Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht

Berliner Beauftragter
für Datenschutz und
Informationsfreiheit

Dokumente zu Datenschutz und Informationsfreiheit

2005

Dokumente
zu Datenschutz
und Informationsfreiheit

2005

Impressum

Herausgeber:

Die 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 03/3 56 0 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: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH

Stand: Januar 2006

Inhaltsverzeichnis

Vorwort

Eine moderne Informationsgesellschaft braucht mehr Datenschutz. Die gleich lautende Entschließung der Datenschutzbeauftragten des Bundes und der Länder formuliert das zentrale Datenschutzproblem des Jahres 2005, aber wohl auch der kommenden Jahre auf prägnante Weise.

Im Mittelpunkt des Datenschutzes im Jahr 2005 standen die folgenden Kernfragen:

- Wie kann der Kernbereich der privaten Lebensgestaltung vor dem Hintergrund immer weiter gehender Vorratsdatenspeicherungen noch geschützt werden?

- Welchen Stellenwert hat Datenschutz zukünftig im Bereich der Leistungsverwaltung, aufgezeigt am Beispiel des Arbeitslosengeldes II?

- Wie können moderne Technologien sicher und damit vertrauenswürdig ausgestaltet werden?

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu diesen drei zentralen Bereichen gleich in mehreren Entschließungen datenschutzrechtliche Positionen formuliert. An den Schwerpunkten wird sichtbar, dass alle drei Bereiche immer wieder zu datenschutzrechtlichen Forderungen herausgefordert haben und dies auch zukünftig tun werden. Am Beispiel der Einführung des Arbeitslosengeldes II zeigt sich an der Ausgestaltung, wie wenig datenschutzrechtliche Fragen bei allen Weiterentwicklungen berücksichtigt worden sind. Dies ist nicht anders in den anderen Schwerpunkten. Oftmals muss beim Datenschutz nachgebessert werden oder beim Einsatz moderner Technologien wird den datenschutzrechtlichen Fragen nicht die Bedeutung eingeräumt, die notwendig wäre, um das Vertrauen der Bürger für die neuen Technologien gewinnen zu können.

Wie immer haben sich die Datenschutzbeauftragten auf den Konferenzen mit zahlreichen weiteren wichtigen Themen befasst. Die Einführung der elektronischen Gesundheitsakte bleibt ein Datenschutzthema, ebenso wie datenschutzrechtliche Fragen der Strafverfolgung und hier der Einsatz von DNA-Analysen, der im Jahr 2005 vom Gesetzgeber ausgeweitet wurde. Ein wichtiges Thema war auch die Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006 in Deutschland. Ein EU-Vertragsverletzungsverfahren, das gegen die Bundesrepublik Deutschland eingeleitet wurde, hat die Konferenz der Datenschutzbeauf-

tragten dazu veranlasst, noch einmal die Gewährleistung einer vollständig unabhängigen Datenschutzkontrolle in Deutschland einzufordern. Wie auch die EU-Kommission, sehen die Datenschutzbeauftragten in den bei den Innenministerien oder Regierungspräsidien der Länder angesiedelten Referaten für die Aufsicht über den privaten Bereich keine vollständig unabhängige Aufsichtsform, wie die EU-Datenschutzrichtlinie sie fordert.

Auf europäischer Ebene ist die Arbeit der sog. Artikel-29-Gruppe der Europäischen Kommission ein fester Baustein des Datenschutzes geworden. Die Datenschutzbeauftragten der Mitgliedsstaaten hatten in der Artikel-29-Gruppe Themen zu beraten, die die Zukunft des Datenschutzes entscheidend beeinflussen werden. Ganz besondere Bedeutung nimmt hier die Stellungnahme zur Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, ein. Letztlich hat aber auch die Artikel-29-Gruppe eine Entscheidung für die Vorratsspeicherung nicht verhindern können.

Die vielen offenen datenschutzrechtlichen Fragen bei dem immer weiter verbreiteten Einsatz von RFID-Technik haben die Artikel-29-Gruppe veranlasst, hierzu ein Arbeitspapier zu erstellen, das Grundlage für die datenschutzrechtlichen Forderungen in den EU-Mitgliedsstaaten beim Einsatz dieser Technologie sein kann. Ebenfalls verabschiedet wurden Arbeitspapiere zum Datenschutz in Unternehmen, dem durch die Globalisierung der Wirtschaft immer mehr Bedeutung zukommt.

Die Europäische Konferenz der Datenschutzbeauftragten hat 2005 in Kraków (Polen) unter dem Vorsitz der polnischen Datenschutzbeauftragten getagt. Hervorzuheben ist hier die Stellungnahme zu Strafverfolgung und Informationsaustausch in der EU, an der die Bedeutung des Themas „Datenschutz bei Sicherheitsbehörden“ nochmals deutlich wird.

Auch die Entschließungen der 27. Internationalen Konferenz der Datenschutzbeauftragten, die im Herbst 2005 in Montreux in der Schweiz stattfand, zeigen, dass den Datenschutzthemen eine weltweite Bedeutung zukommt. Ein gutes Beispiel ist hier die Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten. Die Fragen der Datensicherheit beim Einsatz von Biometrie machen eben nicht an Grenzen einzelner Staaten halt und fordern daher zu einvernehmlichen weltweiten Standards auf. Auch die Frage eines universellen Rechts auf den Schutz personenbezogener Daten und der Privatsphäre hat durch den Welthandel eine neue Dimension erhalten. Die Nutzung des Internets bringt ständig Grenzüberschreitungen mit sich, sodass die datenschutzrechtlichen Fragen in Zukunft immer weniger auf ein einzelnes Land bezogen beurteilt werden und schon gar nicht gelöst werden können.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation ist im Frühjahr 2005 in Madeira (Portugal) und im Herbst in Berlin zu ihrer 37. und 38. Sitzung zusammen gekommen. Es entstanden Arbeitspapiere zum Datenschutz bei Online-Wahlen, zu Web Browser Caching sowie zu einer netzwerkbasierten Telemedizin.

Im Bereich der Informationsfreiheit hat die Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland (AGID) im Mai 2005 eine Entschließung „Jetzt nicht kneifen – das Informationsfreiheitsgesetz endlich verabschieden!“ gefasst. Das Informationsfreiheitsgesetz des Bundes wurde im Sommer 2005 tatsächlich verabschiedet und ist seit dem 1. Januar 2006 in Kraft. Es besteht die Hoffnung, dass sich dadurch auch einige Bundesländer ermutigt fühlen, nunmehr den Anschluss an die Informationsfreiheit zu wagen.

