unter bestimmten Kriterien zugänglich ist,* ***wobei die in dem biologischen Material enthaltenen Informationen bis zu einzelnen Personen zurückverfolgt werden können***.

Die Frage der Speicherungsdauer für genetische Daten hängt auch damit zusammen, inwieweit das Anonymisierungsverfahren praktikabel ist. In der Regel können identifizierbare Merkmale nach einigen Jahren aus der Forschungsdatenbank entfernt werden; die Daten sind dann anonym und lassen sich definitiv nicht mehr mit einer bestimmbaren Person in Verbindung bringen. In Frankreich dürfen z. B. nach dem so genannten „Loi Huriet", einem am 20.12.1988 erlassenen Gesetz über klinische Versuche, Daten erst 15 Jahre nach ihrer Erhebung anonymisiert werden. Die niederländische Datenschutzbehörde hatte sich bereits mehrmals mit Fällen zu befassen, in denen eine Anonymisierung oder Löschung von Daten in Biobanken den Nutzen und die Funktionsfähigkeit dieser Datenbanken in erheblichem Maße zu beeinträchtigen drohte, denn man hätte die Daten dann nicht mehr bestimmbaren Personen zuordnen können. Beispiele dafür sind Forschungsdatenbanken für Längsschnittstudien, die mitunter mehrere Generationen umfassen, wie dies etwa bei der Registrierung von Krebserkrankungen geschieht. In diesen Fällen sollte die in Fachkreisen geführte Argumentation für längere Aufbewahrungszeiten berücksichtigt werden.

Eine weitere Frage betrifft die Sicherheitsmaßnahmen zum Schutz von Daten, die zu Zwecken der medizinischen und naturwissenschaftlichen Forschung verwendet werden. Hinsichtlich der Nutzung von Biobanken bedarf es strenger Sicherheitsvorkehrungen im Sinne des Artikels 17 der Richtlinie, d. h. es sind sowohl organisatorische als auch technische Maßnahmen erforderlich, um die betreffenden Daten zu schützen. Die Verantwortlichen für die Verarbeitung der Daten sollten z. B. dazu angehalten werden, Erhebungen über potenzielle Risiken durchzuführen, entsprechende Sicherheitskonzepte zu entwickeln, für eine ständige Information und Schulung der Mitarbeiter zu sorgen, Kontrollsysteme für einen

beschränkten Zugang einzuführen, um einen unbefugten Zugang durch Verwaltungspersonal oder andere Personen zu verhindern, usw.

- **Identifikation**

Genetische Daten haben sich in verschiedenen Bereichen als ein wichtiges Identifikationsmittel erwiesen. Das betrifft vor allem die Unterstützung polizeilicher Ermittlungen zur Identifizierung von Straftätern sowie die bessere Identifikation von Vermissten. In dem letztgenannten Fall ließe sich die Verarbeitung genetischer Daten, die ohne Einwilligung der betroffenen vermissten Person erfolgt, insofern rechtfertigen, als Umstände vorliegen, die ein vitales Interesse dieser Person begründen. Bei der Ermittlung von Straftaten ist nach dem Strafrecht einiger Mitgliedstaaten die Verarbeitung genetischer Daten von Verdächtigen auch ohne deren Einwilligung möglich.

Aus Sicht des Datenschutzes ist der wichtigste Bereich, in dem sich die Genetik zu Identifikationszwecken einsetzen lässt, die Durchführung von Tests zur Feststellung der Vaterschaft oder anderer Verwandtschaftsbeziehungen. In den meisten Fällen werden diese Tests durch eine zivilgerichtlichen Entscheidung angeordnet, und es bedarf einer ausdrücklichen Einwilligung der Betroffenen.

Im Internet gibt es jedoch inzwischen eine wachsende Flut von Seiten, die Gentests insbesondere zur Feststellung der Vaterschaft anbieten. Es handelt sich dabei um ein neuartiges technisches Verfahren, das auch unter der Bezeichnung „Gentests im Direktvertrieb“ oder „Gentests für zu Hause“ bekannt ist. Mit Hilfe eines solchen Tests lässt sich die Vaterschaft eines Kindes feststellen, indem man z. B. der betreffenden Person Proben entnimmt und per Post an ein Labor schickt, das diese dann analysiert. Aus dem Testergebnis geht hervor, ob der „Vater“ auch der genetische Vater des Kindes ist. Diese Dienstleistungen werden im Internet angeboten, und die benötigten Proben lassen sich unbemerkt entnehmen, wie z. B. eine Haarprobe von einem Kissen. Die Tatsache, dass die Probenahme möglicherweise unbemerkt bleibt, könnte also bedeuten, dass ein Gentest ohne das Wissen der betroffenen Person und folglich ohne ihre Einwilligung durchgeführt wird.

Um zu verhindern, dass genetisches Material ohne weiteres, d. h. ohne dass die betroffene Person etwas davon erfährt (und somit ohne ihre Einwilligung), gewonnen und für Vaterschaftstests weiterverarbeitet werden kann, bedarf es einer eindeutigen Regelung, die in einigen Mitgliedstaaten bereits existiert. Ferner sollten Ausnahmebestimmungen in diesem Bereich spezifische Garantien vorsehen, um die Interessen/Rechte der betroffenen Person zu wahren. So hat beispielsweise die niederländische Datenschutzbehörde entschieden, dass jede Person, bei der genetische Tests durchgeführt werden, eine Erklärung unterzeichnen sollte, aus der hervorgeht, dass die entnommenen DNA-Proben von ihr selbst stammen und dass sie in den Test einwilligt. In Bezug auf Tests bei Minderjähri-

gen sollten deren gesetzliche Vertreter eine entsprechende schriftliche Erklärung abgeben, in der sie jeweils persönlich in den Test einwilligen und bestätigen, dass die DNA-Proben von dem betreffenden Kind stammen. Der gesetzliche Vertreter sollte schließlich auch mitteilen, ob es noch weitere gesetzliche Vertreter gibt und, wenn dies der Fall ist, erklären, dass diese weiteren gesetzlichen Vertreter gegen den Gentest keine Einwände haben.

V. Fazit

Angesichts des hohen Tempos der technologischen, wissenschaftlichen und wirtschaftlichen Entwicklungen auf dem Gebiet der Genetik und unter Berücksichtigung des breiten Spektrums an Verwendungszwecken, zu denen genetische Daten verarbeitet werden können, hielt die Datenschutzgruppe die Zeit für gekommen, einen gemeinsamen Ansatz zu definieren, um geeignete Garantien für die Verarbeitung genetischer Daten festzulegen. Die wichtigsten Punkte dieses Ansatzes lassen sich wie folgt zusammenfassen:

- Die Verwendung genetischer Daten, die nicht unmittelbar dem Schutz der Gesundheit der betroffenen Person und der wissenschaftlichen Forschung dient, sollte generell an die Verpflichtung geknüpft sein, entsprechende nationale Vorschriften zu erlassen und umzusetzen, wobei die in der Richtlinie vorgesehenen Grundsätze des Datenschutzes und insbesondere die Grundsätze der Zweckbestimmung und der Verhältnismäßigkeit zu beachten sind. Nach diesen Grundsätzen ist eine pauschale Anwendung des genetischen Screenings auf breiter Basis rechtswidrig.

  Ferner sollte gemäß diesen Grundsätzen die Verarbeitung genetischer Daten in den Bereichen Beschäftigung und Versicherungen nur in ganz bestimmten, per Gesetz vorgesehenen Ausnahmefällen gestattet werden, um einzelne Personen vor Diskriminierungen aufgrund ihres genetischen Profils zu schützen.

  Da es ohne weiteres möglich ist, genetisches Material ohne das Wissen der betroffenen Person zu gewinnen und dann zu Informationszwecken zu untersuchen, bedarf es strenger Vorschriften, um die Gefahren in Verbindung mit neuen Formen von „Identitätsdiebstahl“ zu bannen, zumal die Risiken in diesem Bereich besonders groß wären, wenn man bedenkt, dass es vielleicht um Fragen der Vaterschaft und Mutterschaft geht und das Material sogar zum Zwecke des Klonens eingesetzt werden könnte. Man sollte deshalb bei Regelungen für genetische Daten nicht unberücksichtigt lassen, welcher rechtliche Status den DNA-Proben zukommt, die zur Gewinnung der in Frage stehenden Informationen dienen. In diesem Zusammenhang kommt es insbesondere darauf an, dass der betroffenen Person weitgehende Rechte eingeräumt werden, sowohl in Bezug auf den Umgang mit diesen Proben als auch im Hinblick auf deren Vernichtung und/oder Anonymisierung nach Gewinnung der benötigten Informationen.

Notwendig sind schließlich auch entsprechende Verfahrensregeln, die sicherstellen, dass genetische Daten nur unter der Aufsicht von Fachleuten verarbeitet werden, die über geeignete Qualifikationen verfügen und aufgrund spezifischer Befugnisse und Vorschriften zur Verarbeitung dieser Daten berechtigt sind.

- In Mitgliedstaaten, in denen die Zwecke sowie die geeigneten Garantien für die Verarbeitung genetischer Daten nicht per Gesetz geregelt sind, sollten die Datenschutzbehörden umso stärker darauf hinwirken, dass die in der Richtlinie verankerten Grundsätze der Zweckbestimmung und der Verhältnismäßigkeit vollständig respektiert werden.

  In dieser Hinsicht empfiehlt die Datenschutzgruppe den Mitgliedstaaten, bei der Verarbeitung genetischer Daten die Möglichkeit einer Vorabkontrolle durch die Datenschutzbehörden gemäß Artikel 20 der Richtlinie zu prüfen. Dies sollte insbesondere bei der Einrichtung und Nutzung von Biobanken geschehen.

  Darüber hinaus ließe sich im Bereich des „Online-Direktvertriebs von Gentests", für den es keinen rechtlichen Rahmen gibt, einiges bewirken, wenn die Datenschutzbehörden enger zusammenarbeiten und sich über vorbildliche Verfahren austauschen.

- Nicht unerwähnt bleiben sollte hier die Entstehung einer neuen, rechtlich relevanten sozialen Gruppe: Die Rede ist von der biologischen Gruppe, der Gruppe der Verwandten, die rein technisch gewissermaßen den Gegenpol zur Familie bildet. Diese Gruppe schließt nicht nur bestimmte Familienmitglieder wie etwa Ehepartner oder Pflegekinder ein, sondern – rechtlich oder tatsächlich – möglicherweise auch Personen außerhalb des Familienkreises (z. B. Gametenspender).

Die Datenschutzgruppe beabsichtigt, dieses Arbeitspapier nach einer gewissen Zeit zu überarbeiten, um die von den Datenschutzbehörden gesammelten Erfahrungen im Hinblick auf die Verarbeitung genetischer Daten berücksichtigen zu können. Der vorliegende Text sollte als eine Ausgangsbasis für weitere Diskussionen über die anstehenden Fragen betrachtet werden. Die Datenschutzgruppe wird die diesbezüglichen Entwicklungen genau verfolgen und dann möglicherweise entscheiden, sich zu einem späteren Zeitpunkt eingehend mit spezifischen Bereichen zu befassen, um mit dem technologischen Fortschritt bei der Verarbeitung genetischer Daten Schritt zu halten.

Geschehen zu Brüssel, am 17. März 2004

Im Namen der Arbeitsgruppe
Der Vorsitzende
Peter Schaar

Stellungnahme 9/2004 vom 9. November 2004 (WP 99) zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus (Ratsdokument 8958/04 vom 28.4.2004)

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

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

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

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14 –

hat folgende Stellungnahme angenommen:

In den letzten Jahren hat die Datenschutzgruppe sich wiederholt zur Speicherung von Telekommunikationsverkehrsdaten[2] geäußert, und die Konferenz der europäischen Datenschutzbeauftragten hat mehrere gemeinsame Erklärungen zu diesem

[1] Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/law/index.htm

[2] Siehe: Empfehlung 3/97 über Anonymität im Internet; Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs; Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke; Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000, KOM(2000) 385; Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität; Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus; Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.–11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation; Stellungnahme1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung. Der Anhang dieser Stellungnahme enthält eine Zusammenfassung dieser Papiere. Außerdem sind alle Unterlagen abrufbar unter http://europa.eu.int/comm/internal_market/privacy.

Thema abgegeben[3]. Der Vorschlag für einen Rahmenbeschluss über die Vorratsspeicherung solcher Verkehrsdaten, den vier Mitgliedstaaten dem Rat der Europäischen Union vorgelegt haben, erfordert erneut eine Stellungnahme der Datenschutzgruppe. Da sich die Erörterungen in der zuständigen Arbeitsgruppe des Rates noch im Anfangsstadium befinden, hat diese Stellungnahme vorläufigen Charakter. Die Datenschutzgruppe hat die Absicht, die Frage zu einem späteren Zeitpunkt auf der Grundlage eines überarbeiteten Entwurfes erneut zu prüfen.

Die Datenschutzgruppe hat den Entwurf auf seine Vereinbarkeit mit Artikel 8 der Europäischen Menschenrechtskonvention hin geprüft.

In diesem Zusammenhang muss berücksichtigt werden, dass die Bürger für alltägliche Tätigkeiten zunehmend elektronische Kommunikationsnetze und -dienste nutzen. Die bei dieser Form der Kommunikation generierten Daten, die so genannten „Verkehrsdaten", können Informationen über Ort, Zeitpunkt und Gesprächspartner von Mobil- oder Festnetztelefongesprächen, Telefaxkommunikation, E-Mails, SMS und anderen Formen der Internetkommunikation enthalten und daher in zunehmendem Maße die Lebensführung der Nutzer widerspiegeln.

In ihrer *Empfehlung 2/99 vom 3. Mai 1999 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs* definierte die Datenschutzgruppe die Überwachung des Fernmeldeverkehrs als die Kenntnisnahme von Inhalt von und/oder Daten im Zusammenhang mit privaten Telekommunikationsverbindungen zwischen zwei oder mehreren Teilnehmern durch einen Dritten, insbesondere der mit der Telekommunikationsnutzung verbundenen Verkehrsdaten. In diesem Zusammenhang stellte die Datenschutzgruppe seinerzeit auch fest, dass jede Überwachung des Fernmeldeverkehrs (einschließlich der Überwachung und des Data Mining von Verkehrsdaten) eine Verletzung des Rechts von Einzelpersonen auf Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstelle. Daraus folgt, dass Überwachungen abzulehnen sind, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen.

Nach Auffassung der Datenschutzgruppe gelten dieselben grundlegenden Erfordernisse für die Speicherung von Verkehrsdaten, soweit sie über das für die

[3] Siehe in Stockholm (April 2000) und Cardiff (2002) angenommene Erklärungen.

Erbringung der Kommunikationsdienstleistungen und andere legitime Geschäftszwecke Notwendige hinausgehen, sowie für jeden anschließenden Zugriff auf diese Daten für Strafverfolgungszwecke[4].

Die Datenschutzgruppe bezweifelt ernsthaft, dass der Beschlussentwurf diese Grundanforderungen erfüllt. Was das erste Erfordernis (gesetzliche Grundlage) betrifft, so hält sie es nicht für sinnvoll, zum jetzigen Zeitpunkt darauf einzugehen, da sich die Diskussionen im Rat noch in einem sehr frühen Stadium befinden. Mit Blick auf das dritte Erfordernis (notwendig zum Schutz legitimer, in der Konvention aufgeführter Interessen) stellt die Datenschutzgruppe das eigentliche Ziel des Entwurfs in Frage. Soll er wirklich nur wie angegeben (Erwägungsgrund 7) der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten dienen, und sind andere Ziele des Artikels 8 ausgeschlossen? Das Ziel muss zuallererst klar sein.

Zum zweiten Kriterium (in einer demokratischen Gesellschaft notwendig) ist zu sagen, dass die Speicherung gemäß der Auslegung des EGMR einem zwingenden gesellschaftlichen Bedarf („pressing social need“) entspringen muss (siehe unter anderem Urteil in der Sache Klass gegen Bundesrepublik Deutschland vom 18. November 1977, Europäischer Gerichtshof für Menschenrechte, Reihe A, Nr. 28). Der Gerichtshof für Menschenrechte hat zwar die Befugnis der Vertragsstaaten anerkannt, in Ausnahmefällen und unter besonderen Umständen die Korrespondenz und Telekommunikation von Personen auch heimlich zu überwachen. Er hat aber hinzugefügt:

„… dies bedeutet nicht, dass die Vertragsstaaten ein unbeschränktes Ermessen haben, Personen in ihrem Hoheitsgebiet einer heimlichen Überwachung zu unterwerfen. Angesichts der Tatsache, dass entsprechende Befugnisse mit der Begründung, die Demokratie verteidigen zu wollen, diese gerade zu unterminieren oder zu zerstören drohen, betont der Gerichtshof, dass die Vertragsstaaten zur

[4] Diese Sichtweise wird von der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte gestützt. Dieser hat beispielsweise in seinem Amann-Urteil (S. 30 ff.) festgestellt, dass bereits die Speicherung von Informationen einen Grundrechtseingriff darstelle, unabhängig davon, ob diese Daten gegen die betroffene Person verwendet werden oder nicht. Auch im Rotaru-Urteil hat er die Speicherung historischer Daten durch den Geheimdienst als Eingriff in die Grundrechte eingestuft. Im Urteil PG gegen UK (S. 42 ff.) hat der Gerichtshof die Auffassung vertreten, die Erfassung des Fernmeldeverkehrs verstoße nicht per se gegen Artikel 8, beispielsweise dann nicht, wenn sie durch die Telefongesellschaft für Abrechnungszwecke vorgenommen werde. Hingegen stelle der Zugriff der Polizei auf Informationen des Providers über angerufene Nummern einen Eingriff in die Privatsphäre oder das Fernmeldegeheimnis dar. Im Fall Malone (S. 84 ff.) vertrat der Gerichtshof ebenfalls die Auffassung, dass die Weitergabe solcher Daten von der Telefongesellschaft an die Polizei einen Eingriff in das Recht auf Schutz der „Korrespondenz“ nach Artikel 8 darstelle. Aus diesen Fällen könnte man ableiten, dass die Verpflichtung der Telekom-Gesellschaften zur Speicherung von Verkehrsdaten als solche nicht gegen Artikel 8 verstößt, die Weiterverarbeitung dieser Daten oder ihre Weitergabe an die Behörden indessen sehr wohl im Widerspruch dazu steht. Diese Schlussfolgerung wäre falsch. In der Sache MM. gegen Niederlande stellte der Gerichtshof fest, dass die Behörden die Haftbarkeit nicht umgehen können, indem sie Privatpersonen einsetzen, wenn sie einen wesentlichen Beitrag zur Ausführung der Überwachung leisten. Dies würde mithin bedeuten, dass beispielsweise Datenspeicherung und Data Mining für die Zwecke der öffentlichen Ordnung durch die Telekom-Gesellschaften in ihren eigenen Systemen ebenfalls einen Eingriff in die Grundrechte darstellen.

Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten“ (Klass, S. 3).

Die im Beschlussvorschlag vorgesehene Verpflichtung zur routinemäßigen, flächendeckenden Vorratsspeicherung sämtlicher Verkehrs-, Nutzer- und Teilnehmerdaten würde die ausnahmsweise zulässige Überwachung zur evident unverhältnismäßigen Regel machen. Der vorgeschlagene Beschluss wäre nicht nur auf einzelne Personen anwendbar, die auf Grund besonderer Gesetze überwacht würden, sondern auf alle Personen, die die elektronische Kommunikation nutzen. Ferner würden alle versandten oder empfangenen Mitteilungen erfasst. Nicht alles, was sich für die Strafverfolgung als nützlich erweisen könnte, ist wünschenswert oder kann als in einer demokratischen Gesellschaft notwendig angesehen werden, zumal wenn es zu einer systematischen Registrierung der gesamten elektronischen Kommunikation führt. Dass eine so umfängliche Speicherung von Verkehrsdaten der einzig gangbare Weg zur Bekämpfung der Kriminalität oder zur Wahrung der nationalen Sicherheit ist, dafür liefert der Rahmenbeschluss keinerlei überzeugenden Argumente. Mit der Verpflichtung der Provider zur Speicherung von Verkehrsdaten, die sie nicht für eigene Zwecke benötigen, würde der Grundsatz der Zweckbindung in beispielloser Weise durchbrochen.

Untersuchungen europäischer Telefongesellschaften haben gezeigt, dass das Gros der von Strafverfolgungsbehörden abgerufenen Daten nicht älter als sechs Monate war. Das belegt, dass längere Aufbewahrungsfristen eindeutig unverhältnismäßig sind.

Es soll darauf hingewiesen werden, dass die Vertreter der Strafverfolgungsbehörden bisher jeglichen Nachweis für die Notwendigkeit so weit reichender Maßnahmen schuldig geblieben sind. Es fällt auf, dass sie bei den in jüngster Zeit veranstalteten Workshops, bei denen Hintergrund und Folgen des Beschlussentwurfes beleuchtet werden sollten, ausnahmslos durch Abwesenheit geglänzt haben.

Die Konvention zur Bekämpfung der Datennetzkriminalität (Cybercrime-Konvention) sieht nur eine einzelfallbezogene Sicherungsspeicherung nach dem Modell des „fast freeze – quick thaw“ vor, das entgegen der Auffassung der vier Regierungen, die den Rahmenbeschluss vorschlagen, durchaus geeignet ist, Straftaten zu verhüten oder sie zu verfolgen. Es ist bezeichnend für die gegenwärtige rechtspolitische Diskussion, dass der jetzt gemachte Vorschlag ernsthaft erörtert wird, noch bevor die Cybercrime-Konvention in den meisten Unterzeichnerstaaten in Kraft getreten ist und in ihren praktischen Auswirkungen bewertet werden kann. Die Artikel-29-Gruppe hat bereits in ihrer Stellungnahme 5/2002 festgestellt, dass bei der Aufbewahrung von Verkehrsdaten für Zwecke der Strafverfolgung die Bedingungen des Artikels 15 Absatz 1 der Richtlinie 2002/58/EG strikt einzuhalten sind, d. h. in jedem Einzelfall ist die Aufbewahrung nur während einer begrenzten Zeit und nur wenn dies in einer demokratischen Gesell-

schaft notwendig, angemessen und verhältnismäßig ist, zulässig. Auch die europäischen Datenschutzbeauftragten haben sich auf ihrer Internationalen Konferenz in Cardiff (9.–11. September 2002) zur zwangsweisen systematischen Speicherung von Verkehrsdaten der Telekommunikation geäußert. Sie erklärten, dass die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger eindeutig unverhältnismäßig und deshalb abzulehnen wäre.

Der Entwurf des Rahmenbeschlusses wird diesen Anforderungen nicht nur nicht gerecht, es wird damit versucht, sie explizit außer Kraft zu setzen, indem kein konkreter Tatverdacht und keine hinreichend sichere Tatsachenbasis im Einzelfall gefordert werden, sondern die Vorratsspeicherung pauschal und präventiv für eine mögliche zukünftige Strafverfolgung zulasten aller, die elektronische Kommunikationsnetze nutzen, angeordnet werden soll.

Die Datenschutzgruppe hält die Pflichtspeicherung aller Arten von Verkehrsdaten der Telekommunikation für Zwecke der öffentlichen Ordnung unter den im Beschlussentwurf vorgesehenen Bedingungen für eindeutig unverhältnismäßig und deshalb für unzulässig nach Artikel 8 der Menschenrechtskonvention.

Geschehen zu Brüssel am 9. November 2004

Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar

ANHANG

Zusammenfassung der Erklärungen der Artikel-29-Datenschutzgruppe zur Speicherung von Telekommunikationsverkehrsdaten

Empfehlung 3/97 zur Anonymität im Internet

In Empfehlung 3/97 über Anonymität im Internet hat die Artikel-29-Datenschutzgruppe erklärt, dass, auch wenn Verkehrsdaten in einigen Rechtsordnungen in gewissem Umfang durch das Brief- und Fernmeldegeheimnis geschützt sind, die massive Zunahme solcher Daten Anlass zu berechtigter Sorge gibt. In dem Maße wie Onlinedienste leistungsfähiger und beliebter werden, wird sich auch das Problem der Transaktionsdaten ausweiten. Wenn immer mehr Alltagstätigkeiten online abgewickelt werden, wird immer mehr von dem, was wir tun, erfasst.

Allein durch ihr Vorhandensein schaffen identifizierbare Transaktionsdaten ein Instrument, mit dem das Verhalten des Einzelnen mit beispielloser Intensität überwacht und kontrolliert werden kann. Nach Auffassung der Datenschutzgruppe sollten Regierungen und Behörden im Internet nicht mehr Möglichkeiten zur Einschränkung der Rechte des Einzelnen und zur Überwachung potenziell rechtswidrigen Verhaltens haben als in der Offline-Welt.

Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs, angenommen am 3. Mai 1999

In ihrer Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs (einschließlich Monitoring und Data Mining von Verkehrsdaten) vom 3. Mai 1999 hat die Datenschutzgruppe sich mit dem Verhältnis von Fernmeldeüberwachung und Grundrechten auseinandergesetzt. Dabei hat sie die Überwachung des Fernmeldeverkehrs definiert als die Kenntnisnahme von Inhalt von und/oder Daten im Zusammenhang mit privaten Telekommunikationsverbindungen zwischen zwei oder mehreren Teilnehmern durch einen Dritten, insbesondere der mit der Telekommunikationsnutzung verbundenen Verkehrsdaten. Sie hat betont, dass jede Überwachung des Fernmeldeverkehrs eine Verletzung des Rechts von Einzelpersonen auf Schutz der Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstellt. Aus diesem Grund sind Überwachungen abzulehnen, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen.

In diesem rechtlichen Kontext müssen breit angelegte erkundende oder allgemeine Überwachungen verboten sein. Die Datenschutzgruppe verweist insbesondere auf die Fälle Leander und Klass, in denen der Gerichtshof festgestellt hatte, dass ausreichende Garantien benötigt würden, die einen Missbrauch ausschließen, da ein geheimes Überwachungssystem zum Schutz der nationalen Sicherheit das Risiko in sich berge, die Demokratie unter dem Vorwand, sie zu verteidigen, zu unterminieren, wenn nicht gar zunichte zu machen. Im Urteil Klass kam der Gerichtshof zu dem Schluss, dass die einschlägigen deutschen Rechtsvorschriften nicht gegen Artikel 8 der Europäischen Menschenrechtskonvention verstießen, da sie nur eine Überwachung bestimmter verdächtiger Personen oder deren mutmaßlicher Kontaktpersonen zuließen. Die Datenschutzgruppe führt in dieser Empfehlung (Ziff. 9) die Anforderungen auf, die einzelstaatliche Rechtsvorschriften über Telefonüberwachungen erfüllen müssen.

Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke, angenommen am 7. September 1999

Die Pflicht zur Löschung oder Anonymisierung von Verkehrsdaten ist durch die Sensibilität dieser Daten begründet, die individuelle Kommunikationsprofile offen legen, einschließlich Informationsquellen und Aufenthaltsorten der Benutzer von Festnetz- oder Mobiltelefonen, sowie durch die potenzielle Bedrohung der Privatsphäre durch das Sammeln, die Offenlegung oder die Weiterverwendung solcher Daten.

Die Datenschutzgruppe merkt an, dass die gesetzlich zulässigen Speicherzeiträume von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich sind. Sie empfiehlt, nicht zuzulassen, dass Verkehrsdaten allein für Strafverfolgungszwecke aufgehoben werden, und die Dienstanbieter nicht zu verpflichten, die Daten länger aufzubewahren, als es für Abrechnungszwecke notwendig ist, und spricht sich für eine weitere Harmonisierung des Aufbewahrungszeitraums in der EU aus.

Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 – KOM (2000) 385, angenommen am 2. November 2000

Verkehrsdaten wie zum Beispiel URLs können Aufschluss über persönliche Interessen geben (unter anderem durch Hinweise auf religiöse Überzeugung, politische Meinung, Gesundheit oder Sexualleben). Diese Daten sollten mit der für die Kommunikation geltenden Vertraulichkeit behandelt werden.

Ein weiterer, noch zu erörternder Aspekt, der von der Datenschutzgruppe angesprochen wird, ist, dass einige dieser Daten auch als sensible Daten im Sinne des Artikels 8 der allgemeinen Datenschutzrichtlinie 95/46/EG angesehen werden könnten, die prinzipiell nicht verarbeitet werden dürfen.

Angesichts der weitgefassten Definition der Verkehrsdaten vertritt die Gruppe die Auffassung, dass es nicht unbedingt akzeptabel ist, wenn alle Verkehrsdaten auf die gleiche Weise behandelt werden. Einige Arten von Verkehrsdaten benötigen unter Umständen mehr Schutz als andere.

Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität, angenommen am 22. März 2001

Wenn das Verfahrensrecht harmonisiert wird, muss auch die Angleichung der Garantien und Voraussetzungen für die darauf gestützten Maßnahmen in Betracht gezogen werden. Auch in diesem Zusammenhang hat die Datenschutzgruppe betont, dass eine allgemeine Überwachungspflicht in Form der routinemäßigen Speicherung von Verkehrsdaten, wie sie ursprünglich in der Cybercrime-Konvention (Version 25) vorgeschlagen worden war, einen unzulässigen Eingriff in die in Artikel 8 der Europäischen Menschenrechtskonvention garantierten Grundrechte darstellen würde.

Außerdem wäre denkbar, dass die Wirtschaft mehr Rechtssicherheit benötigt wenn es darum geht, wem wann Zugang zu vertraulichen Informationen und vertraulicher Kommunikation zu gewähren ist.

Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus

In *der am 14. Dezember 2001 angenommenen Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus* erklärt die Datenschutzgruppe, die Bekämpfung des Terrorismus sei ein notwendiges und gültiges Anliegen einer demokratischen Gesellschaft. Aber bei diesem Kampf müssten bestimmte Bedingungen beachtet werden, die ebenfalls elementarer Bestandteil unserer demokratischen Gemeinwesen sind. Die Datenschutzgruppe ist sich der Ernsthaftigkeit des Terrorismusproblems durchaus bewusst – eines Phänomens, mit dem Europa schon geraume Zeit konfrontiert ist. Sie hält indessen langfristige Überlegungen für erforderlich über Maßnahmen, die lediglich nur „nützlich“ oder „wünschenswert“ sind, wie beispielsweise die flächendeckende anlassunabhängige Vorratsspeicherung von Telekommunikationsdaten. Die Maßnahmen dürfen Grundrechte und Grundfreiheiten nicht einschränken. Ein wichtiges Element des Kampfes gegen den Terrorismus ist, dass wir die grundlegenden Werte bewahren, auf denen unsere Demokratien basieren, denn

genau diese Werte wollen diejenigen zerstören, die den Einsatz von Gewalt propagieren.

Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzbeauftragten auf der internationalen Konferenz in Cardiff (9. – 11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation, angenommen am 11. Oktober 2002

Die Datenschutzgruppe hat die Berechtigung und die Rechtmäßigkeit der zwangsweisen systematischen Speicherung von Verkehrsdaten, um einen möglichen Zugang durch Strafverfolgungs- und Sicherheitsorgane zu gestatten, ernsthaft in Zweifel gezogen.

Eine lange und harte Auseinandersetzung über die Regelung dieser Frage in Richtlinie 2002/58/EG führte zur Festlegung strenger Voraussetzungen für die Speicherung von Verkehrsdaten für Strafverfolgungszwecke in Artikel 15 Absatz 1 der Richtlinie; danach sollte die Speicherung in jedem Fall nur befristet erfolgen dürfen und nur, wenn es in einer demokratischen Gesellschaft angemessen und verhältnismäßig ist. Die Datenschutzgruppe stellt fest, dass die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger eindeutig unverhältnismäßig und deshalb abzulehnen wäre.

Außerdem erklärte sie, sie erwarte vor der Verabschiedung von Maßnahmen, die sich in Bereichen ergeben könnten, die unter die dritte Säule fallen, gehört zu werden.

Stellungnahme 1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung, angenommen am 29. Januar 2003

In *der am 20. Januar 2003 angenommenen Stellungnahme 1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung* gibt die Datenschutzgruppe Orientierungshilfe für die Harmonisierung des Zeitraums, in dem die Verwendung von Verkehrsdaten für Abrechnungszwecke gesetzlich zulässig ist. Für Abrechnungszwecke sollten die Daten normalerweise nicht länger als drei bis sechs Monate gespeichert werden. Verarbeitet werden dürfen nur solche Verkehrsdaten, die dem Zweck angemessen und dafür relevant sind und nicht über das Notwendige hinausgehen. Andere Verkehrsdaten müssen gelöscht oder anonymisiert werden.

Vorgehensweisen, die nicht mit diesen Grundsätzen übereinstimmen, und Praktiken, die nicht eindeutig gemäß Artikel 15 der Richtlinie 2002/58/EG gesetzlich zugelassen sind, sind prima facie mit den Anforderungen der Datenschutzrichtlinie unvereinbar.

2. Europäische Kommission

Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG)

(ABl. EG vom 29. Dezember 2004, L 385/74)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN –

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], insbesondere auf Artikel 26 Absatz 4,

in Erwägung nachstehender Gründe:

(1) Um die Aufrechterhaltung der Datenströme aus der Gemeinschaft zu erleichtern, ist es wünschenswert, dass die für die Verarbeitung Verantwortlichen in der Gemeinschaft Daten weltweit auf der Grundlage derselben Datenschutzregeln übermitteln können. Solange es keine globalen Datenschutznormen gibt, sind Standardvertragsklauseln ein wichtiges Instrument, das die Übermittlung personenbezogener Daten aus allen Mitgliedstaaten nach denselben Regeln ermöglicht. Die Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG[2] legt daher Standardvertragsklauseln fest, die angemessene Garantien für die Übermittlung von Daten in Drittländer bieten.

(2) Seit Verabschiedung dieser Entscheidung wurden viele Erfahrungen gesammelt. Darüber hinaus haben mehrere Wirtschaftsverbände[3] gemeinsam alternative Standardvertragsklauseln entworfen, die ein Datenschutzniveau gewährleisten sollen, das dem Niveau der Standardvertragsklauseln

[1] ABl. L 281 vom 23.11.1995, S. 31. Richtlinie geändert durch die Verordnung (EG) Nr. 1882/2003 (ABl. L 284 vom 31.10.2003, S. 1).

[2] ABl. L 181 vom 4.7.2001, S. 19.