Da der Transparenzgedanke ein entscheidendes Merkmal der Informationsfreiheit als Bürgerrecht ist, hat die Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten auf ihrer Sitzung im Herbst in Düsseldorf zwei Entschließungen zur Transparenz, einmal in öffentlichen Unternehmen und einmal im Hinblick auf die Aktivitäten und Bezügen der Mitglieder öffentlicher Organe und Gremien verabschiedet. Mit einer Politik der kleinen Schritte soll dem Grundgedanken der Informationsfreiheit damit immer mehr Rechnung getragen werden.

Im Herbst 2005 wurde schließlich in Berlin die Europäische Konferenz der Informationsbeauftragten gegründet. Sie will sich verstärkt für Informationsfreiheit im europäischen Raum einsetzen und dabei auch für eine Harmonisierung der rechtlichen Grundlagen. Auch hier gilt: Das Informationsfreiheitsrecht macht nicht an einer Grenze halt.

Wir hoffen, dass die Zusammenstellung des Anlagenbandes auf ein breites Interesse stößt und vielleicht manch einen ermutigt, sich mit den Fragen des Datenschutzes und der Informationsfreiheit etwas mehr zu beschäftigen, denn wir alle sind von ihnen betroffen.

Dr. Alexander Dix
Berliner Beauftragter
für Datenschutz und Informationsfreiheit

Dagmar Hartge
Landesbeauftragte für Datenschutz
und Akteneinsicht Brandenburg

A Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 69. Konferenz vom 11./12. März 2005 in Kiel

Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Ein-

führungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

2. Entschließungen zwischen der 69. und 70. Konferenz

Einführung biometrischer Ausweisdokumente (1. Juni 2005)

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife,

der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,

- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,

- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck (15. Juli 2005)

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z.B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es

birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

3. Entschließungen der 70. Konferenz vom 27./28. Oktober 2005 in der Hansestadt Lübeck

Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z. B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeu-

tigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem

Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems

A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung –und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u.a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Telefonieren mit Internettechnologie (Voice over IP – VoIP)

Die Internettelefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,

- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,

- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,

- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,

- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und

- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären

Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend.. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein "Raum der Freiheit, der Sicherheit und des Rechts" werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

4. Entschließung zwischen der 70. und 71. Konferenz vom 15. Dezember 2005

Sicherheit bei eGovernment durch Nutzung des Standards OSCI

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheitsstandard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zu-

nächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

II. Europäische Konferenz der Datenschutzbeauftragten vom 26. - 27. April 2005 in Krakau (Polen)

Erklärung von Krakau

Verschiedene Initiativen auf EU-Ebene sind darauf gerichtet, den von der Europäischen Union angestrebten Raum der Freiheit, der Sicherheit und des Rechts zur verwirklichen. In ihrem neuen mehrjährigen Programm – dem Haager Programm – wiederholt die Union die Notwendigkeit, das organisierte grenzüberschreitende Verbrechen zu bekämpfen und der terroristischen Bedrohung Einhalt zu gebieten.

Die Frühjahrskonferenz 2005 der Europäischen Datenschutzbehörden ist sich der Notwendigkeit einer engeren Zusammenarbeit zwischen Strafverfolgungsbehörden sowohl innerhalb der EU als auch mit Drittstaaten sehr wohl bewusst. Gleichzeitig ist es offensichtlich, dass die Datenschutzkonvention des Europarats von 1981 (Konvention 108), anwendbar in der Union und in den Mitliedsaaten, zu allgemein gehalten ist, um den Datenschutz im Bereich der Strafverfolgung wirksam zu schützen. Ausgehend von der Verpflichtung der Union zur Achtung der Menschenrechte und Grundfreiheiten, sollten daher Initiativen zur Verbesserung der Strafverfolgung in der EU, wie zum Beispiel das Verfügbarkeitsprinzip, nur auf der Grundlage von Datenschutzregelungen eingeführt werden, die einen hohen und gleichwertigen Datenschutzstandard gewährleisten.

Die Konferenz stellte mit Befriedigung fest, dass das Haager Programm das Verfügbarkeitsprinzip strengen Bedingungen hinsichtlich der Achtung der Grundsätze des Datenschutzes unterstellt.

Die Konferenz begrüßt ebenfalls den Ansatz der Kommission, sich für einen Kernbestand von Leitprinzipien beim Umgang mit personenbezogenen Daten im Bereich der Dritten Säule einzusetzen, der in enger Zusammenarbeit mit den Datenschutzbehörden entwickelt werden soll. Außerdem ist die Konferenz durch Schritte ermutigt worden, welche die Kommission zur Entwicklung eines neuen rechtlichen Rahmen zum Datenschutz in der Dritten Säule unternommen hat, der hoffentlich zu einem angemessenen Bestand von Regelungen für Strafverfolgungen in Übereinstimmung mit dem gegenwärtigen Datenschutzniveau in der Ersten Säule führen wird. Bei der Entwicklung dieser detaillierten Datenschutzregelungen soll der Datenschutzstandard der Richtlinie 95/46/EG als Grundlage dienen.

Angesichts der Notwendigkeit einen harmonisierten Datenschutzansatz in der Union zu entwickeln, liegt es nahe, dass, sobald der Europäische Verfassungs-

vertrag in Kraft tritt, ein umfassendes Europäisches Datenschutzgesetz gelten sollte, das sämtliche Bereiche der Verarbeitung personenbezogener Daten abdeckt.

Das neue Rechtsinstrument würde die wichtigste Fortentwicklung des Datenschutzrechts seit der Annahme der Datenschutzrichtlinie 95/46/EG sein und große Auswirkungen auf die zukünftige Architektur des Datenschutzes in Europa haben. Um Unterschiede zwischen der Ersten und der Dritten Säule zu vermeiden, was einen negativen Einfluss auf Durchsetzung und Transparenz hätte, und im Hinblick auf die Grundrechtscharta und die kommende Europäische Verfassung, welche die Säulen abschaffen wird, ruft die Konferenz zur Wahrung – und, wo nötig, zur Wiederherstellung des Zusammenhangs, der Konsistenz und der Einheit des Datenschutzes auf. Die Grundsätze der Richtlinie 95/46 sollten den gemeinsamen Kernbereich eines umfassenden europäischen Datenschutzgesetzes bilden. Die darin enthaltenen Vorschriften über die Grundsätze der Zulässigkeit, die Rechte der Betroffenen und die Regeln der Durchsetzung sind hier besonders zu nennen. In Bezug auf ihre institutionellen Vorschriften ist die Notwendigkeit einer EU-Arbeitsgruppe hervorzuheben, die sich aus Vertretern der nationalen und der EU-Datenschutzaufsichtsbehörden zusammensetzt, die unabhängig arbeiten und die mit Aufgaben der Zusammenarbeit, der Kontrolle sowie mit Beratungsaufgaben zu betrauen sind.

Die Konferenz hat das beigefügte Positionspapier zur Strafverfolgung und zum Informationsaustausch in der EU angenommen. Dieses Papier richtet sich als konstruktiver Beitrag zu aktuellen Initiativen und insbesondere im Hinblick auf die Arbeit der Kommission an einem Datenschutzinstrument für die Dritte Säule vor allem an die EU-Institutionen. Selbstverständlich ist die Konferenz der EU-Datenschutzbehörden weiterhin gerne bereit, an der Schaffung eines praktikablen Rahmens mitzuwirken, der auch die Grundrechte achtet.

Stellungnahme zu Strafverfolgung und Informationsaustausch in der EU

Einführung

Die Frühjahrskonferenz der Europäischen Datenschutzbehörden hat die folgende Stellungnahme verabschiedet:

Entwurf eines Rahmenbeschlusses vom 4. Juni 2004 (10215/04) zur Vereinfachung des Informations- und Erkenntnisaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, insbesondere hinsichtlich schwerer Straftaten einschließlich terroristischer Handlungen.

Sachstand

Unter Bezugnahme auf die Erklärung des Europäischen Rates zur Bekämpfung des Terrorismus vom 25. März 2004, in der der Rat aufgefordert wird, den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten zu verbessern und zu vereinfachen, hat das Königreich Schweden einen Entwurf für einen Rahmenbeschluss mit dem Ziel vorbereitet, einen „gemeinsamen und vereinfachten Rahmen für den Austausch von Informationen und Erkenntnissen zwischen den zuständigen Strafverfolgungsbehörden der Mitgliedstaaten“[1] zu schaffen.

Der Rahmenbeschluss

Im Erläuterungsprotokoll wird festgestellt, dass bestehende Unterschiede in den einzelstaatlichen Rechtsvorschriften und Verwaltungsstrukturen der Mitgliedstaaten die größten Hindernisse für den Informations- und Erkenntnisaustausch innerhalb der EU darstellen und dass ein Rahmenbeschluss die beste Methode darstellt, diese Probleme anzugehen. Es folgt eine kurze Zusammenfassung der entsprechenden Bestimmungen des Entwurfs des Rahmenbeschlusses.

Der geplante Rahmenbeschluss würde von den Strafverfolgungsbehörden in den Mitgliedstaaten verlangen, den Strafverfolgungsbehörden in anderen Mitgliedstaaten auf Anfrage bestimmte Informationen und Erkenntnisse zur Verfügung zu stellen. Im Speziellen sollen durch den Beschluss Regelungen festgelegt werden, nach denen die Strafverfolgungsbehörden der Mitgliedstaaten … vorhandene Informationen und Erkenntnisse zur Durchführung strafrechtlicher Ermittlungen oder kriminalpolizeilicher Einsätze austauschen können (Artikel 1 Absatz 1).

[1] Übernommen von Seite 4 des Erläuterungsprotokolls

Diese Informationen müssten unverzüglich und vorzugsweise innerhalb des erbetenen Zeitrahmens (Artikel 4 Absatz 3) bereitgestellt werden, und die Strafverfolgungsbehörden dürften eine Informationsanfrage nur dann ablehnen, wenn sie sich auf eine der Ausnahmeregelungen berufen können, die ihnen im Beschluss eingeräumt werden (Artikel 11).

Alle Strafbestände, die mit einer Höchststrafe von 12 Monaten oder mehr geahndet werden, wären von dem Beschluss erfasst (Artikel 3). Der Rahmenbeschlussentwurf enthält darüber hinaus ein Verzeichnis der Straftaten, die als schwerer eingestuft werden, und bei denen es deshalb erforderlich wäre, dass Informationen binnen höchstens 12 Stunden nach einer Anfrage zur Verfügung gestellt werden (Artikel 4 Buchstabe a Absatz 2).

Daten können ausgetauscht werden über die Personen, die verdächtigt werden, eine in Artikel 3 (Artikel 6 Absatz 1 Buchstabe a) erfasste Straftat begangen zu haben, über die Personen, die nach kriminalpolizeilichen Erkenntnissen oder anderen beweiserheblichen Umständen eine derartige Straftat begehen könnten (Artikel 6 Absatz 1 Buchstabe b) oder über diejenigen Personen, die unter keine dieser Kategorien fallen, aber tatsächliche Gründe für die Annahme sprechen, dass ein Informations- und Erkenntnisaustausch zur Aufdeckung, Verhütung oder Ermittlung einer Straftat beitragen könnte, bei denen eine der unter Artikel 4 Absatz a des Beschlusses (Artikel 6 Absatz 1 Buchstabe c) genannte Straftat begangen wurde.

In Artikel 7 Absatz 1 ist geregelt, dass das SIRENE-Büro oder Europol oder „eine beliebige andere Vorkehrung auf bilateraler oder multilateraler Ebene unter den Mitgliedstaaten“ genutzt werden kann, um Informationen und Erkenntnisse nach diesem Beschluss auszutauschen.

Artikel 9 sieht vor, dass in dem Fall, dass vorhandene Kommunikationskanäle genutzt werden, die Datenschutzregelungen, die für diese Kanäle gelten – wie jene, die in der Europolkonvention enthalten sind – auch auf die Austauschvorgänge anzuwenden sind, die von diesem Beschluss erfasst werden.

Artikel 9 sieht vor, dass „gleichwertige Standards des Datenschutzes“ gelten sollten, wenn andere Kanäle genutzt werden.

Allgemeine Bemerkungen

Falls dieser Rahmenbeschluss umgesetzt wird, würde damit ein bewährter Standard in der EU-Politik in diesem Bereich fortgeführt. Die Zusammenarbeit zwischen den Strafverfolgungsbehörden wird als ein wichtiger, wenn nicht sogar entscheidender Aspekt in der Bekämpfung von Kriminalität und Terrorismus angesehen. Kulturelle, organisatorische und rechtliche Hindernisse, die einen

Datenaustausch verhindern, müssen angegangen werden. Viele Initiativen, einschließlich dieses Rahmenbeschlussentwurfs, führen zu einem deutlichen Anstieg des Austausches von Informationen für Strafverfolgungszwecke, wobei deutlich mehr personenbezogene Daten zwischen den Mitgliedstaaten ausgetauscht werden. Auch wenn der Datenaustausch an sich für die Bekämpfung von Kriminalität und Terrorismus notwendig sein mag, ist die Liste der von dem Beschluss erfassten Straftaten groß und geht weit über den relativ engen Katalog von Straftaten hinaus, wie sie in anderen EU-Instrumenten erfasst werden, wie z. B. in der Europol-Konvention. Auch die Kategorie von Personen, über die Daten ausgetauscht werden können, ist weit gefasst; insbesondere Artikel 6 Buchstabe c ist unklar und könnte zu einem weitgehenden Datenaustausch von Personen führen, die überhaupt nicht verdächtigt werden, Straftaten begangen zu haben. Es sollte klare Kriterien für die Festlegung geben, wann personenbezogene Daten ausgetauscht werden können.