[3] Internationale Handelskammer (ICC), Japan Business Council in Europe (JBCE), Europäische Verband der informations- und kommunikationstechnischen Industrie (EICTA), EU-Ausschuss der Amerikanischen Handelskammer in Belgien (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT), Federation of European Direct Marketing Associations (FEDMA).

in der Entscheidung 2001/497/EG vergleichbar ist, auch wenn dabei andere Instrumente eingesetzt werden.

(3) Da die Verwendung von Standardvertragsklauseln bei internationalen Datenübermittlungen freiwillig erfolgt und nur eine Möglichkeit gemäß der Richtlinie 95/46/EG darstellt, personenbezogene Daten auf rechtlich zulässige Weise in ein Drittland zu übermitteln, sollte es Datenexporteuren in der Gemeinschaft und Datenimporteuren in Drittländern freistehen, Daten unter Verwendung eines der Standardverträge zu übermitteln oder aber sich auf eine andere Rechtsgrundlage zu stützen. Da jeder Standardvertrag in sich geschlossen ist, sollte es den Datenexporteuren allerdings nicht erlaubt werden, die Standardverträge zu ändern bzw. verschiedene Standardverträge miteinander zu kombinieren.

(4) Die Standardvertragsklauseln der Wirtschaftsverbände sollen die Wirtschaftsteilnehmer zur intensiveren Nutzung von Vertragsklauseln veranlassen; zu diesem Zweck setzen sie auf Instrumente wie flexiblere Prüfungspflichten oder präzisere Regelung des Auskunftsrechts.

(5) Als Alternative zur gesamtschuldnerischen Haftung gemäß der Entscheidung 2001/497/EG beinhaltet der nun vorgelegte Standardvertrag außerdem ein auf die Sorgfaltspflicht abstellendes Haftungssystem, das Datenexporteur und Datenimporteur gegenüber der betroffenen Person für die Verletzung ihrer jeweiligen Vertragspflichtenhaftbar macht; ebenso ist der Datenexporteur haftbar, wenn er sich nicht im Rahmen des Zumutbaren davon überzeugt, dass der Datenimporteur seine Rechtspflichten aus den Klauseln zu erfüllen in der Lage ist (Auswahlverschulden – *culpa in eligendo*), in welchem Fall die betroffene Person gerichtlich gegen den Datenexporteur vorgehen kann. Die Durchsetzung von Klausel I Buchstabe b) des neuen Standardvertrags ist in dieser Hinsicht besonders wichtig, vor allem im Hinblick auf das Recht des Datenexporteurs, Prüfungen in den Räumlichkeiten des Datenimporteurs durchzuführen oder Nachweise zu verlangen, dass dieser über genügend Finanzmittel verfügt, um seinen Verpflichtungen nachzukommen.

(6) Für den Fall, dass die betroffene Person ihre Rechte als Drittbegünstigte ausübt, wird der Datenexporteur bei der Beschwerdeabhilfe stärker zur Verantwortung gezogen; der Datenexporteur ist nämlich verpflichtet, Kontakt zum Datenimporteur aufzunehmen und die Einhaltung der Vertragspflichten nötigenfalls innerhalb der Standardfrist von einem Monat durchzusetzen. Falls der Datenexporteur sich weigert, die Einhaltung der Vertragspflichten durchzusetzen, und der Datenimporteur seine Vertragspflichten weiter verletzt, kann die betroffene Person die Einhaltung der Klauseln gegenüber dem Datenimporteur erzwingen und ihn in einem Mitgliedstaat

gerichtlich belangen. Die Anerkennung einer gerichtlichen Zuständigkeit und der Entscheidung des zuständigen Gerichts oder einer Kontrollstelle schmälert in keiner Weise die prozessualen Rechte des in einem Drittland ansässigen Datenimporteurs, z. B. sein Recht auf Einlegung von Rechtsmitteln.

(7) Damit diese zusätzliche Flexibilität jedoch nicht missbraucht wird, erscheint es angebracht, dass die Datenschutzkontrollstellen auf der Grundlage des neuen Standardvertragsklauseltyps Datenübermittlungen leichter verbieten oder aussetzen können, falls sich der Datenexporteur weigert, gegenüber dem Datenimporteur geeignete Maßnahmen zur Durchsetzung der Vertragspflichten zu ergreifen, oder der Datenimporteur sich weigert, redlich mit den zuständigen Datenschutzkontrollstellen zusammenzuarbeiten.

(8) Die aufgrund der Richtlinie 95/46/EG oder der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[4] erlassenen Vorschriften bleiben von den Standardvertragsklauseln unberührt, insbesondere was den Versand kommerzieller Kommunikation für Direktmarketingzwecke betrifft.

(9) Auf dieser Grundlage können die Garantien, die die vorgelegten Standardvertragsklauseln beinhalten, als angemessen im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG angesehen werden.

(10) Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die nach Artikel 29 der Richtlinie 95/46/EG eingesetzt wurde, hat eine Stellungnahme[5] zu dem Schutzniveau abgegeben, das die vorgelegten Standardvertragsklauseln bieten; diese Stellungnahme wurde bei der Ausarbeitung dieser Entscheidung berücksichtigt.

(11) Um die Anwendung der Änderungen an der Entscheidung 2001/497/EG bewerten zu können, sollte die Kommission diese drei Jahre, nachdem sie die Mitgliedstaaten davon in Kenntnis gesetzt hat, bewerten.

(12) Die Entscheidung 2001/497/EG sollte entsprechend geändert werden.

(13) Die in dieser Entscheidung vorgesehenen Maßnahmen entsprechen der Stellungnahme des Ausschusses, der gemäß Artikel 31 der Richtlinie 95/46/EG eingesetzt wurde –

---

[4] ABl. L 201 vom 31.7.2002, S. 37.

[5] Stellungnahme 8/2003, siehe http://europa.eu.int/comm/privacy/

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

Die Entscheidung 2001/497/EG wird wie folgt geändert:

1. In Artikel 1 wird folgender Absatz hinzugefügt:

   „Die für die Verarbeitung Verantwortlichen haben die Wahl zwischen Standardvertrag I und II im Anhang. Sie dürfen die Klauseln weder ändern noch Klauseln aus beiden Verträgen miteinander kombinieren."

2. Artikel 4 Absätze 2 und 3 erhalten folgende Fassung:

   „(2) Für die Zwecke von Absatz 1 können die zuständigen Kontrollstellen, sofern der für die Verarbeitung Verantwortliche angemessene Garantien auf der Grundlage des Standardvertrags II im Anhang geltend macht, im Rahmen ihrer Befugnisse Datenübermittlungen verbieten oder aussetzen, wenn

   a) der Datenimporteur sich weigert, mit den Datenschutzkontrollstellen redlich zusammenzuarbeiten oder eindeutige Vertragspflichten zu erfüllen;

   b) der Datenexporteur sich weigert, binnen der Regelfrist von einem Monat nach entsprechender Aufforderung durch die zuständige Kontrollstelle geeignete Maßnahmen zur Durchsetzung der Vertragspflichten gegenüber dem Datenimporteur zu ergreifen.

   Eine Weigerung des Datenimporteurs zur redlichen Zusammenarbeit oder zur Durchsetzung der Vertragspflichten im Sinne von Unterabsatz 1 besteht nicht, wenn die Zusammenarbeit oder Durchsetzung zu einer Kollision mit nationalen, für den Datenimporteur verbindlichen Rechtsvorschriften führen würde und diese Vorschriften nicht über das hinausgehen, was in einer demokratischen Gesellschaft unter Zugrundelegung der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgeführten Interessen erforderlich ist; hierunter fallen insbesondere die Androhung von Sanktionen nach internationalem und/oder nationalem Recht, steuerrechtliche Anzeigepflichten oder Anzeigepflichten zur Bekämpfung der Geldwäsche.

   Die Pflicht zur Zusammenarbeit im Sinne von Unterabsatz 1 Buchstabe a) beinhaltet für den Datenimporteur insbesondere die Bereitschaft, seine Datenverarbeitungseinrichtungen überprüfen zu lassen oder den Empfehlungen der Datenschutzkontrollstelle in der Gemeinschaft Folge zu leisten.

(3) Das Verbot oder die Aussetzung im Sinne der Absätze 1 und 2 wird aufgehoben, sobald die Gründe für das Verbot oder die Aussetzung nicht mehr vorliegen.

(4) Wenn die Mitgliedstaaten Maßnahmen gemäß den Absätzen 1, 2 und 3 ergreifen, informieren sie unverzüglich die Kommission, die ihrerseits die Informationen an die anderen Mitgliedstaaten weiterleitet.“.

3. Artikel 5 Satz 1 erhält folgende Fassung:

„Die Kommission bewertet drei Jahre, nachdem sie den Mitgliedstaaten diese Entscheidung und etwaige Änderungen an dieser Entscheidung bekannt gegeben hat, ihre Durchführung anhand der verfügbaren Informationen.“.

4. Der Anhang wird wie folgt geändert:

1. Nach der Überschrift wird „STANDARDVERTRAG I“ eingefügt.

2. Der Wortlaut des Anhangs zu dieser Entscheidung wird angefügt.

Artikel 2

Diese Entscheidung gilt ab dem 1. April 2005.

Artikel 3

Diese Entscheidung ist an die Mitgliedstaaten gerichtet.

Brüssel, den 27. Dezember 2004

Für die Kommission
Charlie McCREEVY
Mitglied der Kommission

ANHANG

„STANDARDVERTRAG II

Standardvertragsklauseln für die Übermittlung personenbezogener Daten aus der Gemeinschaft in Drittländer (Übermittlung zwischen für die Datenverarbeitung Verantwortlichen)

Vereinbarung über die Datenübermittlung

zwischen

_____ (Name)

_____ (Adresse und Sitzland)

nachstehend als ‚Datenexporteur' bezeichnet,

und

_____ (Name)

_____ (Adresse und Sitzland)

nachstehend als ‚Datenimporteur' bezeichnet,

beide nachstehend als ‚Partei', zusammen als ‚Parteien' bezeichnet

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) Die Begriffe ‚personenbezogene Daten', ‚besondere Kategorien personenbezogener Daten/sensible Daten', ‚verarbeiten/-Verarbeitung', ‚für die Verarbeitung Verantwortlicher', ‚Auftragsverarbeiter', ‚betroffene Person' und ‚Kontrollstelle' werden entsprechend den Begriffsbestimmungen der Richtlinie 95/46/EG vom 24. Oktober 1995 verwendet (wobei mit ‚Kontrollstelle' die Datenschutzkontrollstelle gemeint ist, die für das Sitzland des Datenexporteurs zuständig ist).

b) ‚Datenexporteur' bezeichnet den für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten übermittelt.

c) ‚Datenimporteur' bezeichnet den für die Verarbeitung Verantwortlichen, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung gemäß den Bestimmungen dieser Vertragsklauseln entgegenzunehmen, und der nicht an ein System eines Drittlandes gebunden ist, das angemessenen Schutz gewährleistet.

d) ‚Klauseln' bezeichnet diese Standardvertragsklauseln als eigenständiges Dokument, das keine Geschäftsbedingungen beinhaltet, die von den Parteien im Rahmen getrennter geschäftlicher Vereinbarungen getroffen wurden.

Die Einzelheiten der Übermittlung (sowie die abgedeckten personenbezogenen Daten) sind in Anhang B aufgeführt, der integraler Bestandteil dieser Klauseln ist.

I. **Pflichten des Datenexporteurs**

Der Datenexporteur gibt folgende Zusicherungen:

a) Die personenbezogenen Daten wurden nach den für den Datenexporteur geltenden Gesetzen gesammelt, verarbeitet und übermittelt.

b) Er hat sich im Rahmen des Zumutbaren davon überzeugt, dass der Datenimporteur seine Rechtspflichten aus diesen Klauseln zu erfüllen in der Lage ist.

c) Er stellt dem Datenimporteur auf Antrag Exemplare der einschlägigen Datenschutzgesetze oder entsprechende Fundstellennachweise seines Sitzlandes zur Verfügung, erteilt aber keine Rechtsberatung.

d) Er beantwortet Anfragen der betroffenen Personen und der Kontrollstelle bezüglich der Verarbeitung der personenbezogenen Daten durch den Datenimporteur, es sei denn, die Parteien haben vereinbart, dass der Datenimporteur die Beantwortung übernimmt; der Datenexporteur übernimmt die Beantwortung im Rahmen der Zumutbarkeit und aufgrund der ihm zugänglichen Informationen auch dann, wenn der Datenimporteur nicht antworten will oder kann. Sie erfolgt innerhalb einer angemessenen Frist.

e) Er stellt betroffenen Personen, die Drittbegünstigte im Sinne von Klausel III sind, auf Verlangen ein Exemplar der Klauseln zur Verfügung, es sei denn, die Klauseln enthalten vertrauliche Angaben; in diesem Fall hat er das Recht, diese Angaben zu entfernen. Werden Angaben entfernt, teilt der Datenexporteur den betroffenen Personen schriftlich die Gründe für die Entfernung mit und belehrt sie über ihr Recht, die Kontrollstelle auf

die Entfernung aufmerksam zu machen. Der Datenexporteur leistet indessen der Entscheidung der Kontrollstelle Folge, den betroffenen Personen Zugang zum Volltext der Klauseln zu gewähren, wenn diese sich zur Geheimhaltung der entfernten vertraulichen Informationen verpflichten. Der Datenexporteur stellt ferner auch der Kontrollstelle auf Antrag ein Exemplar der Klauseln zur Verfügung.

II. Pflichten des Datenimporteurs

Der Datenimporteur gibt folgende Zusicherungen:

a) Er verfügt über die technischen und organisatorischen Voraussetzungen zum Schutz der personenbezogenen Daten gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugriff; damit ist ein Sicherheitsniveau gewährleistet, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten gerecht wird.

b) Seine Verfahrensregeln gewährleisten, dass von ihm zum Zugriff auf die personenbezogenen Daten befugte Dritte, einschließlich des Auftragsverarbeiters, die Geheimhaltung und Sicherheit der personenbezogenen Daten beachten und wahren. Die unter der Verantwortung des Datenimporteurs tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die personenbezogenen Daten nur auf seine Anweisung verarbeiten. Diese Bestimmung gilt nicht für Personen, die von Rechts wegen zum Zugriff auf die personenbezogenen Daten befugt oder verpflichtet sind.

c) Zum Zeitpunkt des Vertragsabschlusses bestehen seines Wissens in seinem Land keine entgegenstehenden Rechtsvorschriften, die die Garantien aus diesen Klauseln in gravierender Weise beeinträchtigen; er benachrichtigt den Datenexporteur (der die Benachrichtigung erforderlichenfalls an die Kontrollstelle weiterleitet), wenn er Kenntnis von derartigen Rechtsvorschriften erlangt.

d) Er verarbeitet die personenbezogenen Daten zu den in Anhang B dargelegten Zwecken und ist ermächtigt, die Zusicherungen zu geben und die Verpflichtungen zu erfüllen, die sich aus diesem Vertrag ergeben.

e) Er nennt dem Datenexporteur eine Anlaufstelle innerhalb seiner Organisation, die befugt ist, Anfragen bezüglich der Verarbeitung der personenbezogenen Daten zu behandeln, und arbeitet redlich mit dem Datenexporteur, der betroffenen Person und der Kontrollstelle zusammen, damit derartige Anfragen innerhalb einer angemessenen Frist beantwor-

tet werden. Wenn der Datenexporteur nicht mehr besteht oder wenn die Parteien Entsprechendes vereinbaren, verpflichtet sich der Datenimporteur zur Einhaltung der Bestimmungen von Klausel I Buchstabe e).

f) Auf Antrag des Datenexporteurs weist er nach, dass er über ausreichende Finanzmittel verfügt, um die Verpflichtungen aus Klausel III zu erfüllen (wozu auch Versicherungsschutz zählen kann).

g) Auf Antrag des Datenexporteurs und sofern dies nicht willkürlich ist, überlässt er seine zur Verarbeitung benötigten Datenverarbeitungseinrichtungen, Dateien und Unterlagen der Überprüfung, dem Audit und/oder der Zertifizierung durch den Datenexporteur (oder von ihm ausgewählte unabhängige oder unparteiische Prüfer oder Auditoren, gegen die der Datenimporteur keine begründeten Einwände erhebt), um zu gewährleisten, dass die Zusicherungen in diesen Klauseln eingehalten werden, wobei die Überprüfung rechtzeitig anzukündigen und während der üblichen Geschäftszeiten durchzuführen ist. Sofern die Zustimmung oder Genehmigung durch eine Regulierungs- oder Kontrollstelle im Land des Datenimporteurs erforderlich ist, bemüht sich dieser, die Zustimmung oder Genehmigung zügig zu erhalten.

h) Er verarbeitet die personenbezogenen Daten gemäß

   i) den Datenschutzbestimmungen des Landes, in dem der Datenexporteur ansässig ist, oder

   ii) den einschlägigen Bestimmungen[1] etwaiger Kommissionsentscheidungen nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG, sofern der Datenimporteur die einschlägigen Bestimmungen derartiger Genehmigungen bzw. Entscheidungen einhält und in einem Land ansässig ist, für das diese Genehmigungen oder Entscheidungen gelten, obwohl diese hinsichtlich der Übermittlung personenbezogener Daten auf ihn keine Anwendung finden[2], oder

   iii) den Grundsätzen für die Datenverarbeitung in Anhang A.

   Der Datenimporteur wählt die Möglichkeit: _____

   Paraphe des Datenimporteurs: _____;

[1] ‚Einschlägige Bestimmungen' sind sämtliche unter diese Klauseln fallende Genehmigungen oder Entscheidungen mit Ausnahme der Vollzugsbestimmungen.

[2] Wird diese Möglichkeit gewählt, sind jedoch die Bestimmungen von Anhang A Ziffer 5 über das Recht auf Zugriff, Berichtigung, Löschung und Widerspruch anzuwenden, die dann vergleichbaren Bestimmungen der gewählten Kommissionsentscheidung vorgehen.

i) Er verzichtet auf die Offenlegung oder Übermittlung personenbezogener Daten an für die Verarbeitung Verantwortliche Dritte, die außerhalb des Europäischen Wirtschaftsraums (EWR) ansässig sind, es sei denn, er setzt den Datenexporteur von der Übermittlung in Kenntnis und

   i) der für die Verarbeitung Verantwortliche Dritte verarbeitet die personenbezogenen Daten im Einklang mit einer Kommissionsentscheidung, in der die Kommission einem Drittland ein angemessenes Datenschutzniveau zuerkennt, oder

   ii) der für die Verarbeitung Verantwortliche Dritte unterzeichnet diese Klauseln oder eine andere, von einer zuständigen Stelle in der EU genehmigte Datenübermittlungsvereinbarung oder

   iii) die betroffenen Personen haben das Recht zum Widerspruch, nachdem sie über den Zweck der Übermittlung informiert wurden, ferner über die Empfängerkategorien und darüber, dass das Empfängerland der Daten möglicherweise andere Datenschutzstandards aufweist, oder

   iv) die betroffenen Personen haben im Hinblick auf die Weiterübermittlung sensibler Daten zweifelsfrei ihre Zustimmung zu der Weiterübermittlung erteilt.

III. **Haftung und Rechte Dritter**

a) Jede Partei haftet gegenüber der anderen Partei für Schäden, die sie durch einen Verstoß gegen diese Klauseln verursacht. Die gegenseitige Haftung der Parteien ist auf den tatsächlich erlittenen Schaden begrenzt. Strafschadenersatzansprüche (d. h. die Zahlung von Strafen für grobes Fehlverhalten einer Partei) sind ausdrücklich ausgeschlossen. Jede Partei haftet gegenüber der betroffenen Person für Schäden, die sie durch die Verletzung von Rechten Dritter im Rahmen dieser Klauseln verursacht. Die Haftung des Datenexporteurs gemäß den für ihn maßgeblichen Datenschutzvorschriften bleibt davon unberührt.

b) Die Parteien räumen den betroffenen Personen das Recht ein, diese Klausel sowie Klausel I Buchstaben b), d) und e), Klausel II Buchstaben a), c), d), e), h), i), Klausel III Buchstabe a) sowie die Klauseln V, VI Buchstabe d) und VII als Drittbegünstigte gegenüber dem Datenimporteur oder dem Datenexporteur durchzusetzen, wenn diese im Hinblick auf die Daten der betroffenen Personen ihre Vertragspflichten verletzen; zu diesem Zweck erkennen sie die Zuständigkeit der Gerichte im Sitzland des Datenexporteurs an. Wirft die betroffene Person dem

Datenimporteur Vertragsverletzung vor, muss sie den Datenexporteur zunächst auffordern, ihre Rechte gegenüber dem Datenimporteur durchzusetzen; wird der Datenexporteur nicht innerhalb einer angemessenen Frist tätig (im Regelfall innerhalb eines Monats), kann die betroffene Person ihre Rechte direkt gegenüber dem Datenimporteur durchsetzen. Eine betroffene Person kann direkt gegen einen Datenexporteur vorgehen, wenn dieser sich im Rahmen des Zumutbaren nicht davon überzeugt hat, dass der Datenimporteur seine rechtlichen Verpflichtungen aus diesen Klauseln zu erfüllen in der Lage ist (der Datenexporteur muss beweisen, dass er alle zumutbaren Anstrengungen unternommen hat).

IV. Anwendbares Recht

Diese Klauseln unterliegen dem Recht des Landes, in dem der Datenexporteur ansässig ist; davon ausgenommen sind die Rechtsvorschriften über die Verarbeitung der personenbezogenen Daten durch den Datenimporteur gemäß Klausel II Buchstabe h), die nur gelten, wenn sich der Datenimporteur nach dieser Klausel dafür entschieden hat.

V. Beilegung von Streitigkeiten mit betroffenen Personen oder der Kontrollstelle

a) Bei einer Streitigkeit oder einer Klage der betroffenen Person oder der Kontrollstelle gegen eine Partei oder beide Parteien bezüglich der Verarbeitung personenbezogener Daten setzen die Parteien einander davon in Kenntnis und bemühen sich gemeinsam um eine zügige, gütliche Beilegung.

b) Die Parteien erklären sich bereit, sich jedem allgemein zugänglichen, nicht bindenden Schlichtungsverfahren zu unterwerfen, das von einer betroffenen Person oder der Kontrollstelle angestrengt wird. Beteiligen sie sich an dem Verfahren, können sie dies auf dem Weg der Telekommunikation tun (z. B. per Telefon oder anderer elektronischer Mittel). Die Parteien erklären sich ferner bereit, eine Beteiligung an anderen Vermittlungsverfahren, Schiedsverfahren oder sonstigen Verfahren der Streitbeilegung zu erwägen, die für die Zwecke des Datenschutzes entwickelt werden.

c) Die Parteien unterwerfen sich den rechtskräftigen Endentscheidungen des zuständigen Gerichts im Sitzland des Datenexporteurs oder der Kontrollstelle.

VI. **Beendigung des Vertrags**

a) Verstößt der Datenimporteur gegen seine Verpflichtungen aus diesen Klauseln, kann der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur vorläufig aussetzen, bis der Verstoß beseitigt oder der Vertrag beendet ist.

b) Tritt einer der folgenden Fälle ein:

i) Die Übermittlung personenbezogener Daten an den Datenimporteur wird vom Datenexporteur gemäß Buchstabe a) länger als einen Monat ausgesetzt;

ii) die Einhaltung dieser Klauseln durch den Datenimporteur verstößt gegen Rechtsvorschriften des Importlandes;

iii) der Datenimporteur missachtet Zusicherungen, die er im Rahmen dieser Klauseln gegeben hat, in erheblichem Umfang oder fortdauernd;

iv) das zuständige Gericht im Sitzland des Datenexporteurs oder der Kontrollstelle stellt rechtskräftig fest, dass der Datenimporteur oder der Datenexporteur gegen die Klauseln verstoßen haben, oder

v) es wird ein Antrag auf Insolvenzverwaltung oder Abwicklung des Datenimporteurs in dessen privater oder geschäftlicher Eigenschaft gestellt, der nicht innerhalb der nach geltendem Recht vorgesehenen Frist abgewiesen wird; die Abwicklung wird gerichtlich angeordnet; für einen beliebigen Teil seines Vermögens wird ein Zwangsverwalter bestellt; ein Treuhänder wird bestellt, falls es sich bei dem Datenimporteur um eine Privatperson handelt; dieser leitet einen außergerichtlichen Vergleich ein, oder es kommt zu einem je nach Rechtsordnung gleichwertigen Verfahren,

so ist der Datenexporteur berechtigt, unbeschadet etwaiger sonstiger Ansprüche gegen den Datenimporteur, diesen Vertrag zu kündigen, wovon er gegebenenfalls die Kontrollstelle in Kenntnis setzt. Tritt einer der in Ziffer i), ii) oder iv) genannten Fälle ein, kann der Datenimporteur seinerseits den Vertrag kündigen.

c) Jede Partei kann den Vertrag kündigen, wenn i) die Kommission eine positive Angemessenheitsfeststellung gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG (oder einer Vorschrift, die diese Vorschrift ersetzt) in Bezug auf das Land (oder einen Bereich davon) trifft, in das die Daten

übermittelt und in dem sie vom Datenimporteur verarbeitet werden, oder ii) die Richtlinie 95/46/EG (oder eine Vorschrift, die diese Vorschrift ersetzt) in dem betreffenden Landes unmittelbar zur Anwendung gelangt.

d) Die Parteien vereinbaren, dass sie auch nach der Beendigung dieses Vertrags, ungeachtet des Zeitpunkts, der Umstände oder der Gründe (ausgenommen die Kündigung gemäß Klausel VI Buchstabe c), weiterhin an die Verpflichtungen und/oder Bestimmungen dieser Klauseln in Bezug auf die Verarbeitung der übermittelten Daten gebunden sind.

VII. **Änderung der Klauseln**

Die Parteien dürfen diese Klauseln nur zum Zwecke der Aktualisierung von Anhang B ändern; gegebenenfalls müssen sie die Kontrollstelle davon in Kenntnis setzen. Es steht den Parteien allerdings frei, erforderlichenfalls weitere Geschäftsklauseln hinzuzufügen.

VIII. **Beschreibung der Übermittlung**

Die Einzelheiten zur Übermittlung und zu den personenbezogenen Daten sind in Anhang B aufgeführt. Die Parteien vereinbaren, dass sie gegebenenfalls in Anhang B enthaltene vertrauliche Informationen nicht gegenüber Dritten offen legen, es sei denn, sie sind gesetzlich dazu verpflichtet oder handeln auf Aufforderung einer zuständigen Regulierungsstelle oder staatlichen Einrichtung oder gemäß Klausel I Buchstabe e). Die Parteien können weitere Anhänge vereinbaren, die zusätzliche Übermittlungen betreffen; diese sind gegebenenfalls der Kontrollstelle zu unterbreiten. Ersatzweise kann Anhang B so formuliert werden, dass er eine Vielzahl von Übermittlungen abdeckt.

Datum: _____ _____

_____ _____

Für den DATENIMPORTEUR Für den DATENEXPORTEUR

....

....

....

ANHANG A

GRUNDSÄTZE FÜR DIE DATENVERARBEITUNG

1. Zweckbindung: Personenbezogene Daten dürfen nur für die in Anhang B festgelegten oder anschließend von der betroffenen Person genehmigten Zwecke verarbeitet und danach verwendet oder weiter übermittelt werden.

2. Datenqualität und Verhältnismäßigkeit: Personenbezogene Daten müssen sachlich richtig sein und nötigenfalls auf dem neuesten Stand gehalten werden. Sie müssen den Übermittlungs- und Verarbeitungszwecken angemessen und dafür erheblich sein und dürfen nicht über das erforderliche Maß hinausgehen.

3. Transparenz: Die betroffenen Personen müssen Informationen erhalten, die eine Verarbeitung nach Treu und Glauben gewährleisten (beispielsweise Angaben zum Verarbeitungszweck und zur Übermittlung), sofern diese Informationen nicht bereits vom Datenexporteur erteilt wurden.

4. Sicherheit und Geheimhaltung: Der für die Verarbeitung Verantwortliche muss geeignete technische und organisatorische Sicherheitsvorkehrungen gegen die Risiken der Verarbeitung treffen, beispielsweise gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugriff. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. Recht auf Auskunft, Berichtigung, Löschung und Widerspruch: Nach Artikel 12 der Richtlinie 95/46/EG hat die betroffene Person das Recht, entweder direkt oder durch Dritte, Auskunft über alle ihre personenbezogenen Daten zu erhalten, die von einer Organisation vorgehalten werden; dies gilt nicht für Auskunftsersuchen, die aufgrund ihrer unzumutbaren Periodizität oder ihrer Zahl, Wiederholung oder Systematik offensichtlich übertrieben sind, oder für Daten, über die nach dem für den Datenexporteur geltenden Recht keine Auskunft erteilt werden muss. Vorbehaltlich der vorherigen Genehmigung durch die Kontrollstelle muss auch dann keine Auskunft erteilt werden, wenn die Interessen des Datenimporteurs oder anderer Organisationen, die mit dem Datenimporteur in Geschäftsverkehr stehen, dadurch ernsthaft geschädigt würden und die Grundrechte und Grundfreiheiten der betroffenen Personen hierdurch nicht beeinträchtigt werden. Die Quellen der personenbezogenen Daten müssen nicht angegeben werden, wenn dazu unzumutbare Anstrengungen erforderlich wären oder die Rechte Dritter dadurch verletzt würden. Die betroffene Person muss das Recht haben, ihre personenbezogenen Daten

berichtigen, ändern oder löschen zu lassen, wenn diese unzutreffend sind oder entgegen den vorliegenden Grundsätzen verarbeitet wurden. Bei begründeten Zweifeln an der Rechtmäßigkeit des Ersuchens kann die Organisation weitere Belege verlangen, bevor die Berichtigung, Änderung oder Löschung erfolgt. Dritte, gegenüber denen die Daten offen gelegt wurden, müssen von der Berichtigung, Änderung oder Löschung nicht in Kenntnis gesetzt werden, wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Die betroffene Person muss auch aus zwingenden legitimen Gründen, die mit ihrer persönlichen Situation zusammenhängen, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einlegen können. Die Beweislast liegt im Fall einer Ablehnung beim Datenimporteur; die betroffene Person kann eine Ablehnung jederzeit vor der Kontrollstelle anfechten.

6. Sensible Daten: Der Datenimporteur trifft die zusätzliche Vorkehrungen (beispielsweise sicherheitsbezogener Art), die entsprechend seinen Verpflichtungen nach Klausel II zum Schutz sensibler Daten erforderlich sind.

7. Direktmarketing: Werden Daten zum Zwecke des Direktmarketings verarbeitet, sind wirksame Verfahren vorzusehen, damit die betroffene Person sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke entscheiden kann (‚Opt-out').

8. Automatisierte Entscheidungen: ‚Automatisierte Entscheidungen' im Sinne dieser Klauseln sind mit Rechtsfolgen behaftete Entscheidungen des Datenexporteurs oder des Datenimporteurs bezüglich einer betroffenen Person, die allein auf der automatisierten Verarbeitung personenbezogener Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person beruhen, beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens. Der Datenimporteur darf keine automatisierten Entscheidungen über eine betroffene Person fällen, es sei denn:

   a) i) Der Datenimporteur fällt die Entscheidungen im Rahmen eines Vertragsabschlusses oder der Ausführung eines Vertrags mit der betroffenen Person, und

      ii) die betroffene Person erhält die Möglichkeit, die Ergebnisse einer einschlägigen automatisierten Entscheidung mit einem Vertreter der entscheidungtreffenden Partei zu erörtern, oder aber Erklärungen gegenüber dieser Partei abzugeben,

      oder

   b) die für den Datenexporteur geltenden Rechtsvorschriften sehen etwas anderes vor.

ANHANG B

BESCHREIBUNG DER ÜBERMITTLUNG

(von den Parteien auszufüllen)

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

.....
.....
.....
.....

Übermittlungszwecke

Die Übermittlung ist zu folgenden Zwecken erforderlich:

.....
.....
.....
.....

Kategorien übermittelter Daten

Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

.....
.....
.....
.....

Empfänger

Die übermittelten personenbezogenen Daten dürfen nur gegenüber folgenden Empfängern oder Kategorien von Empfängern offen gelegt werden:

.....
.....
.....

Sensible Daten (falls zutreffend)

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien sensibler Daten:

.....
.....
.....
.....

Datenschutzmelderegister-Angaben des Datenexporteurs (falls zutreffend)
.....
.....

Sonstige nützliche Informationen (Aufbewahrungszeitraum und sonstige einschlägige Angaben)
.....
.....

Anlaufstelle für Datenschutzauskünfte

Datenimporteur	**Datenexporteur**
.....	.....
.....	.....
.....	.....

VERANSCHAULICHENDE GESCHÄFTSKLAUSELN (FAKULTATIV)

Wechselseitige Entschädigung von Datenexporteur und Datenimporteur:

‚Die Parteien entschädigen sich wechselseitig oder halten sich wechselseitig schadlos für alle Kosten, Ausgaben, Schäden, Auslagen oder Verluste, die die andere Partei durch Verletzung einer dieser Vertragsklauseln verursacht. Der Entschädigungsanspruch setzt voraus, dass a) die zu entschädigenden Parteien die entschädigenden Parteien unverzüglich von dem Bestehen einer Forderung in Kenntnis setzen und b) die entschädigenden Parteien allein dazu berechtigt sind, sich gegen einen solchen Anspruch zu verteidigen oder den Streit beizulegen und (c) die zu entschädigenden Parteien bei der Abwehr derartiger Rechtsansprüche redlich mit den entschädigenden Parteien zusammenarbeiten und diese unterstützen.‘

Streitbeilegung zwischen Datenexporteur und Datenimporteur (die Parteien können selbstverständlich eine andere alternative Streitbeilegung oder die Zuständigkeit eines Gerichts vereinbaren):

‚Alle Rechtsstreitigkeiten zwischen dem Datenimporteur und dem Datenexporteur aus dem vorliegenden Vertrag werden gemäß dem Schlichtungs- und Schiedsreglement der Internationalen Handelskammer endgültig durch einen oder mehrere Schiedsrichter entschieden, die in Übereinstimmung mit diesem Reglement ernannt werden. Ort des Schiedsverfahrens ist […]. Die Zahl der Schiedsrichter beträgt […].‘

Kostenteilung:

‚Jede Partei trägt die Kosten für die Erfüllung ihrer Vertragspflichten.‘

Zusätzliche Beendigungsklausel:

‚Bei Beendigung dieses Vertrags gibt der Datenimporteur alle personenbezogenen Daten sowie alle Kopien der personenbezogenen Daten, die Gegenstand dieser Klauseln sind, unverzüglich an den Datenexporteur zurück, oder aber der Datenimporteur vernichtet auf Antrag des Datenexporteurs alle Exemplare derselben und bescheinigt dem Datenexporteur die Vernichtung, es sei denn, der nationale Gesetzgeber oder die nationale Regulierungsbehörde verbietet die vollständige oder teilweise Rückübermittlung oder Zerstörung dieser Daten; in diesem Fall werden die Daten geheim gehalten und zu keinem weiteren Zweck aktiv verarbeitet. Auf Verlangen des Datenexporteurs erlaubt der Datenimporteur dem Datenexporteur oder einem vom Datenexporteur ausgewählten Prüfer, gegen den der Datenimporteur keine begründeten Einwände erhebt, den Zugang zu seinen Räumlichkeiten, damit die Ausführung dieser Bestimmungen überprüft werden kann; die Überprüfung ist rechtzeitig anzukündigen und während der üblichen Geschäftszeiten durchzuführen.‘ “.