Der Entwurf des Rahmenbeschlusses führt eine Verpflichtung zum Austausch von Informationen ein, wenn diese verfügbar sind. Angesichts der potentiell weit reichenden Auswirkungen dieser Entwicklung möchten wir hervorheben, wie wichtig eine Prüfung der Verhältnismäßigkeit dieses Vorschlags ist. Die Bekämpfung des Terrorismus wird immer mehr als Begründung für neue Initiativen in diesem Bereich herangezogen, viele davon gehen aber weit über diesen Zweck hinaus. Es ist daher wichtig zu erkennen, dass eine Einschränkung von Grundrechten, die für die Bekämpfung des Terrorismus gerechtfertigt sein kann, nicht notwendigerweise gerechtfertigt ist, wenn es um andere kriminelle Aktivitäten geht.

Durch die Einführung des Grundsatzes, dass Daten bei Verfügbarkeit ausgetauscht werden müssen, wird eine Verbindung zum Haager Programm[2] [2] hergestellt, in dem das Verfügbarkeitsprinzip eingeführt wird. Das Haager Programm legt strikte Bedingungen fest, die einzuhalten sind, wenn das Verfügbarkeitsprinzip angewendet werden soll, wie z. B. das Erfordernis, die Informationsquellen und die Vertraulichkeit der Daten zu schützen, das Erfordernis, die Integrität der auszutauschenden Daten zu gewährleisten, die Aufsicht darüber, dass der Datenschutz beachtet wird, sowie geeignete Kontrollen vor und nach dem Austausch der Daten. Der Rahmenbeschlussentwurf entspricht jedoch nicht diesen strikten Bedingungen, sodass es daher notwendig ist, diese Bedingungen im Beschluss zu entwickeln.

Nach dem Beschlussentwurf sollen bestehende Kommunikationskanäle für den Datenaustausch genutzt werden, und es sollen bestehende Datenschutzregelungen Anwendung finden. So einfach ist dies aber nicht. Es gibt Unterschiede zwi-

[2] Schlussfolgerungen der Präsidentschaft 4/5. November 2004 (14292/04) Anhang 4: Das Haager Programm

schen Datenschutzregelungen, die gemäß Schengen Anwendung finden, und jenen, die z. B. für Europol gelten. Darüber hinaus wurden die Regelungen europaweit noch nicht harmonisiert. Die Regelungen, die für das SIRENE-Büro gelten, sind in den einzelstaatlichen Rechtsvorschriften jedes Mitgliedstaates enthalten; sie sind nicht harmonisiert worden. Dies kann zu Diskrepanzen führen, und es kann durchaus eine Situation entstehen, in der Daten in einem empfangenden Mitgliedstaat längere Zeit aufbewahrt werden, als sie in dem die Daten bereitstellenden Mitgliedstaat aufbewahrt worden wären. Um diese Komplikationen zu vermeiden und im Interesse der Klarheit sollten die Datenschutzregelungen, die für den Datenschutz gemäß diesem Beschluss gelten, im Text des Beschlusses selbst auch enthalten sein. So wie diese Regelungen Fragen der Aufbewahrung, der Datenqualität, Sicherheit und Kontrolle behandeln sollten, sollten diese auch deutlich machen, wer für die weitere Verarbeitung der gemäß diesem Beschluss ausgetauschten Daten verantwortlich ist. Ein besonderes Paket von Datenschutzregeln ist in der Stellungnahme zur Strafverfolgung und zum Informationsaustausch in der EU enthalten, der von der Konferenz in Krakau verabschiedet wurde.

Schlussfolgerung

Um alle erforderlichen Sicherheitsvorkehrungen zu bieten, die für ein angemessenes Niveau im Datenschutz in Einklang mit dem bestehenden rechtlichen Rahmen sorgen, empfiehlt die Konferenz, dass der Rahmenbeschluss unter Berücksichtigung der in dieser Stellungnahme enthaltenen Bemerkungen geändert werden sollte.

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

ARTIKEL-29-DATENSCHUTZGRUPPE

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

Die Sekretariatsgeschäfte werden wahrgenommen von:

Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft).

Website: www.europa.eu.int/comm/privacy

Stellungnahme zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg. vom 21.9.2005) (WP 113)

Angenommen am 21. Oktober 2005

ZUSAMMENFASSUNG

Der Vorschlag der Europäischen Kommission für eine Richtlinie über die Vorratsspeicherung von Daten stellt uns vor eine historische Entscheidung.

Die Aufbewahrung von Verkehrsdaten ist ein Eingriff in das unverletzliche Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses.

Eingriffe in dieses Grundrecht müssen einem zwingenden Bedarf entspringen, sie sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein.

Die Anbieter öffentlich zugänglicher Kommunikationsdienste wären erstmals gezwungen, Milliarden von Daten über die Kommunikationsvorgänge aller Bürger zu Ermittlungszwecken zu speichern.

Der Terrorismus stellt unsere Gesellschaft vor eine reale und drängende Herausforderung. Die Regierungen müssen auf diese Herausforderung in einer Form reagieren, die dem Bedürfnis der Bürger, in Frieden und Sicherheit zu leben, wirkungsvoll nachkommt, ohne die Menschenrechte des Einzelnen, darunter das Recht auf Privatsphäre und Datenschutz, auszuhöhlen, denn diese Rechte gehören zu den Eckpfeilern unserer demokratischen Gesellschaft.

Die Initiative der Europäischen Kommission könnte im Endergebnis zur Festlegung von maximalen Aufbewahrungsfristen führen, die kürzer sind als diejenigen, die in anderen Vorschlägen der letzten Zeit vorgesehen sind.

Nach Auffassung der Datenschutzgruppe ist es fraglich, ob sich die von den zuständigen Behörden in den Mitgliedstaaten vorgebrachten Rechtfertigungsgründe für eine obligatorische und allgemeine Vorratsdatenspeicherung auf kristallklare Beweise stützen. Die Datenschutzgruppe hegt auch Zweifel, ob die im Richtlinienentwurf vorgeschlagenen Aufbewahrungsfristen überzeugen können.

Wie oben erwähnt muss klar aufgezeigt und nachgewiesen werden, dass eine obligatorische und allgemeine Vorratsdatenspeicherung gerechtfertigt ist. Gleiches gilt für die maximal zulässige Aufbewahrungsdauer. In jedem Fall müssen auch die Bedingungen, unter denen den zuständigen Behörden zur Bekämpfung der terroristischen Bedrohung der Zugriff auf die Daten und deren Nutzung zu gestatten ist, eindeutig benannt werden.

Die Zwecke, zu denen die Daten gespeichert werden, müssen in der Richtlinie klar umrissen werden; dabei sollte auf die Bekämpfung des Terrorismus und der organisierten Kriminalität Bezug genommen werden statt auf nicht näher bestimmte „schwere Straftaten“.

Der Existenz von Vorgehensweisen, die weniger in die Privatsphäre eingreifen (z. B. „quick freeze“-Verfahren) ist Rechnung zu tragen.

Der Zeitraum, über den die Daten gespeichert werden müssen, sollte so kurz wie möglich sein und die für alle Mitgliedstaaten geltende Höchstgrenze darstellen; dabei sollte es den Mitgliedstaaten freistehen, kürzere Aufbewahrungsfristen festzulegen. Die möglicherweise eingeführten Maßnahmen müssen umfassend bekannt gemacht werden.

Die Beweise, auf die sich diese Maßnahmen stützen, müssen regelmäßig bewertet werden. Die beabsichtigten Maßnahmen zur Vorratsdatenspeicherung sollten

einer zeitlichen Befristung auf Grundlage einer periodischen Bewertung unterliegen, die mindestens alle 2-3 Jahre durchzuführen und zu veröffentlichen wäre (Konzept der „sunset legislation"). Die Datenschutzgruppe hält eine Dreijahresfrist für angemessen.

In jedem Fall ist es im bestehenden europäischen Rechtsrahmen inakzeptabel, den Kommunikationsdiensteanbietern die betreffenden Aufbewahrungspflichten aufzuerlegen, ohne vorab angemessene und spezifische Schutzvorkehrungen zu treffen.

Zum Abschluss schlägt die Datenschutzgruppe zwanzig spezifische Schutzvorkehrungen vor, unter besonderer Berücksichtigung der Anforderungen an Empfänger und Weiterverarbeitung, der Notwendigkeit von Autorisierungen und Kontrollen, der von Diensteanbietern zu ergreifenden Maßnahmen im Hinblick auf die Sicherheit und die logische Trennung der Daten, der Festlegung der betroffenen Datenkategorien und ihrer Aktualisierung und der Notwendigkeit, Inhaltsdaten von der Speicherung auszunehmen.

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

hat folgende Stellungnahme angenommen:

I. Hintergrund

Im Rahmen der europäischen Initiativen zur Bekämpfung des Terrorismus und der organisierten Kriminalität unterbreitete die Europäische Kommission am 21. September dieses Jahres einen *„Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG"*[1].

Der Gegenstand dieses Vorschlags ist für alle Bürger von erheblicher Bedeutung.

Die Freiheit und die Vertraulichkeit des Briefverkehrs und sonstiger Kommunikationsformen gehören zu den Säulen einer modernen demokratischen Gesellschaft. Ihre Unverletzlichkeit ist in verschiedenen Rechtsinstrumenten, z. T. mit Verfassungsrang, verankert und steht unter dem besonderen Schutz der Europäi-

[1] KOM (2005) 438 endg. vom 21.9.2005 (noch nicht im Amtsblatt veröffentlicht).

schen Menschenrechtskonvention, die eine der Grundlagen des Gemeinschaftsrechts bildet.

Der Richtlinienentwurf stellt uns vor eine historische Entscheidung. Mit der vorgeschlagenen Richtlinie soll erstmals europaweit die Pflicht eingeführt werden, Milliarden von Daten über die Kommunikationsvorgänge aller Bürger zu Ermittlungszwecken zu speichern. Nach geltendem Gemeinschaftsrecht werden derartige Daten von den Anbietern elektronischer Kommunikationsdienste entweder gar nicht gespeichert oder nur für einen begrenzten Zeitraum und ausschließlich zu Vertragszwecken.

Die Vorratsspeicherung von Verkehrsdaten ist ein Eingriff in das Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses, das dem Einzelnen durch Artikel 8 der Europäischen Menschenrechtskonvention garantiert wird. In einer demokratischen Gesellschaft können Eingriffe in dieses Grundrecht gerechtfertigt sein, wenn sie für die nationale Sicherheit notwendig sind. Sie können letzten Endes dazu führen, dass sämtliche Kontakte und Beziehungen von Personen verfolgt und aufgezeichnet werden, einschließlich der Orte, an denen sie stattfinden, und der verwendeten Kommunikationsmittel. Der Europäische Gerichtshof für Menschenrechte hat betont, dass bei heimlicher Überwachung die Gefahr besteht, dass die Demokratie mit der Begründung, sie verteidigen zu wollen, unterminiert oder zerstört wird. Er hat darüber hinaus bekräftigt, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten.[2]

Aus diesem Grund müssen Eingriffe in dieses Grundrecht einem zwingenden Bedarf entspringen und sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein. Die Vorratsspeicherung von Verkehrsdaten (einschließlich Standortdaten) zu Strafverfolgungszwecken muss strengen Auflagen genügen[3]; sie darf insbesondere nur während eines begrenzten Zeitraums erfolgen und nur dann, wenn dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Die Befugnisse der Strafverfolgungsbehörden müssen zwar eine wirksame Bekämpfung des Terrorismus ermöglich, aber sie dürfen weder unbegrenzt sein noch missbraucht werden. Es ist auf Verhältnismäßigkeit und Ausgewogenheit zu achten, um sicherzustellen, dass wir die Gesellschaft, die wir schützen wollen, nicht untergraben. Dies gilt insbesondere dann, wenn Kommunikationsdiensteanbieter zur Speicherung von Daten gezwungen werden, die sie selbst nicht benötigen, denn damit wäre letzten Endes eine beispiellose, fortgesetzte und alles durchdringende Überwachung jeder Art von Kommunikation und Be-

[2] Klass und andere gegen Deutschland, Absatz 49.

[3] Siehe insbesondere Artikel 15 Absatz 1 der Richtlinie 2002/58/EG.

wegung sämtlicher Bürger im Alltag möglich. Es würde eine riesige Menge an Informationen gespeichert, die tatsächlich nur in einer begrenzten Zahl von Fällen für Ermittlungszwecke von Nutzen sind.

Zu berücksichtigen ist ferner, dass von einer derart umfassenden Speicherpflicht auch Kommunikationsvorgänge betroffen sind, die heikle Fragen in Bezug auf das Berufs- und/oder Untersuchungsgeheimnis oder bestimmte Tätigkeiten unter besonderem rechtlichem Schutz stehender Institutionen aufwerfen.

Aus diesem Grund vertreten sowohl die Datenschutzgruppe als auch die Konferenz der Europäischen Datenschutzbeauftragten seit Jahren einen festen und klaren Standpunkt. Die Datenschutzgruppe[4] und die Europäische Konferenz[5] haben seit 1997 wiederholt die Notwendigkeit einer allgemeinen Vorratsspeicherung von Daten in Frage gestellt.

---

[4] Siehe
- Stellungnahme 9/2004 zum Entwurf eines Rahmenbeschlusses […] (Ratsdokument 8958/04 vom 28.4.2004). Der Anhang dieser Stellungnahme enthält eine Zusammenfassung der folgenden Dokumente:
- Stellungnahme 1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung;
- 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;
- Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus;
- Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität;
- 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;
- Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke;
- Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs;
- Empfehlung 3/97 über Anonymität im Internet.