IV. Internationale Konferenz der Datenschutzbeauftragten vom 14.–16. September 2004 in Breslau (Polen)

Resolutionen zum Entwurf eines ISO-Rahmenstandards zum Datenschutz

– Übersetzung –

Auf Vorschlag des Berliner Beauftragten für Datenschutz und Informationsfreiheit, des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, der Belgischen Datenschutzkommission, des Britischen Informationsbeauftragten, des Deutschen Bundesbeauftragten für den Datenschutz, des Unabhängigen Zentrums für Datenschutz Schleswig-Holstein, der Informations- und Datenschutzbeauftragten von Ontario, der Polnischen Generalinspekteurin für den Datenschutz, des Datenschutzbeauftragten von Hong Kong, der Spanischen Datenschutzbehörde, der staatlichen Datenschutzbehörde der Republik Litauen und des Eidgenössischen Datenschutzbeauftragten hat die Internationale Datenschutzkonferenz Folgendes beschlossen:

- Die Internationale Standardisierungsorganisation (ISO) hat eine Arbeitsgruppe zu Datenschutztechnologien im Rahmen des Gemeinsamen Technischen Ausschusses (JTC 1) eingerichtet, um die Notwendigkeit der Entwicklung eines Standards für Datenschutztechnologien und gegebenenfalls das Verfahren zur Formulierung und den Geltungsbereich eines solchen Standards zu prüfen und bis zum November 2004 zu berichten;

- Der Gemeinsame Technische Ausschuss (JTC 1) der ISO leitet dem Unterausschuss 27 (Sicherheit der Informationstechnik) Vorschläge für einen Datenschutz-Rahmenstandard zur Entscheidung in einem beschleunigten Verfahren zu;

- Die Internationale Allianz für Sicherheit, Vertrauen und Datenschutz (International Security, Trust and Privacy Alliance – ISTPA –) ist eine weltweite Vereinigung von Unternehmen, Institutionen und Technologie-Anbietern, die zusammenarbeiten, um gegenwärtige und entstehende Probleme in Bezug auf Sicherheit, Vertrauen und Datenschutz zu klären und zu lösen;

- Die ISO hat den Entwurf eines Internationalen Standards (ISO/IEC (PAS) DIS 20886) für einen Datenschutzrahmen erhalten, den ISTPA[1] in einem beschleu-

[1] vgl. http://www.istpa.org

nigten Verfahren eingebracht hat und über den durch schriftliche Abstimmung bis zum 11. Dezember 2004 abgestimmt werden soll;

- Das Projekt zum Test und zur Bewertung von Datenschutz fördernden Technologien (Privacy Enhancing Technology Testing & Evaluation Project – PETTEP –)[2] ist eine weltweite Gruppe von Datenschutzbeauftragten, Wissenschaftlern, öffentlichen und nicht-öffentlichen Stellen und Datenschutzexperten, denen es um die Entwicklung international anerkannter Test- und Evaluationskriterien für die Datenschutzkonformität von Informationstechnologien und -systemen geht;

- Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat bei ihrer 35. Sitzung in Buenos Aires am 14./15. April 2004 ein Arbeitspapier zu einem zukünftigen ISO-Datenschutzstandard angenommen[3];

- Die Internationale Konferenz der Datenschutzbeauftragten (im Folgenden die „Konferenz") möchte die Entwicklung eines effektiven und universell akzeptierten Internationalen Standards über Datenschutztechnologien unterstützen und der ISO ihren Sachverstand für die Entwicklung eines solchen Standards zur Verfügung stellen;

- Die Konferenz erkennt an, dass die Befolgung jedes gegenwärtigen oder zukünftigen ISO-Standards nicht notwendigerweise die Befolgung von rechtlichen Bestimmungen impliziert oder ersetzt. Die Konferenz sieht aber in der Entwicklung solcher Standards der Informationstechnologie ein Mittel, um die Beteiligten bei der Befolgung rechtlicher Regelungen zum Datenschutz zu unterstützen. Die Konferenz erkennt an, dass trotz der Tatsache, dass jedes Mitgliedsland gegenwärtig und in Zukunft eigene, in bestimmter Hinsicht von anderen verschiedene Datenschutzgesetze hat, insgesamt ein hohes Maß an Übereinstimmung zwischen diesen rechtlichen Anforderungen besteht, denen am Besten zu entsprechen wäre, wenn sie durch die Entwicklung eines Internationalen Standards zur datenschutzrechtlichen Informationstechnik unterstützt würden.

Die Konferenz nimmt die folgenden Resolutionen an:

1. **Die Konferenz empfiehlt, dass ein weltweiter Datenschutzstandard und insbesondere ein Standard für Datenschutztechnologien von der ISO formuliert wird, der die Umsetzung bestehender rechtlicher Bestimmungen zum Datenschutz und die Formulierung solcher Bestimmungen – wo sie noch fehlen – unterstützt.**

[2] PETTEP ist ein Projekt, das von der Informations- und Datenschutzbeauftragten von Ontario geleitet wird und das Test- und Bewertungskriterien für datenschutzfreundliche Informationstechnik untersucht.

[3] http://datenschutz-berlin.de/doc/int/iwgdpt/index.htm

2. **Die Konferenz ist der Auffassung, dass die Entwicklung eines Internationalen Datenschutzstandards sowohl auf gerechte Informationspraktiken als auch auf die Begriffe der Datensparsamkeit, Datenminimierung und Anonymität gestützt sein muss. Um effektiv zu sein, muss ein Standard für Informationstechnologie:**

   - **Evaluations- und Testkriterien bereitstellen, die es erlauben, die Datenschutzfunktionalität jedes Systems oder jeder Technologie zu bewerten, um auf diese Weise die Daten verarbeitenden Stellen bei der Befolgung nationaler und internationaler Vorschriften zum Datenschutz zu unterstützen;**

   - **einen Grad an Vertrauenswürdigkeit hinsichtlich der Technologien und Systeme zur Verarbeitung personenbezogener Daten gewährleisten, die den Anspruch erheben, datenschutzgerecht zu sein;**

   - **in der Lage sein, Datenschutzerfordernisse bezüglich personenbezogener Daten zu erfüllen, unabhängig von der Kombination und Zahl von Organisationen, die an der Verwendung und am Austausch dieser personenbezogener Daten beteiligt sein mögen.**

3. **Die Konferenz unterstützt die jüngst erfolgte Einrichtung einer vorläufigen Arbeitsgruppe zum Datenschutz (Privacy Study Group – PSG), um die Notwendigkeit eines Standards wie auch seinen Geltungsbereich und die Methode für die Entwicklung eines solchen Standards innerhalb der Internationalen Standardisierungsorganisation zu untersuchen.**

4. **Die Konferenz unterstützt nachhaltig die Beschleunigung und unverzügliche Einrichtung eines neuen, ständigen Unterausschusses der ISO für die Entwicklung von Standards zu Informationstechnologien mit Bezug zum Datenschutz. Der neue Unterausschuss sollte die Arbeit zu speziellen Datenschutzproblemen berücksichtigen, die gegenwärtig in mehreren bestehenden Unterausschüssen geleistet wird.**

5. **Die Konferenz unterstützt entschieden die Aufnahme des Projektes zum Test und zur Bewertung von datenschutzfördernden Technologien (PETTEP) als eine offizielle Verbindungsorganisation zur ISO JTC 1 Datenschutzarbeitsgruppe (PSG). Dies gibt den Datenschutzbeauftragten die Möglichkeit, direkt innerhalb der ISO-Arbeitsgruppe zu arbeiten, zudem eröffnet es den Mitgliedern von PETTEP die offizielle Möglichkeit, der Datenschutzarbeitsgruppe Vorschläge zu machen und zu ihrer Arbeit und ihren Diskussionen beizutragen.**

6. **Die Konferenz unterstützt und ermutigt interessierte Datenschutzbeauftragte, PETTEP beizutreten, was sie in die Lage versetzen würde, als**

PETTEP-Mitglieder eine unmittelbare Stimme bei den Diskussionen zur Entwicklung eines ISO-Datenschutztechnologie-Standards zu haben.

7. Die Konferenz erkennt an, dass PETTEP bereits in die PSG aufgenommen worden ist und bittet PETTEP darum, die Entschließungen der Konferenz aufzugreifen und sie der Datenschutzarbeitsgruppe zum frühestmöglichen Zeitpunkt vorzulegen.

8. Auch wenn die Konferenz die Zielrichtungen und das Engagement der ISTPA im Bereich des Datenschutzes anerkennt, bittet sie darum, den ISTPA-Rahmenentwurf als eine öffentlich erhältliche Spezifikation zurückzuziehen, bis die folgenden Punkte aufgegriffen worden sind:

- **Der Begriff des Datenschutzes, auf den der Entwurf eines Datenschutzrahmenstandards sich stützt, und die Anerkennung der Grenzen der Datenerhebung. Der Entwurf definiert „Datenschutz" als „den korrekten Umgang und die Nutzung personenbezogener Information während ihrer Lebensdauer, in Übereinstimmung mit den Datenschutzprinzipien und den Festlegungen des Betroffenen". Die Verfasser des Entwurfs meinen, dass die Erhebung und Verarbeitung personenbezogener Daten wesentlich für das reibungslose Funktionieren einer modernen Gesellschaft und des Handels ist. Diese Aussage beruht auf der Annahme, dass es keine Grenzen für die Erhebung von personenbezogenen Daten gibt. Es kann Situationen geben, in denen die Erhebung und Verarbeitung personenbezogener Daten in diesem Sinne wesentlich ist. Dies sollte aber nicht als Regel zu Grunde gelegt werden.**

9. Die Konferenz bittet die ISO, alle gegenwärtig vorliegenden Anträge für die Behandlung von öffentlich zugänglichen Spezifikationen im Bereich des Datenschutzes zur Annahme in einem Schnellverfahren (oder die Einführung neuer Anträge mit öffentlich zugänglichen Spezifikationen bezüglich des Datenschutzes) zurückzustellen, da die Entwicklung eines Datenschutzstandards gründlicher Erörterung bedarf.

10. Die Konferenz bittet darum, dass die ISO Anträge für öffentlich zugängliche Spezifikationen und andere Anträge mit Bezug auf den Datenschutz als Beiträge und Bausteine für die Entwicklung eines Gesamtrahmens und die mögliche Entwicklung zukünftiger Standards innerhalb dieses Rahmens betrachtet.

[4] ebenda S. 13

[5] ebenda S. 10

V. Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 35. Sitzung am 14./15. April 2004 in Buenos Aires

Arbeitspapier zu Datenschutz bei der Verarbeitung von Bildern und Tönen in Multimedia Messaging Services

– Übersetzung –

Mobiltelefone und Fotohandys der neuen Generation werden schnell zu etwas Alltäglichem, was teilweise auch auf die ständig verbesserte Bildqualität zurückzuführen ist.

Obgleich die diesen Geräten zugrundeliegende Technologie sich nicht wesentlich von derjenigen unterscheidet, die etwa in Standardkameras implementiert ist und daher die relevanten rechtlichen Probleme im Prinzip die selben sind, bedingt es besonders die Portabilität und der diskrete Charakter von Kamerahandys, auch in Verbindung mit der Möglichkeit zur Aufnahme von Tönen, dass sie eingesetzt werden können, ohne dass der Fotografierte selbst dies bemerkt.

Dieser Umstand bringt erhöhte Risiken nicht nur für die Privatsphäre des Einzelnen mit sich, sondern kann auch zur Verletzung von Betriebs- und Geschäftsgeheimnissen führen. Tatsächlich wurden bereits Nutzungsverbote für Kamerahandys bestimmte Geschäftsräume betreffend und/oder innerhalb von Fabriken und Arbeitsstätten ausgesprochen.[1]

Es muss betont werden, dass diese Art der Verarbeitung unter den Anwendungsbereich von Strafvorschriften (z. B. Verbreitung jugendgefährdender Schriften) und zivilrechtlichen Regelungen (z. B. Schutz des Rechtes am eigenen Bild, Urheberrechte) fallen kann.

Bild- und Tondateien können personenbezogene Daten, einschließlich sensitiver Daten, enthalten, soweit sie sich auf bestimmte oder bestimmbare natürliche Personen beziehen. In diesem Fall muss berücksichtigt werden, welche Datenschutzprinzipien, insbesondere das Erfordernis nach Information und Einwilligung, Anwendung finden; es sei denn die Datenverarbeitung wird ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen.[2]

---

[1] Siehe hierzu ITU, „Social and Human Considerations for a More Mobile World – Background Paper“, Februar 2004, verfügbar unter http://www.itu.int/osg/spu/ni/futuremobile/SocialconsiderationsBP.pdf , S. 17.

[2] Siehe die Entschließungen einiger europäischer Datenschutzbehörden (Italien, 12. März 2003; Ungang, Dezember 2003). Siehe auch das Informationspapier 05.03, Mobile phones with cameras, veröffentlicht vom Office of the Victorian Privacy Commissioner, Australia, verfügbar unter http://www.privacy.vic.gov.au.

Im Hinblick sowohl auf die oben stehenden Erwägungen als auch auf die besonderen Schwierigkeiten bei der Durchsetzung in diesem Gebiet bedingt durch die oben angesprochenen Grundeigenschaften der involvierten Technik (Schnelligkeit, Digitalisierung, leichte Benutzung) möchte die Arbeitsgruppe die Aufmerksamkeit aller betroffenen Unternehmen auf die Notwendigkeit eines erhöhten öffentlichen Bewusstseins für die Datenschutzrisiken lenken, die der Gebrauch von Fotohandys mit sich bringt.

Um diese Ziel zu erreichen, empfiehlt die Arbeitsgruppe eine Reihe von Handlungsoptionen:

– Verbesserung der Aufklärung der Nutzer, wobei besonders ihrem Alter und ihrer Unerfahrenheit Rechnung getragen werden sollte;

– Verbesserung der Informationen durch die Hersteller über den angemessenen Umgang mit Fotohandys;

– Implementierung von technischen Vorkehrungen zur Vereinfachung der Anwendung der relevanten Datenschutzprinzipien und zur Steigerung des Bewusstseins. Mögliche Mittel zur Erreichung dieses Ziels könnten ein Tonsignal[3] sein, das ausgelöst wird, wenn die Fotografierfunktion in Betrieb ist, sowie die Entwicklung von Technologien, die es erlauben, die Fotografierfunktion in gekennzeichneten Bereichen („sicherer Hafen“, z. B. Fitnesscenter) abzuschalten.[4]

[3] Dies ist in Japan auf der Basis einer Selbstregulierung der Industrie bereits umgesetzt während in Südkorea im November 2003 ein Gesetzesvorhaben verabschiedet wurde, das ein aktiviertes Tonsignal mit einer Stärke von mindestens 65 decibel für Fotohandys, unabhängig von deren Einstellungen, fordert.

[4] Siehe ITU, a.a.O, S. 18.

Arbeitspapier zu einem zukünftigen ISO Datenschutzstandard

– Übersetzung –

Die Arbeitsgruppe begrüßt die Initiativen zur Annahme eines Rahmenstandards zum Datenschutz und zur Einrichtung einer Arbeitsgruppe für Datenschutztechnologie, die gegenwärtig bei der Internationalen Standardisierungsorganisation (ISO) beraten werden. Ein globaler Datenschutzstandard könnte dazu beitragen, die Datenschutzgarantien insbesondere in den Ländern zu schaffen oder zu verbessern, die bisher keinerlei angemessene Datenschutzgesetzgebung aufweisen. Die Standardisierung von Datenschutztechnologie könnte eine wichtige Rolle spielen, wenn es darum geht, Datenverarbeiter bei der Umsetzung nationaler und internationaler rechtlicher Vorschriften zum Datenschutz zu unterstützen.

Technische Standards zu Datenschutz und Technologie bedürfen der eingehenden Diskussion. Die schnelle Annahme eines globalen Standards liegt möglicherweise nicht im langfristigen Interesse der internationalen Gemeinschaft.

Deshalb fordert die Arbeitsgruppe die nationalen Datenschutzbehörden auf, Empfehlungen an die nationalen Standardisierungsgremien zu richten, um technische Normen zu verabschieden, die mit dem rechtlichen Rahmen zum Datenschutz übereinstimmen.