(Sämtliche genannten Dokumente sind abrufbar unter http://europa.eu.int/comm/internal_market/privacy.)

[5] Siehe die in Stockholm (April 2000) und Cardiff (April 2002) angenommenen Erklärungen.

II. Vorläufige Bewertung und allgemeine Voraussetzungen

1. Gespeicherte Daten können für Ermittler von Nutzen sein, aber die oben genannten Voraussetzungen müssen deutlich aufgezeigt und belegt sein.

Erstens muss das Ziel einer derartigen Maßnahme unmissverständlich zum Ausdruck gebracht werden. Zweitens muss klar aufgezeigt und nachgewiesen werden, dass eine obligatorische und allgemeine Vorratsdatenspeicherung gerechtfertigt ist. Gleiches gilt für die maximal zulässige Aufbewahrungsdauer. Drittens müssen die Bedingungen, unter denen den zuständigen Behörden zur Bekämpfung der terroristischen Bedrohung der Zugriff auf die Daten und deren Nutzung zu gestatten ist, eindeutig benannt werden.

Die Beweise müssen zumindest regelmäßig bewertet und die Bewertungsergebnisse veröffentlicht werden; dabei ist zu berücksichtigen, dass der Terrorismus und das organisierte Verbrechen auf die Einführung von Maßnahmen zur generellen Überwachung der Bürger mit Strategien zur Vermeidung bestimmter Kommunikationsmittel reagieren könnten. Dies hätte zur Folge, dass neue Methoden einer noch strengeren Überwachung entwickelt werden müssten und somit eine Spirale möglicher Eingriffe in die Grundrechte der Bürger in Gang gesetzt würde, die nur schwer aufzuhalten wäre. Darüber hinaus würde eine solche Entwicklung das Wesen der Gesellschaft verändern, die wir zu bewahren trachten.

Die Datenschutzgruppe erkennt an, dass sich einige Bedingungen in unseren Gesellschaften hinsichtlich der mit der terroristischen Bedrohung verbundenen Risiken verändert haben, und nimmt zur Kenntnis, dass manche Daten gelegentlich für bestimmte Ermittlungen nützlich sind und zu Recht verwendet werden. Des Weiteren stellt die Datenschutzgruppe fest, dass die Initiative der Europäischen Kommission im Endergebnis zur Festlegung von maximalen Aufbewahrungsfristen führen könnte, die kürzer sind als diejenigen, die in der Vergangenheit vorgesehen waren und zu denen sich die Datenschutzgruppe ablehnend geäußert hat – zuletzt in ihrer am 9. November 2004 angenommenen Stellungnahme 9/2004 (WP 99).

Gleichwohl hat es nicht den Anschein, dass sich die Begründungen für die Datenspeicherung, obwohl sie sich angeblich an den Anforderungen seitens der zuständigen Behörden in den Mitgliedstaaten orientieren, auf kristallklare Beweise stützen können. Demzufolge erscheinen die vorgeschlagenen Fristen bislang nicht überzeugend.

Es gibt andere nützliche Maßnahmen, die für Ermittlungszwecke in Betracht gezogen werden können und die in geringerem Maße in die Grundrechte der Bürger eingreifen, beispielsweise das „quick freeze"-Verfahren, das weder die

Kommunikationsanbieter noch die Internet-Diensteanbieter zur generellen Speicherung von Verkehrsdaten verpflichten würde. Bei diesem Verfahren wenden sich die Strafverfolgungsbehörden in begründeten Fällen an die Unternehmen und verlangen die Speicherung bestimmter Daten. Anschließend haben die Behörden mehrere Wochen Zeit zum Sammeln von Beweismitteln, um eine richterliche Anordnung zu erwirken. Gestützt auf diese Anordnung erhalten sie dann Zugriff auf die Daten.

In jedem Fall muss eine allgemeine Aufbewahrungsfrist klar geregelt werden. Sie sollte möglichst kurz sein und weitest gehend mit der Aufbewahrungsfrist übereinstimmen, die für die ursprünglichen Zwecke gilt, zu denen die Daten von den Kommunikationsdiensteanbietern aufgezeichnet werden.

2. Die von der Kommission derzeit vorgeschlagene Harmonisierung der Rechtsvorschriften in den Mitgliedstaaten muss klarstellen, dass die Festlegung einer verbindlichen Speicherfrist auf europäischer Ebene auf Grundlage einer auf europäischer Ebene durchgeführten Bewertung der Verhältnismäßigkeit erfolgt, die auch dem grenzüberschreitenden Charakter des organisierten Verbrechens sowie den Erfordernissen eines Höchstmaßes an Sicherheit in allen Mitgliedstaaten Rechnung trägt.

Des Weiteren muss klargestellt werden, dass die in der Richtlinie genannte Aufbewahrungsfrist als für alle Mitgliedstaaten geltende einheitliche Höchstgrenze zu betrachten ist.

Das heißt, es muss deutlich zum Ausdruck kommen, dass die Mitgliedstaaten keine längeren Speicherfristen als in der Richtlinie vorgesehen festlegen dürfen, während es ihnen freisteht, kürzere Zeiträume vorzuschreiben. Außerdem ist darauf hinzuweisen, dass die Daten nach Ablauf der genannten Fristen gelöscht werden müssen. Vor diesem Hintergrund ist der derzeitige Wortlaut des Artikels 11 des Richtlinienentwurfs als nicht zufriedenstellend anzusehen.

Die Datenschutzgruppe begrüßt, dass der Vorschlag in Artikel 12 eine mindestens alle zwei Jahre durchzuführende regelmäßige Bewertung vorsieht.

Diese Bewertung sollte sich auch auf die Notwendigkeit der von den Strafverfolgungsbehörden in spezifischen und genau umrissenen Fällen verwendeten Verkehrsdaten beziehen und unter Mitwirkung der Datenschutzbehörden erfolgen. Das Ergebnis der Bewertungen ist zu veröffentlichen.

Dabei ist jedoch darauf hinzuweisen, dass sich die Bewertung nicht auf einen unbegrenzten Zeitraum beziehen sollte, da der Vorschlag auf der konkreten Beurteilung der in ihm genannten Annahmen und Voraussetzungen basiert. Daher müssen die beabsichtigten Maßnahmen zur Vorratsdatenspeicherung gemäß

dem Konzept der Befristung von Rechtsvorschriften („sunset legislation“) zeitlich befristet werden. Die Datenschutzgruppe hält eine Dreijahresfrist für angemessen. Nach Ablauf dieses Zeitraums müssen die innerstaatlichen Maßnahmen, mit denen die Speicherung von Daten in Umsetzung der Richtlinie vorgeschrieben wird, ihre Rechtskraft verlieren, unbeschadet der Möglichkeit, die Analyse, die im Vorfeld einer neuerlichen Entscheidung des Rates und des Europäischen Parlaments zur Billigung einer neuen Richtlinie erforderlich ist, auch vor Ablauf der drei Jahre einzuleiten.

Im Hinblick auf den Grundsatz der Verhältnismäßigkeit begrüßt die Datenschutzgruppe, dass die Datenmenge, die zur Internetnutzung vorgehalten werden soll, beschränkt wird. Darüber hinaus ist die Festlegung einer Höchstmenge zu speichernder Daten einer Minimalliste vorzuziehen. Generell sind die zu speichernden Daten auf diejenigen zu beschränken, die von den Anbietern zu technischen Zwecken und zur Gebührenabrechnung gesammelt werden.

Wesentlich sind Festlegungen bezüglich des Zugangs zu den Daten und der Verwendungszwecke; es ist sicherzustellen, dass Maßnahmen zur generellen Vorratsdatenspeicherung von strengsten Schutzmaßnahmen begleitet sind und einer Prüfung unterzogen werden.

3. Die Schutzvorkehrungen, die der geltende Rechtsrahmen für den Datenschutz innerhalb der ersten Säule (Richtlinien 95/46/EG und 2002/58/EG) bietet, müssen für die mit der Vorratsdatenspeicherung verknüpften Strafverfolgungszwecke näher spezifiziert werden. Solche spezifischen Schutzvorkehrungen sind von entscheidender Bedeutung, um sicherzustellen, dass der Schutz, den Richtlinie 2002/58/EG insbesondere für das Recht auf Vertraulichkeit bei der Verwendung öffentlich zugänglicher elektronischer Kommunikationsdienste bietet, nicht in wesentlichen Punkten ausgehöhlt wird.

Darüber hinaus bedarf es nach Ansicht der Datenschutzgruppe eines angemessenen Schutzes in Bezug auf die Datenverarbeitung in Bereichen, die gegenwärtig nicht in den Geltungsbereich dieser Richtlinien fallen.

Aus diesem Grund vertritt die Datenschutzgruppe u. a. die Auffassung, dass der Richtlinienentwurf selbst entsprechende Schutzmaßnahmen vorsehen sollte oder aber zusammen mit anderen geeigneten Rechtsinstrumenten bewertet und verabschiedet werden sollte. Die Datenschutzgruppe ist insbesondere der Meinung, dass in diesem Zusammenhang auch der „Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“ einer sorgfältigen Bewertung zu unterziehen ist.

Abschließend ist die Datenschutzgruppe angesichts der Auswirkungen auf die Grundrechte und -freiheiten der betroffenen Bürger der Überzeugung, dass die möglicherweise einzuführenden Maßnahmen umfassend bekannt gemacht werden müssen.

III. Sonstige spezifische Schutzvorkehrungen

Im Übrigen müssen nach Auffassung der Datenschutzgruppe die folgenden Aspekte zumindest in Angriff genommen werden:

1. ZWECKE

Die Daten dürfen nur zu spezifischen Zwecken der Bekämpfung des Terrorismus und der organisierten Kriminalität gespeichert werden, statt auf andere, nicht näher bestimmte „schwere Straftaten" Bezug zu nehmen. Diese beschränkte Zweckbestimmung sollte auch im Titel der vorgeschlagenen Richtlinie zum Ausdruck kommen.

2. EMPFÄNGER

Die Richtlinie sollte vorsehen, dass die Daten nur eigens benannten Strafverfolgungsbehörden verfügbar gemacht werden und nur insoweit, als dies zur Ermittlung, Feststellung, Verfolgung und/oder Verhütung von Terrorakten notwendig ist. Ein Verzeichnis der eigens benannten Strafverfolgungsbehörden sollte öffentlich zugänglich sein.

3. DATA MINING

Die Terrorismusprävention darf nicht mit flächendeckendem Data Mining auf Grundlage der in der Richtlinie genannten Informationen über das Reise- und Kommunikationsverhalten von Personen einhergehen, die von den Strafverfolgungsbehörden nicht zum Kreis der Verdächtigen gezählt werden. Der Zugang muss auf diejenigen Daten beschränkt werden, die im Rahmen spezifischer Ermittlungen benötigt werden.

4. WEITERVERARBEITUNG

Jedwede Weiterverarbeitung vorgehaltener Daten durch die Strafverfolgungsbehörden für andere verwandte Verfahren muss verboten oder gestützt auf spezifische Schutzvorkehrungen streng begrenzt werden; jeder Zugriff anderer staatlicher Behörden auf die Daten muss unterbunden werden. Die in früheren europäischen Rechtsinstrumenten festgelegten Vorschriften für den Bereich der elekt-

ronischen Kommunikation dürfen nicht in einer Art und Weise angewandt werden, die mit diesem Grundsatz unvereinbar ist.

5. ZUGRIFFSPROTOKOLLE

Jeder Abruf der Daten ist zu protokollieren. Die Aufzeichnungen dürfen nur auf Anforderung und nur der Behörde und/oder dem unter Punkt 6 genannten Organ sowie den Datenschutzbehörden zu Kontrollzwecken zur Verfügung gestellt werden und müssen ein Jahr nach Erstellung gelöscht werden.

6. RICHTERLICHE/UNABHÄNGIGE PRÜFUNG

Der Zugang zu den Daten muss grundsätzlich im Einzelfall von einer Justizbehörde ordnungsgemäß genehmigt werden, unbeschadet der Tatsache, dass der Zugriff in manchen Ländern für bestimmte Fälle unter unabhängiger Aufsicht rechtlich zulässig ist. Wo dies angebracht ist, sollten die Genehmigungen die in den betreffenden Fällen benötigten Daten aufführen.

7. ADRESSATEN

Die Richtlinie muss eindeutig festlegen, für welche Anbieter öffentlich zugänglicher Kommunikationsdienste die Pflichten gelten. In Bezug auf das Internet ist eine Beschränkung auf Zugangsanbieter und auf Individualkommunikation (E-Mail-Dienste, Internettelefonie) erforderlich.

8. IDENTIFIZIERUNG

Ferner muss in dieser Richtlinie auch klargestellt werden, dass keine Identifikationspflicht in den Fällen besteht, in denen eine Identifizierung weder zur Gebührenabrechnung noch zu anderen Vertragszwecken erforderlich ist.

9. ZWECKE DER ÖFFENTLICHEN ORDNUNG

Den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern öffentlich zugänglicher elektronischer Kommunikationsnetze darf nicht gestattet werden, allein zu Zwecken der öffentlichen Ordnung gespeicherte Daten zu ihren eigenen Zwecken zu verarbeiten.