Um größtmögliche Transparenz und Sicherheit für die Datenverarbeiter (Unternehmen und Behörden) zu gewährleisten, die einen zukünftigen Standard umsetzen wollen, betont die Arbeitsgruppe, dass die Befolgung eines technischen Standards nicht notwendigerweise die Befolgung von Rechtsnormen impliziert oder ersetzt.

Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke

Allgemeine Empfehlungen

– Übersetzung –

Drahtlose Kommunikation bietet zahlreiche Vorteile wie Portabilität und Flexibilität, erhöhte Produktivität und niedrigere Installationskosten und wird zunehmend populärer. Drahtlose Technologie deckt eine breite Auswahl an unterschiedlichen Fähigkeiten ab, ausgerichtet auf verschiedene Anwendungen und Bedürfnisse. Vorrichtungen drahtloser lokaler Netzwerke (Wireless local area network – WLAN) erlauben den Nutzern zum Beispiel, ihre Laptops von einer Stelle zur anderen innerhalb ihres Büros oder zu Hause zu bewegen, ohne dass dafür Kabel notwendig wären und ohne dass die Netzwerkverbindung verloren geht.

Ad hoc Netzwerke, wie solche, die durch Bluetooth ermöglicht werden, erlauben den Datenabgleich mit Netzwerksystemen, die Anwendungsteilung zwischen verschiedenen Geräten und beseitigen die Notwendigkeit von Druckerkabeln und sonstigen Verbindungen zu Zusatzgeräten. Mobile Endgeräte wie Personal Digital Assistants (PDA) und Mobiltelefone erlauben Außendienstmitarbeitern den Abgleich von persönlichen Datenbanken und liefern den Zugang zu betrieblich bereitgestellten Diensten wie E-Mail und Internet. Drahtlose Technologie stellt für die Zukunft eine größere Funktionalität in Aussicht.

Dennoch gibt es Risiken bei der Nutzung von drahtloser Technologie, insbesondere weil das der Technik zugrundeliegende Kommunikationsmedium, die Funkverbindung, offen ist für Angriffe, wenn nicht angemessene Sicherheitsvorkehrungen getroffen werden.

Die Risiken umfassen:

– Das Abfangen von Standortdaten und anderen persönlichen Daten über den Netzwerknutzer;
– Unautorisierter und unbemerkter Zugang zu betrieblichen Netzwerken durch externe Nutzer;
– Umgehung von betrieblichen Firewalls und E-Mail-Filterung durch Nutzer drahtloser Netze, die auch Zugang zu Unternehmens- oder Behördennetzen haben, was zu einem Verlust des Schutzes vor Virusattacken und Spam führt;
– Abhören persönlicher Kommunikation und unentdeckte Verbindungen zwischen Nutzern drahtloser Netze, insbesondere auf öffentlichen Plätzen.

Die Arbeitsgruppe fordert sowohl die IEEE Task Group[1] und die WI-FI Alliance[2] als auch die Verkäufer von Produkten der drahtlosen Technologie auf, der Datensicherheit und dem Datenschutz einen hohen Stellenwert bei der gegenwärtigen und zukünftigen Entwicklung von drahtlosen Technologien einzuräumen[3].

Empfehlungen

A) Risikoanalyse und gewünschtes Sicherheitsniveau

Betreiber drahtloser Netzwerke[4] sollten sich der technischen und der sicherheitstechnischen Auswirkungen von drahtlosen und mobilen Technologien bewusst sein.

Betreiber drahtloser Netzwerke sollten eine Risikoeinschätzung durchführen und eine Sicherheitspolitik entwickeln bevor sie drahtlose Technik einsetzen, um sicherzustellen, dass sie die Risiken für ihre Informationen, Systemoperationen und die Kontinuität der Operationen überprüft haben, und diese handhaben und entschärfen können.

Nutzern drahtloser Netzwerke sollten die technischen und sicherheitstechnischen Auswirkungen drahtloser und mobiler Technologien bewusst gemacht werden.

In ihrem eigenen Interesse sollten alle Nutzer eine persönliche Risikoeinschätzung durchführen, bevor sie drahtlose Technologie oder Dienste kaufen, benutzen oder betreiben, weil ihre eigenen persönlichen Sicherheitsanforderungen bestimmen welche Produkte oder Dienste in Betracht kommen.

B) Netzwerkparametereinstellungen

Betreiber drahtloser Netzwerke sollten den Einsatz drahtloser Technologie sorgfältig planen und geeignete Parameter an den Geräten setzen, um sowohl die

---

[1] IEEE 802.11 Working Group for Wireless Area Networks (WLANs). http://grouper.ieee.org/groups/802/11/. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters IEEE.

[2] Wi-Fi Wireless Fidelity http://www.wi-fi.org/OpenSection/index.asp The Wi-Fi Alliance organization, a nonprofit industry group, promotes the acceptance of 802.11 wireless technology worldwide, and ensures that all Wi-Fi CERTIFIED 802.11-based wireless networking gear works with all other Wi-Fi CERTIFIED equipment of the same frequency band and features.

[3] NIST Publication 800-48: Wireless Network Security 802.11, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf. NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs.

[4] Englisch: „network manager" = anyone who wants to deploy and use wireless networks.

Netzwerkfunktion als auch die Sicherheit der Dienste zu garantieren. Insbesondere sollte der Netzwerkzugang durch hohe Sicherheitsstandards zusätzlich geschützt werden.

Nutzer sollten angeleitet werden und es sollte ihnen bewusst gemacht werden, wie sie ihr drahtloses Gerät konfigurieren müssen, um ein hohes Sicherheitsniveau und Vertraulichkeit herzustellen.

C) Sicherheitsmanagement

Betreiber drahtloser Netzwerke sollten Sicherheitsmaßnahmen einführen und kontrollieren, um die Sicherheit der drahtlosen Netzwerke zu erhalten.

Betreiber drahtloser Netzwerke müssen regelmäßig die inhärenten Sicherheitsmerkmale, wie z.B. die Authentifizierung und Verschlüsselung, die in drahtlosen Netzwerken existieren überprüfen. Die Authentifizierung ist in drahtlosen Netzwerken besonders wichtig und könnte auf einer strengeren Zugriffskontrolle mit regelmäßigem Wechsel der Passwörter basieren.

Betreiber drahtloser Netzwerke sollen die Nutzer über das Sicherheitsniveau in den Netzwerken und über die verfügbaren Maßnahmen zur Sicherstellung der Vertraulichkeit der Kommunikation informieren.

D) Weitere Erwägungen

Anbieter drahtloser Netzwerke sollten die rechtlichen Anforderungen[5] einhalten, die in den unterschiedlichen Rechtssystemen differieren können.

Die Arbeitsgruppe betont ferner, dass Sicherheitskonzepte für die Nutzer schwer zu verstehen sind. Die praktische Anwendung dürfte selbst für erfahrene IT-Spezialisten schwierig sein. Die Industrie als Ganzes sollte das Problem sowohl auf der technischen als auch auf der Informationsebene angehen, um das Vertrauen in die Technologie zu verbessern. Die Voreinstellungen sollten ein hohes Datenschutzniveau gewährleisten.

Internet-Diensteanbieter, insbesondere Web-Mailer, sollten die Möglichkeit zur Verschlüsselung auf Anwendungsebene bieten. Werden sensitive Daten über drahtlose Netzwerke übertragen ist eine starke Verschlüsselung unverzichtbar.

Nutzer sollten nicht davon abgehalten werden, öffentlich zugängliche Dienste anonym oder unter Pseudonym zu nutzen.

[5] Vgl. Art. 4 Richtlinie 2002/58/EC des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Arbeitpapier zu Meinungsäußerungsfreiheit und Persönlichkeitsrecht bei Online-Publikationen*

– Übersetzung –

Bedenkt man, dass mehr als 10 Jahre vergangen sind, seit das Internet für Online-Publikationen genutzt wird, ist es notwendig, das Verhältnis zwischen den elementaren Menschenrechten der freien Meinungsäußerung und des Persönlichkeitsrechts erneut zu überdenken. In jüngster Zeit wurde von Personen, die personenbezogene Daten im Internet veröffentlicht haben, geltend gemacht, dass das Recht auf freie Meinungsäußerung ihnen erlaube, das Recht der Betroffenen am Schutz ihrer persönlichen Daten zu übergehen.

Es muss aber betont werden, dass diese genannten Rechte dieselbe Priorität genießen und im allgemeinen keines von beiden dem anderen vorgehen sollte.

Das Datenschutzniveau bei Online-Publikationen sollte sich vielmehr an einem vorsichtig ausgewogenen Kompromiss zwischen dem individuellen Persönlichkeitsrecht und dem Recht auf freie Meinungsäußerung orientieren.

Beziehen sich Informationen über das Privat- oder Familienleben, die private Korrespondenz und die Privatwohnung auf eine bestimmte oder bestimmbare natürliche Person, müssen die zentralen Vorschriften über den Datenschutz Anwendung finden. Das Recht auf freie Meinungsäußerung darf gegenüber dem Persönlichkeitsrecht nicht die Oberhand gewinnen.

Ungeachtet besonderer Privilegien für journalistische Aktivitäten, die gesetzlich geregelt werden können, sollten die folgenden vorrangigen Prinzipien bei Online-Publikationen Beachtung finden:

– Die Daten müssen in legaler und fairer Weise erhoben werden.
– Es muss ein Recht auf Gegendarstellung und auf Berichtigung von unwahren Tatsachen eingeräumt werden.
– Es muss ein Recht auf Zugang zu den veröffentlichten Daten eingeräumt werden.
– Es muss ein Beschwerdeverfahren eingerichtet werden.

Journalisten sind nicht verpflichtet, ihre Informationsquellen zu überprüfen und gegenüber den betroffenen Personen oder anderen offen zu legen, außer in gesetzlich besonders vorgesehenen Fällen.

* Aufgrund von Zuständigkeitsproblemen waren Norwegen und Schweden nicht in der Lage, das Dokument zu unterstützen.

2. 36. Sitzung am 18./19. November 2004 in Berlin

Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

– Übersetzung –

Wie in der realen Welt besteht Kriminalität zum größten Teil aus Eigentumsdelikten. Die am meisten verbreitete Form sind offenbar Betrug und Urheberrechtsverletzungen.

Das Zentrum für Beschwerden gegen Internetbetrug (Internet Fraud Complaint Center (IFCC)) nennt Internetbetrug in seinem Bericht für 2002 als wachsendes Problem[1]. Betrug bei Versteigerungen war das am häufigsten angezeigte Vergehen.

Der Ministerrat der OECD hat die „OECD Richtlinien zum Schutz der Verbraucher vor betrügerischen grenzüberschreitenden Handelspraktiken“ am 11. Juni 2003 beschlossen[2]. Viele Mittel wurden zur Bekämpfung der Cyberkriminalität/des Online-Betrugs vorgeschlagen. Die meisten davon betreffen verbesserte Formen der Strafverfolgung und verbesserte Zusammenarbeit zwischen den Regierungen. Auch wenn diese Mittel zweifellos nützlich sind, können sie auch zu Datenerhebungen und -übermittlungen Anlass geben, die Datenschutzprobleme aufwerfen.

Demgegenüber sind Mittel, die die Vorbeugung in den Vordergrund stellen, bisher offenbar weniger beachtet worden. Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation betont die positiven Wirkungen, die präventive Techniken auf die Senkung der Kriminalitätsrate im allgemeinen und die Sicherung von Aspekten des Datenschutzes bei der Strafverfolgung haben können. Die Internationale Arbeitsgruppe zum Datenschutz bei der Telekommunikation hat sich mit diesem Fragenkreis bereits früher befasst[3].

Die folgenden Methoden und Techniken können zur datenschutzgerechten Bekämpfung des Online-Betrugs genutzt werden:

---

[1] http://www1.ifccfbi.gov/strategy/wn030409.asp

[2] http://www.oecd.org/dataoecd/24/33/2956464.pdf

[3] Common Position on the detection of fraud in telecommunications adopted at the 27th Meeting of the Working Group on 4-5 May 2000 in Rethymnon / Crete,
available online http://www.datenschutz-berlin.de/doc/int/iwgdpt/fr_en.htm

- **Digitale Signaturen** können dazu beitragen, die Geschäftspartner zu identifizieren;

- **Treuhanddienste** können den Austausch von Waren und Geld für beide Parteien durch den Einsatz von vertrauenswürdigen Dritten sicherer machen;

- **Auditierung und Gütesiegel** können den Kunden helfen, vertrauenswürdige Online-Händler zu erkennen;

- **Verbesserte Bezahlverfahren** sind weniger anfällig für Betrugsmanöver;

- **Besser informierte Kunden** werden seltener Opfer solcher Manöver;

- **Besser informierte Unternehmen** neigen eher dazu, Systeme zu nutzen, die besser gegen Betrug geschützt sind;

- **Verbesserte Sicherheit** kann viele Formen betrügerischen Handelns verringern, das Computersysteme ins Visier nimmt oder deren Schwächen ausnutzt, um Menschen zu täuschen.

Die Erläuterungen zu diesem Dokument enthalten praktische Beispiele hierfür.

Schlussfolgerungen

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation empfiehlt, dass Behörden

- in erster Linie Mittel einsetzen sollten, die dem Online-Betrug vorbeugen, bevor sie Maßnahmen ergreifen, die derartige Straftaten nach ihrer Begehung bekämpfen sollen,

- Informationen und Beispiele der datenschutzfreundlichen Bekämpfung von Online-Betrug sammeln sollten,

- solche Informationen austauschen sollten,

- die Annahme datenschutzfreundlicher Verhaltensmaßregeln durch die Wirtschaft, insbesondere die Diensteanbieter, fördern sollten und

- die Öffentlichkeit und die Wirtschaft entsprechend informieren sollten.

Erläuternder Bericht zum Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

Dieser erläuternde Bericht stellt detaillierter einige der Verfahren zusammen, die genutzt werden können, um Online-Betrug ohne Verletzung von Bürgerrechten zu bekämpfen. In diesem Bericht wird auf vorhandene Beispiele entsprechender Dienstleistungen und Produkte hingewiesen. Dies ist nicht als positive Bewertung durch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation zu verstehen. Die Beispiele dienen lediglich als Anhaltspunkte für bereits vorhandene Lösungen. Die Informationen und Hyperlinks entsprechen dem Stand vom November 2004.

Digitale Signaturen

Digitale Signaturen können dazu beitragen, die Geschäftspartner zu identifizieren. Eine digitale Signatur ist eine von mehreren Möglichkeiten, um sich der Identität des Geschäftspartners zu vergewissern.

Digitale Signaturen sind nicht überall verfügbar und sie sind nicht perfekt. Es wird immer Mittel geben, um echte, aber irreführende Zertifikate zu erhalten oder um Menschen dazu zu verleiten, ohne digitale Signatur ein Geschäft abzuschließen, aber digitale Signaturen sind dennoch hilfreich.

Unternehmen können signierte Verkaufszertifikate ausstellen, die dem Käufer den Nachweis des Kaufs ermöglichen.

Treuhandsysteme

Systeme, in denen der Kaufpreis nicht sofort an den Verkäufer ausgezahlt, sondern von einem vertrauenswürdigen Dritten treuhänderisch verwaltet wird („escrow service“ – Treuhanddienst), können Betrug bei der Lieferung verhindern, bei dem ein unehrlicher Verkäufer Vorauszahlung verlangt und dann nicht liefert. Diese Art des Betrugs ist besonders verbreitet bei Online-Auktionen. Der IFCC 2002 Internet Betrugsbericht nennt den Fall „Vereinigte Staaten gegen Teresa Smith“, in dem Frau Smith Computer auf Internet-Auktionsplattformen verkaufte, aber nicht lieferte. Sie betrog auf diese Weise mehr als 300 Opfer und erschlich mehr als $ 800.000.

Bei einem Treuhanddienst übergibt der Käufer den Kaufpreis dem Treuhänder. Der Verkäufer erhält eine Information vom Treuhänder, dass das Geld für ihn bereit liegt und nicht zurückgezogen werden kann, während der Käufer den Treuhänder anweist, das Geld auszuzahlen, wenn er den Kaufgegenstand erhalten hat.

Im Streitfall bleibt das Geld beim Treuhänder hinterlegt, bis eine Einigung erzielt werden kann. Ein richtig eingesetzter Treuhanddienst kann Online-Betrug erheblich erschweren. Der Betrüger muss den Käufer oder den Treuhänder dazu verleiten, den Kaufpreis zu überweisen (z. B. indem er Gegenstände liefert, die ordnungsgemäß erscheinen, aber qualitativ minderwertig sind, oder indem er eine Auszahlungsanweisung fälscht). Alle diese Manöver sind allerdings für den Betrüger riskant und kostspielig.

Der Nachteil von Treuhanddiensten ist, dass sie für beide Parteien verfügbar und von ihnen akzeptiert sein müssen und dass sie Geld kosten. Personen, die an Geschäften mit legitimen, aber anstößigen Produkten (z. B. Pornographie) beteiligt sind, lehnen die Inanspruchnahme eines Treuhanddienstes möglicherweise aus Datenschutzgründen ab. Hochprofessionelle Betrüger können ihre eigenen Treuhanddienste anbieten. Andere Kriminelle können leichtgläubige Menschen davon abhalten, einen Treuhanddienst zu nutzen.

Ein zusätzlicher Vorteil aus Datenschutzsicht besteht darin, dass der Verkäufer vom Treuhänder die Information erhält, dass der vereinbarte Kaufpreis bereitliegt. Der Verkäufer muss nicht die Kreditwürdigkeit des Käufers überprüfen. Er muss nur dem Treuhänder vertrauen.

Ebay, ein populäres Internet-Auktionshaus, empfiehlt Treuhanddienste:
http://www.ebay.com/help/community/escrow.html

Verkäufer sollten ermutigt werden, mit Treuhanddiensten zusammenzuarbeiten und sie ihren Kunden zu empfehlen.

Auditierung und Gütesiegel

Wie kann man sich der Vertrauenswürdigkeit des Verkäufers versichern? Um diese Frage zu beantworten, sind verschiedene Programme für Audits und Gütesiegel entwickelt worden.

Diese Programme mögen nicht perfekt sein, aber sie sind ein Unterscheidungsmerkmal zwischen einem Online-Shop, über den die Kunden keine Informationen haben, und einem Online-Shop, der von einer vertrauenswürdigen Stelle geprüft worden ist.

Verbesserte Bezahlverfahren

Ein großer Teil des Potentials für Missbrauch und Betrug liegt in technischen und organisatorischen Schwächen der Bezahlverfahren. Vor allem Kreditkarten sind besonders leicht zu missbrauchen. Viele Formen des Betrugs beziehen sich auf Kreditkartenzahlungen.

Die Behörden sollten prüfen, was zur Verbesserung der Bezahlungssysteme getan werden kann, so dass Betrüger weniger Möglichkeiten haben, um Sicherheitslücken auszunutzen.

Kundeninformation

Die beste Waffe gegen Betrug ist Information. Viele Länder haben bereits gute Kundeninformationsdienste, andere sollten nachziehen. In einigen Ländern bietet auch die Polizei Informationen an.

Es gibt genug Informationen (allerdings häufig auf Englisch). Die Bereitstellung und Verbreitung solcher Informationen in einer Sprache und Form, die den Bürgern entspricht, kann von großer Hilfe sein.

Informationen für Unternehmen

Sobald die Wirtschaft Systeme mit höherer Sicherheit einsetzt, die weniger anfällig für Manipulationen sind, dürfte dies die Betrugsfälle reduzieren.

Erhöhte Sicherheit

Betrug im Zusammenhang mit Angriffen auf Computersysteme wird häufig erleichtert durch unzureichende Sicherheitsmaßnahmen und unsichere Programme.

Betrug, der auf Computersysteme abzielt, ist eine verhältnismäßig neue Kriminalitätsform. Beim Computerbetrug ist das Hauptziel des Betrügers das Computersystem des Opfers. Der Kriminelle ist bestrebt, durch Manipulationen am Computer Zugriff auf finanzielle Mittel, Zugriffsrechte oder Ressourcen zu erhalten, die ihm nicht zugänglich sind oder die ihn Geld kosten würden. Einige Betrüger kopieren Kreditkarten-Daten, um Kreditkarten-Gesellschaften oder Banken zu betrügen[4]. Diese Betrugsart kann den Nutzer einbeziehen, allerdings nur zu einem bestimmten Grad, etwa indem jemand dazu verleitet wird, ein Programm herunterzuladen, das es dem Angreifer erlaubt, auf den Computer zuzugreifen („Trojanisches Pferd“).

Andere Kriminelle fälschen e-mails von Banken, um die Empfänger dazu zu veranlassen, Zugangsdaten für ihre Konten einzugeben (dies wird als „phishing“ bezeichnet). Phisher missbrauchen Sicherheitslücken in Browsern und e-mail-Programmen, um den fälschlichen Eindruck zu erwecken, jemand besuche die Website seiner Bank, während er in Wirklichkeit auf einer gefälschten Seite mit einer anderen Adresse ist.

[4] Dies wird häufig als „Identitätsdiebstahl“ bezeichnet.

Eine inzwischen verbreitete Angriffsart ist die heimliche Zweckentfremdung von Computern zur Versendung von unerwünschter Werbung (Spam). Dies ist zwar nicht Betrug im klassischen Sinn, es beruht aber auf Täuschung, um rechtswidrige Handlungen vorzunehmen. Darüber hinaus bieten viele Spam-Versender in betrügerischer Weise Güter und Dienstleistungen an. Weniger Spam bedeutet weniger Betrug.

Der beste Weg, solche Straftaten zu bekämpfen, ist die Verbesserung der Computersicherheit. Die Behörden können bessere Sicherheitsmaßnahmen, schnellere Reaktionen auf Sicherheitslücken und -bedrohungen und Rechtsbehelfe zum Schutz vor Schäden durch unsichere Systeme vorschlagen. Es ist möglich, die Bürger zum Einsatz von Technologie mit höherer Sicherheit aufzufordern.

Hersteller können dies ebenfalls unterstützen, indem sie die Vorteile von Hard- und Software-Lösungen mit höherer Sicherheit herausstellen, insbesondere beim Einsatz von Firewalls bei Breitbandverbindungen. Diese können die Angriffsmöglichkeiten reduzieren, indem sie unerkannte eingehende Verbindungsversuche blockieren.

Manchmal können sogar einfache Dinge wie ein gutes e-mail-Programm und ein gut gemachter Web-Browser hilfreich sein.

Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten (Revision des Gemeinsamen Standpunkts, angenommen auf der 29. Sitzung am 15./16. Februar 2001 in Bangalore)

– Übersetzung –

Aufenthaltsinformationen wurden in mobilen Kommunikationsdiensten von Anfang an verarbeitet. Solange diese Informationen nur zum Aufbau und zur Aufrechterhaltung einer Verbindung zu dem mobilen Endgerät generiert und genutzt wurden, verfügten nur die Anbieter von Telekommunikationsnetzen, die in den meisten Ländern sehr strikt auf die Wahrung des Fernmeldegeheimnisses verpflichtet sind, über Aufenthaltsinformationen. Die Genauigkeit der Ortung richtete sich nach der Größe der betreffenden Funkzelle in den zellularen Netzwerken.

Teilweise veranlasst durch gesetzliche Verpflichtungen, präzisere Informationen über den Aufenthaltsort eines mobilen Endgerätes für Rettungsdienste verfügbar zu machen, haben die Betreiber von Netzwerken damit begonnen, die technische Infrastruktur ihrer Netzwerke zu verändern, um diese Verpflichtungen zu erfüllen. Dies bedeutet, dass in naher Zukunft wesentlich genauere Informationen über den Aufenthaltsort eines jeden mobilen Endgerätes verfügbar sein werden. Endgerätehersteller geben an, dass selbst heute eine Präzision von bis zu fünf Metern technisch möglich ist, wenn GPS-unterstützte Systeme benutzt werden. Gleichzeitig ist abzusehen, dass die Entwicklung des mobilen elektronischen Geschäftsverkehrs zur Schaffung einer Vielzahl neuer Dienste führen wird, die auf der Kenntnis des präzisen Aufenthaltsortes des Nutzers basieren. Diese Dienste werden aller Wahrscheinlichkeit nach nicht nur von Telekommunikationsdiensteanbietern, sondern auch von Dritten angeboten werden, die nicht an die gesetzlichen Beschränkungen des Fernmeldegeheimnisses gebunden sind.

Die verbesserte Genauigkeit von Aufenthaltsinformationen und ihrer Verfügbarkeit nicht nur für die Betreiber mobiler Telekommunikationsnetzwerke kann neue, bisher nicht da gewesene Risiken für den Datenschutz von Nutzern mobiler Endgeräte in Telekommunikationsnetzwerken zur Folge haben. Die Arbeitsgruppe hält es dafür für erforderlich, dass die Technologie zur Ortung mobiler Endgeräte in einer Weise entwickelt wird, die die Privatsphäre so wenig wie möglich beeinträchtigt.

Hinsichtlich des Angebots von Mehrwertdiensten sollten die folgenden Prinzipien beachtet werden:

1. Der Entwurf und die Auswahl technischer Einrichtungen solcher Dienste sollten an dem Ziel orientiert sein, entweder überhaupt keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

2. Präzise Aufenthaltsinformation sollte nicht als ein Standard-Leistungsmerkmal eines Dienstes generiert werden, sondern nur „nach Bedarf", wenn dies notwendig ist, um einen bestimmten Dienst zu erbringen, der an den Aufenthaltsort des Nutzers geknüpft ist.

3. Der Nutzer muss die volle Kontrolle darüber behalten, ob präzise Aufenthaltsinformationen im Netzwerk entstehen. In dieser Hinsicht scheinen Endgerätebasierte Lösungen, bei denen die Entstehung präziser Aufenthaltsinformation durch das mobile Endgerät initiiert wird, ein höheres Maß an Datenschutz zu bieten als Netzwerk-basierte Lösungen, bei denen Aufenthaltsinformationen als ein Standard-Leistungsmerkmal generiert und die Kontrolle des Nutzers sich darauf beschränkt, in welchem Umfang diese Informationen an Dritte übermittelt werden. In jedem Fall sollte der Mobilfunkteilnehmer immer in der Lage sein, sowohl die Inanspruchnahme jedes standortbezogenen Dienstes als auch spezieller standortbezogener Dienste zu kontrollieren. Der Anbieter sollte dem Teilnehmer die Möglichkeit einräumen, bei Abschluss des Teilnehmervertrags in die Nutzungsmöglichkeit jedes standortbezogenen Dienstes einzuwilligen. Der Teilnehmer darf bereits zu diesem Zeitpunkt oder später seine Zustimmung geben und darf die Inanspruchnahme sämtlicher Dienste jederzeit ablehnen. In Fällen, in denen der Mobilfunkteilnehmer eingewilligt hat, sollte der Mobilfunknutzer, der nicht mit dem Teilnehmer identisch ist, die Möglichkeit haben den Dienst zu akzeptieren oder abzulehnen.

4. Der Telekommunikationsdiensteanbieter darf nur in den Fällen Informationen an Dritte liefern, in denen der Mobilfunkteilnehmer zu der anderweitigen Nutzung der Aufenthaltsinformationen seine informierte Einwilligung erteilt hat. Nutzer sollten die Möglichkeit haben, die präzise Aufenthaltsbestimmung jederzeit abschalten zu können, ohne dafür die Verbindung ihres Endgerätes zum Netzwerk trennen zu müssen. Nutzer und Teilnehmer sollten auch die Möglichkeit haben, Aufenthaltsinformationen mit einem selbstgewählten Grad von Genauigkeit zu offenbaren (z. B. auf der Ebene eines einzelnen Gebäudes, einer Straße, einer Stadt oder eines Bundesstaates).

5. Aufenthaltsinformation sollte Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung zu einer solchen Offenlegung erteilt hat. Die Einwilligung kann auf eine einzelne Transaktion oder bestimmte Anbieter von Mehrwertdiensten beschränkt sein. Der Nutzer muss in der Lage sein, auf Daten über seine Präferenzen zuzugrei-

fen, diese zu berichtigen und zu löschen, unabhängig davon, ob diese auf dem mobilen Endgerät oder innerhalb des Netzwerkes gespeichert sind.

6. Die Erstellung von Bewegungsprofilen durch Anbieter von Telekommunikationsdiensten und Anbieter von Mehrwertdiensten sollte durch Gesetz strikt verboten werden, außer wenn dies für die Erbringung eines bestimmten Dienstes notwendig ist und der Nutzer hierzu zweifelsfrei seine informierte Einwilligung gegeben hat.

7. Daten über den Aufenthaltsort stellen eine hoch sensible Kategorie von Informationen dar. Der Zugriff auf solche Informationen sowie deren Übermittlung und Nutzung sollten Gegenstand der gleichen oder gleichartiger Kontrollen sein wie für Inhaltsdaten, die durch das Fernmeldegeheimnis geschützt werden. Die Arbeitsgruppe weist auf ihren Gemeinsamen Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation hin (Hong Kong, 15. April 1998; http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_de.htm).

8. Wo immer dies möglich ist, sollten Betreiber von Mobilfunknetzen Aufenthaltsinformationen nicht zusammen mit personenbezogenen Informationen über den Nutzer an Anbieter von Mehrwertdiensten weiterleiten. Stattdessen sollten pseudonymisierte Informationen genutzt werden. Personenbezogene Informationen (z. B. die Kennung eines mobilen Endgerätes) sollten Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung gegeben hat. Jegliche Aufenthaltsinformation sollte vom Anbieter gelöscht werden, sobald sie für die Erbringung des Dienstes nicht länger erforderlich ist.

9. Ein Anbieter darf die Nutzung eines Dienstes oder die Bedingungen für die Nutzung eines Dienstes nicht von der Einwilligung des Nutzers in die Verarbeitung personenbezogener Aufenthaltsinformationen abhängig machen, wenn diese Daten für die Erbringung des Dienstes nicht erforderlich sind.

Arbeitspapier zu Lehrplänen zur Internetsicherheit unter Berücksichtigung nationaler, kultureller und rechtlicher (einschließlich datenschutzrechtlicher) Anforderungen

– Übersetzung –

Sicherheit von Informationssystemen

In der frühen Entwicklungszeit der Automation war die Sicherheit von Informationssystemen vor allem mit bescheidenen Stand-alone-Systemen in geschlossenen Netzwerken befasst und war entsprechend in ihrer Reichweite begrenzt auf die Übernahme relativ einfacher Regeln für die physische, hard- und softwaremäßige Sicherheit.

Später haben die starke Zunahme von immer leistungsfähigeren Personalcomputern, die Verbreitung neuer Informations- und Kommunikationstechnologien, der umfassende Gebrauch des Internet und die zunehmende Abhängigkeit menschlicher Aktivitäten von einem ordnungsgemäßen Funktionieren der Informationssysteme die Situation komplexer gemacht.

Heute kann die Sicherheit von Informationssystemen nicht mehr begrenzt werden auf Gegenmaßnahmen gegen Symptome angesichts technischer Sicherheitsbedrohungen, sondern es ist nötig, elementare Änderungen von Verhaltensmustern von allen Beteiligten einzuführen, um den eindringlichen Bedrohungen zu begegnen, denen menschliche Werte und Menschenrechte bezüglich der Sicherheit im Internet ausgesetzt sind.

Dieser neue globale und systematische Zugang zur Informationssicherheit ist unterstrichen und vorangetrieben worden durch die OECD, deren Veröffentlichung „Guidelines for the Security of Information Systems and Networks“ die Notwendigkeit anerkennt, eine echte „Sicherheitskultur“ zu entwickeln.

Sicherheit von Informationssystemen versus Datenschutz

Um ihre jeweiligen Aufgaben zu erfüllen, müssen heute alle Organisationen, gleich ob es öffentliche oder private Stellen sind, eine zunehmende Menge von Daten und immer mehr personenbezogene Daten in ihren Informationssystemen erheben, verarbeiten und speichern.

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht und ein wirksamer Datenschutz kann nicht erreicht werden ohne angemessene Sicher-

heit. Das ist bereits 1980 durch die „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ anerkannt worden. Da Sicherheit zwingend erforderlich ist, um Persönlichkeitsrechte zu schützen, verlangt der spezifische gesetzliche Schutz personenbezogener Daten im Vergleich zu anderen Daten und deren Sicherheit oft einen völlig verschiedenen Zugang. Die fundamentalen Datenschutzprinzipien wie das Recht auf Vergessen, das Recht auf Zugang, die Begrenzung der Erhebung und Verarbeitung sowie das Verhältnismäßigkeitsprinzip sind bedauerlicherweise keine grundsätzlichen Prinzipien, die von Sicherheitsexperten notwendigerweise anerkannt werden.

Informationssicherheitsexperten

Heute hat sich die Sicherheit von Informationssystemen nicht nur mit den technischen Risiken der verschiedenen Computerplattformen, Netzwerke, Protokolle oder anderen Bestandteilen von Informationssystemen zu befassen, sondern hat ebenso andere Risiken in Betracht zu ziehen, wie sie mit der Organisation des Unternehmens und ihren Verfahrensweisen zusammenhängen, solche, die sich auf Personaldaten beziehen oder solche, die mit den bestehenden rechtlichen Beschränkungen zusammenhängen wie etwa dem Datenschutz oder dem Urheberrecht.

Diese multidisziplinäre Wahrnehmung von Risiken ist in der Welt von Informationssicherheitsexperten nicht die Regel. Zu oft wird die Sicherheit von Informationssystemen noch als eine Angelegenheit für Computer- oder Technikexperten betrachtet und darüber hinaus nur begrenzt auf prophylaktische technische Maßnahmen, mit der Folge komplexer Sicherheitssysteme, die in einer Zunahme technischer Kontrollen von zweifelhafter Bedeutung resultieren, die den Datenschutz durchaus beeinträchtigen können.

Selbst wenn der Bedarf an hochausgebildeten Sicherheitsexperten umfassend anerkannt ist, gibt es wenige konkrete strukturierte Initiativen, um die bestehenden Erwartungen zu erfüllen. Oft ist der Begriff eines Informationssicherheitsberaters weder eingeführt, definiert noch durch gesetzliche Regelungen umschrieben. Der Zugang zu diesem Beruf ist einem Zertifizierungsprozess überlassen, der durch private Institutionen organisiert wird.

Empfehlungen

Angesichts dieser Situation empfiehlt die Arbeitsgruppe angesichts der erstrangigen Rolle, die die Sicherheit von Informationssystemen und der Datenschutz beim ordnungsgemäßen Funktionieren von Organisationen spielen, dass:

– das Konzept eines Informationssystemssicherheitsberaters unterstützt wird, der dem CISO-Konzept (Corporate Information Security Officer) entspricht, das in verschiedenen internationalen Normen und Veröffentlichungen beschrieben wird und das alle notwendigen Datenschutzaspekte umfasst.

– Angesichts der Verantwortlichkeiten, die mit der Ausübung einer solchen Funktion verbunden sind, besteht unzweifelhaft der Bedarf höherer Professionalität. Sehr oft erfordern diese Funktionen einen Hochschulabschluss. Demgemäß sollte eine akademische oder berufsbildende Qualifikation für Informationssystemssicherheitsberater eingeführt werden, die eine Ausbildung gewährleistet, die die nationalen rechtlichen und kulturellen Traditionen berücksichtigt und die so neutral und unabhängig von wirtschaftlichen Interessen ausgestaltet ist wie irgend möglich. Zertifiziert werden sollten mit der Qualifikation alle notwendigen technischen Kenntnisse über Sicherheit, die einschlägigen Managementfähigkeiten, Wissen darüber, wie Sicherheit am besten organisiert werden kann, Kenntnis fundamentaler Datenschutzregelungen und schließlich alle relevanten rechtlichen Kenntnisse, die Sicherheitsberater in die Lage versetzen, ihre Rolle innerhalb der Organisation korrekt auszufüllen.

VI. Sonstige Dokumente zum Datenschutz

Berliner Memorandum zu Datenschutzerklärungen

– Übersetzung –

Komplizierte/komplexe Datenschutzerklärungen für Verbraucher und Bürger dienen keinem sinnvollen Aufklärungszweck, weil:

- Verbraucher und Bürger sie zu lang und unverständlich finden und deshalb die Erklärungen keine wirksame Rückmeldung von Verbrauchern und Bürgern ermöglichen;

- Unternehmen und Behörden in ihnen ein Hindernis zur Vertrauensbildung bei ihren Kunden und Bürgern sehen; und

- Regulierer/Gesetzgeber erkennen, dass komplexe Datenschutzerklärungen ihre Ziele der Bewusstseinsschärfung und Verbesserung der Normbefolgung konterkarieren.

Dieses Problem besteht in allen Bereichen und zudem grenzüberschreitend. Eine internationale Gruppe von dreiundzwanzig Experten von Verbraucherorganisationen, Datenschutzbehörden, und aus verschiedenen Unternehmensbereichen hat sich am 23. März 2004 in Berlin mit diesen Fragen beschäftigt. In dem Bewusstsein, dass eine neue Struktur/Architektur von Datenschutzerklärungen notwendig ist, sind ihre Diskussionen in dem folgenden Memorandum zusammengefasst.

Wirkungsvolle Datenschutzerklärungen sollten in einem Rahmen abgegeben werden, der die folgenden Kernbegriffe zugrunde legt:

Mehrstufig/Gestaffelt

Informationen über Datenschutz können und sollten normalerweise nicht in einem einzigen Dokument oder in einer Nachricht übermittelt werden. Stattdessen sollte die Information über die Datenschutzpraktiken einer Stelle in einem mehrstufigen Format gegeben werden. Die „kurze“ (komprimierte oder hervorgehobene) Informationsebene sollte die wichtigste Information bereit halten, die Einzelne/Betroffene benötigen, um ihre Stellung zu verstehen und Entscheidungen zu treffen. Noch kürzere Informationsebenen kommen in Betracht für Coupons/Gutscheine, Handy-Displays und andere Orte, an denen Informationen

nötig sind, aber der Platz äußerst knapp ist. Zusätzliche Informationen sollten dann auf längeren, vollständigeren Informationsplattformen/-ebenen leicht zugänglich sein. Dieser Ansatz verbessert sowohl das Verständnis als auch die Befolgung von rechtlichen Regelungen, weil die Datenschutzerklärung – insgesamt gesehen – Inhalte in einer Form vermitteln kann, die verständlicher und sowohl dem jeweiligen Medium als auch der Zielgruppe angemessener ist.

Verständnis und klare Sprache

Alle Ebenen sollten sich einer leicht verständlichen Sprache bedienen. Verständlichkeit für die Adressaten ist ein wichtiges Ziel von Datenschutzerklärungen, damit sie deren Inhalt verstehen, informierte Entscheidungen treffen und das Wissen und Verständnis haben können, um Datenschutzpraktiken zu beeinflussen.

Normbefolgung

Die gesamte Datenschutzerklärung (alle Ebenen zusammen genommen) müssen mit dem jeweils anwendbaren Recht übereinstimmen, während jede Ebene dem Einzelnen diejenige Information vermitteln muss, die er benötigt, um zu dem jeweiligen Zeitpunkt eine informierte Entscheidung zu treffen. Es ist von besonderer Bedeutung, auf „Überraschungen" aufmerksam zu machen – also Formen der Datenverarbeitung, die den anerkannten oder erwarteten Rahmen überschreiten.

Einheitliches Format

Ein einheitliches Format und Layout wird Verständnis und Vergleichbarkeit erleichtern. Verbraucher lernen durch Wiederholung und es ist wichtig, dass Datenschutzerklärungen des privaten und öffentlichen Sektors ein einheitliches Format und Layout haben, um diesen Lerneffekt zu unterstützen. Weitere Diskussionen sind nötig, wie die Einheitlichkeit beibehalten und gleichzeitig die bestehenden Unterschiede berücksichtigt werden können.

Kürze

Die Länge einer Datenschutzerklärung ist entscheidend. Forschungsergebnisse haben gezeigt, dass Menschen nur in der Lage sind, einer Datenschutzerklärung Informationen in begrenztem Umfang zu entnehmen. Die Kurzinformation sollte nicht mehr enthalten als Menschen *auf den ersten Blick* sinnvollerweise aufnehmen können. Die Forschungsergebnisse zeigen übereinstimmend, dass nicht mehr als sieben Kategorien/Themen mit begrenzten Informationen in jeder Kategorie/jedem Thema verwendet werden sollten. Die Langinformationen müssen möglicherweise ausführlich sein, wenn das zur Lesbarkeit und Vollständigkeit beiträgt.

Öffentlicher Sektor

Diese Grundsätze sind in gleicher Weise auf die Erhebung und Verarbeitung von personenbezogenen Daten durch öffentliche Stellen anzuwenden.

Die kurze Datenschutzerklärung

Die Kurzinformation sollte die erste Information sein, die ein Betroffener (online oder auf Papier) erhält, wenn erstmals personenbezogene Daten erhoben werden. Das Ziel dieser Erklärung sollte es sein, die wesentlichen Informationen in besonders lesbarer Form und in einem (bezogen auf den jeweiligen Sektor) vergleichbaren Format zu vermitteln. Die Kurzinformation sollte enthalten:

- Auf wen die Datenschutzerklärung anzuwenden ist (d. h. wer die für die Datenverarbeitung verantwortliche Person oder Stelle ist);
- Die Datenarten, die unmittelbar beim Betroffenen oder bei Dritten über ihn erhoben werden;
- Zwecke der Verarbeitung;
- Die Arten/Kategorien von Stellen, an die Daten weiter gegeben werden können (wenn Übermittlungen stattfinden);
- Hinweis auf Rechte des Einzelnen, die Verwendung der Daten zu begrenzen und/oder Zugangs- und/oder sonstige Rechte auszuüben und wie diese Rechte ausgeübt werden, und
- wie Kontakt zum Datenverarbeiter aufgenommen werden kann, um weitere Informationen zu erhalten, und welche Beschwerdemöglichkeiten (beim Datenverarbeiter oder – soweit notwendig/angemessen – bei einer unabhängigen Kontrollstelle) bestehen.

Die kurze Datenschutzerklärung sollte in einem einheitlichen Format gehalten sein, das es dem Einzelnen erleichtert, die oben genannten Elemente aufzufinden, die für ihn wesentlich sind. Während Erklärungen sich von Organisation zu Organisation (Stelle zu Stelle) und von Bereich zu Bereich unterscheiden werden, wird ein ähnliches Format das Wissen und die Wahlfreiheit des Einzelnen erhöhen. Feldstudien in den USA haben gezeigt, dass Verbraucher Auswahlboxen mit hervorgehobenen Überschriften bevorzugen.

Die vollständige Datenschutzerklärung enthält alle vom nationalen Recht vorgeschriebenen Informationen im Detail. Sie sollte dennoch so lesbar wie möglich und in einer Sprache verfasst sein, die der Einzelne leicht verstehen kann.

B. Dokumente zur Informationsfreiheit

I. Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID)

Verbesserter Zugang zu den Umweltinformationen durch die neue Richtlinie der Europäischen Union

Das bundesdeutsche Umweltinformationsgesetz beruht auf der europäischen Umweltinformationsrichtlinie, die im vergangenen Jahr neu gefasst und wesentlich erweitert worden ist. Deshalb sind die Mitgliedstaaten der Europäischen Union verpflichtet, ihre Umweltinformationsgesetze entsprechend zu ändern.

Die Informationsbeauftragten der Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein stellen fest, dass die Frist zur Umsetzung der Umweltinformationsrichtlinie bereits im Februar 2005 ausläuft. Sie fordern die Gesetzgeber auf, die Verbesserungen der europäischen Richtlinie unverzüglich in nationales Recht umzusetzen. Unter anderem verdienen folgende Punkte eine besondere Aufmerksamkeit:

- Der Begriff der „Informationen über die Umwelt“ ist weiter gefasst als bisher. Nunmehr sind neben Informationen zu Wechselwirkungen von gentechnisch veränderten Organismen zur Umwelt auch Angaben zum Zustand der menschlichen Gesundheit und Sicherheit, zu Belastungen der Nahrungskette und zu umweltbedingten Beeinträchtigungen bei Bauwerken offen zu legen.

- Werden im Umweltbereich öffentliche Aufgaben privatisiert, so gilt das Recht auf Zugang zu Umweltinformationen auch gegenüber privaten Unternehmen.

- Ein Antrag auf Zugang zu Umweltinformationen darf zum Schutz behördlicher oder privater Interessen nur noch abgelehnt werden, wenn die Abwägung entgegen stehender Interessen ein überwiegendes Geheimhaltungsinteresse ergibt.

- Öffentliche Stellen wie private Unternehmen, die öffentliche Umweltaufgaben wahrnehmen, werden verpflichtet, Umweltinformationen von sich aus – auch im Internet – zu veröffentlichen.

Das Ziel des Umweltinformationsgesetzes – also die Verbesserung der Umwelt durch das Engagement der Bürgerinnen und Bürger – kann umso effektiver

erreicht werden, je transparenter das Verwaltungshandeln ist. Die europarechtlich vorgegebenen Verbesserungen tragen zu mehr Transparenz bei. Bund und Länder sollten daher nicht weiter zögern, ihren Verpflichtungen nachzukommen und den Umweltinformationszugang auch in Deutschland zu stärken. Personen, die bei Bundesbehörden oder Landesbehörden, für die noch kein allgemeines Informationszugangsrecht gilt, Verwaltungsakten einsehen möchten, sind darauf besonders angewiesen.

Soweit die Umweltinformationsrichtlinie nicht allein durch ein Bundesumweltinformationsgesetz, sondern auch auf Länderebene umgesetzt werden sollte, regen die Informationsbeauftragten an, ein Zusammenführung von Umweltinformationsgesetz und allgemeinem Informationsgesetz in Erwägung zu ziehen. Für die Bürgerinnen und Bürger könnten Unsicherheiten vermieden werden, wenn ihre Informationsrechte in nur einem Gesetz bestimmt wären.

Öffentlichkeit der Sitzungen von Entscheidungsgremien

Die Forderung nach einer gesetzlichen Regelung der Informationsfreiheit wird bisher in Deutschland nur mit dem Recht auf Zugang zu Informationen in Verbindung gebracht, die bei den Behörden in Form von Akten, elektronisch gespeicherten Daten oder anderer Datenträger vorhanden sind. Von ebenso großer Bedeutung für die Transparenz staatlicher Entscheidungsfindung ist jedoch die Möglichkeit der Teilnahme an den Sitzungen von Gremien, die in einer Vielzahl öffentlicher Stellen mit erheblichen Entscheidungsbefugnissen ausgestattet sind.

Die Öffentlichkeit von Gerichtsverhandlungen ist eine der frühen Errungenschaften des Rechtsstaates. Obwohl auch Plenarsitzungen von Parlamenten von jeher öffentlich stattfinden, tagen in vielen Ländern aber die Landtagsausschüsse in der Regel nach wie vor nichtöffentlich. Dies ist auch auf der kommunalen Ebene der Fall. Bei anderen öffentlichen Stellen, deren Entscheidungen durch demokratische Mitwirkungsgremien legitimiert werden, wie z. B. Bildungs-, Sozial- oder Versorgungseinrichtungen, sind nicht-öffentliche Sitzungen die Regel.

Transparenz staatlichen Verhaltens erfordert aber im Gegenteil, dass auch die Entscheidungsfindung staatlicher Gremien grundsätzlich in der Öffentlichkeit stattfindet. Dies schließt nicht aus, dass für bestimmte Bereiche (z. B. Personalentscheidungen oder Verschlusssachen) oder von Fall zu Fall (z. B. wenn der Schutz personenbezogener Daten dies erfordert) die Öffentlichkeit ausgeschlossen wird.

In den USA wurde in der Folge der Gesetzgebung zur Informationsfreiheit im Rahmen der „Government in the Sunshine Acts“ sowohl auf der Ebene des Bundes als auch der Einzelstaaten festgelegt, dass der Meinungsaustausch in behörd-

lichen Kollegialsitzungen im Lichte der Öffentlichkeit durchzuführen ist. Ort, Zeitpunkt und Gegenstand der Sitzungen sind vor dem Termin öffentlich bekannt zu machen. Der Ausschluss der Öffentlichkeit ist zu begründen. Nichtöffentliche Sitzungen sind zu protokollieren, damit der Inhalt von Sitzungen, bei denen die Öffentlichkeit widerrechtlich ausgeschlossen wurde, nachvollziehbar bleibt.

Die Arbeitsgemeinschaft der Informationsbeauftragten der Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein fordern, dass der Grundsatz der Öffentlichkeit von Sitzungen für alle Gremien eingeführt wird. Diese stellen ihre Verantwortung gegenüber dem Gemeinwohl vor allem dadurch unter Beweis, dass Bürgerinnen und Bürgern Zugang zu den Sitzungen von staatlichen Gremien erhalten. Der Ausschluss der Öffentlichkeit ist nur für bestimmte und abschließend zu regelnde Tatbestände zuzulassen.

II. Internationale Konferenz der Informationsbeauftragten (ICIC)

Einladung zur Internationalen Konferenz der Informationsbeauftragten am 2./3. Februar 2004

Die südafrikanische Menschenrechtskommission wird die zweite Internationale Konferenz der Informationsbeauftragten am 2. und 3. Februar 2004 in Kapstadt, Südafrika, ausrichten. Dies ist eine Folgesitzung der ersten und Gründungskonferenz, die in Berlin, Deutschland, im April 2003 abgehalten wurde. Die Konferenz ist eine jährliche internationale Zusammenkunft von Informationsbeauftragten, um Informationen und Erfahrungen zu den Durchsetzungsmechanismen bei der Einführung des Rechtes auf Informationsfreiheit auszutauschen.

Die Konferenz soll folgende Themen behandeln:

– Wie Informationsbeauftragte das Problem der Nichtbeachtung der Informationsfreiheitsgesetzgebung durch private Institutionen und Regierungsbehörden behandelt haben.

– Allgemein akzeptierte Normen für Ausnahmen des Zugangsrechtes in der Informationsfreiheitsgesetzgebung (Belange des Datenschutzes, vorrübergehende Begrenzungen für Dateien, die sich auf einen laufenden Entscheidungsprozess bei Behörden beziehen oder bei denen die Offenlegung den Erfolg laufender Verwaltungsmaßnahmen gefährden würde; besonders berücksichtigt wird, wie öffentliche Bereiche wie Parlament, Gerichte, unabhängige Behörden usw. von der Anwendung ausgeschlossen werden könnten).

– Erfolge und Herausforderungen bei der Einführung einer Informationsfreiheitsgesetzgebung für private Institutionen angesichts des Umstands, dass mit Ausnahme des südafrikanischen Gesetzes (Promotion of Access to Information Act 2 of 2000) die meisten Informationsfreiheitsgesetze für private Stellen nicht anwendbar sind.

Dr. Leon Wessels
Verantwortlicher Kommissar für das
Recht auf Informationszugang,
Südafrikanische Menschenrechtskommission

Die Schriftenreihe „Dokumente zu Datenschutz und Informationsfreiheit“ wird gemeinsam vom Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit herausgegeben. In ihr werden Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen zum Datenschutz veröffentlicht.

Der vorliegende Band mit Dokumenten aus dem Jahr 2004 enthält Beschlüsse und Entschließungen der

- Konferenz der Datenschutzbeauftragten des Bundes und der Länder,
- Europäischen Konferenz der Datenschutzbeauftragten,
- Europäischen Union,
- Internationalen Konferenz der Datenschutzbeauftragten,
- Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation,
- Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland,
- Internationalen Konferenz der Informationsbeauftragten

sowie

das Berliner Memorandum zu Datenschutzerklärungen.