10. GETRENNTE SYSTEME

Insbesondere müssen die für die Datenspeicherung zu Zwecken der öffentlichen Ordnung verwendeten Systeme von den Systemen, die für die geschäftlichen Zwecke der Anbieter verwendet werden, logisch getrennt und durch strengere Sicherheitsvorkehrungen geschützt werden (z. B. durch Verschlüsselung), um einen unautorisierten Zugang und eine Nutzung durch Unbefugte zu verhindern.

11. SICHERHEITSMAßNAHMEN

Die Gemeinschaftsmaßnahmen müssen Mindeststandards für die von den Anbietern zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen vorschreiben; dabei ist auf die in Richtlinie 2002/58/EG aufgestellten allgemeinen Anforderungen an Sicherheitsmaßnahmen Bezug zu nehmen.

12. DRITTE

Die Gemeinschaftsmaßnahmen müssen festlegen, dass der Zugang Dritter zu den gespeicherten Daten rechtswidrig ist.

13. DEFINITIONEN

Die Datenkategorien müssen klar definiert werden; außerdem muss eine Beschränkung auf Verkehrsdaten erfolgen.

14. AUFLISTUNG DER DATEN UND REVISIONSMECHANISMEN

Die zu speichernden personenbezogenen Daten müssen in der Richtlinie selbst konkret aufgelistet werden. Dies ist für eine genaue Beurteilung der Auswirkungen auf die Grundrechte und -freiheiten der betroffenen Bürger wichtig; dabei sind die Gefahren für ihre Privatsphäre ebenso zu berücksichtigen wie Fragen, die mit der Gewährleistung der Genauigkeit und Korrektheit der vorgehaltenen Daten verbunden sind. Vorschläge zur Änderung des Verzeichnisses der zu speichernden Daten müssen stets einer strengen Prüfung der Notwendigkeit unterzogen werden. Angesichts der Auswirkungen dieser Maßnahmen auf die Grundrechte und -freiheiten sollte die Überarbeitung des besagten Verzeichnisses nur mit Billigung des Europäischen Parlaments und unter Einbeziehung der Datenschutzbehörden erfolgen. Auch die Beteiligung von Vertretern der Verbraucher- und Nutzerverbände, anderer relevanter Nichtregierungsorganisationen und der europäischen Verbände der Kommunikationsindustrie sollte in Betracht gezogen werden. In dieser Hinsicht erscheint es nicht als angemessen, die Überarbeitung des Verzeichnisses wie in der Richtlinie vorgesehen lediglich im Ausschussverfahren durchzuführen.

15. KEINE SPEICHERUNG VON INHALTSDATEN

Da der Kommunikationsinhalt vom Geltungsbereich des Vorschlags ausgenommen sein soll, müssen spezifische Schutzvorkehrungen eingeführt werden, um eine scharfe und wirksame Trennung zwischen Inhalts- und Verkehrsdaten sicherzustellen, sowohl für den Bereich des Internets (d. h. Beschränkung auf Anmelde- und Abmeldedaten oder sonstige Informationen wie Mailserver- und

Web-Cache-Protokolle und Aufzeichnungen des IP-Verkehrs) als auch für den Bereich der Telefonie (Konferenzschaltungen, Fax, SMS, Sprachtelefonie).

16. NICHT ZUSTANDE GEKOMMENE KOMMUNIKATION

Die verschiedenen Kategorien von Verkehrsdaten zu nicht zustande gekommenen Kommunikationen sollten ohne gründliche Bewertung der Angemessenheit im Lichte der oben genannten Grundsätze nicht einbezogen werden.

17. STANDORTDATEN

Die Speicherung von Standortdaten sollte nicht über die Funkzellen-Identifikationsnummer (Cell-ID) zu Beginn eines Kommunikationsvorgangs hinausgehen.

18. WIRKSAME AUFSICHT

Die ursprüngliche Nutzung und jede weitere mit ihr zu vereinbarende Verwendung (einschließlich Vervielfältigung) müssen wirksamen Kontrollen unterliegen, und zwar im Rahmen und zu Zwecken eines Strafverfahrens durch die Justizbehörden sowie in Bezug auf Datenschutzaspekte unabhängig von der Existenz eines Gerichtsverfahrens durch die Datenschutzbehörden.

19. VERÖFFENTLICHUNG

Die Richtlinie sollte die Pflicht zur angemessenen Information aller Bürger über jedwede Verarbeitungsoperationen enthalten, die möglicherweise nach Umsetzung der in ihr vorgesehenen Maßnahmen durchgeführt werden.

20. KOSTEN

Die Datenschutzgruppe stellt fest, dass die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber öffentlich zugänglicher elektronischer Kommunikationsnetze für zusätzliche Kosten von den Mitgliedstaaten entschädigt werden müssen. Die Datenschutzgruppe möchte die Bedeutung dieses Aspekts ausschließlich in Bezug auf direkt mit dem Datenschutz in Verbindung stehende Merkmale betonen. Maßnahmen zur Vorratsdatenspeicherung sollten verbunden sein mit der Erstattung von Investitionen in die Anpassung der Kommunikationssysteme, von Auslagen für die Übermittlung der Daten an die Strafverfolgungsbehörden und für Sicherheitsvorkehrungen. Hier ist eine umfassende Betrachtung erforderlich, um negative Folgen zu vermeiden, sowohl in Bezug auf den Datenschutz als auch in wirtschaftlicher Hinsicht für die Bürger, denen unter Umständen einige der den Anbietern/Betreibern entstehenden Kosten in Rechnung gestellt werden. In diesem Zusammenhang könnte

auch in Erwägung gezogen werden, den Anspruch der Anbieter/Betreiber auf Kostenerstattung von der Einhaltung der Mindeststandards abhängig zu machen und im Einzelfall zu prüfen.

Die Datenschutzgruppe ist zuversichtlich, dass die in dieser Stellungnahme enthaltenen Überlegungen angemessene Berücksichtigung finden werden, und weist darauf hin, dass alle oben genannten Schutzmaßnahmen getroffen werden sollten, ehe die Vorratsspeicherpflicht in die Praxis umgesetzt wird.

Brüssel, den 21. Oktober 2005

Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar

Arbeitsdokument „Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen" (WP 108)

Angenommen am 14. April 2005

Die Beteiligung der Datenschutzbehörden an der Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen erfolgt auf rein freiwilliger Basis[1]. Über die Beteiligung kann von Fall zu Fall entschieden werden. Die Datenschutzbehörden sind nicht verpflichtet, sich an Verfahren zur Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen zu beteiligen. Die Beteiligung von Behörden, die nicht befugt sind, den Transfer von Daten in Drittländer zu genehmigen, erfolgt vorzugsweise im Auftrag der für die Erteilung von Genehmigungen für die Übermittlung von Daten in Drittländer zuständigen einzelstaatlichen Behörde.

Die im vorliegenden Dokument ausgeführten Aspekte sind zweifellos sehr wichtig, aber nicht unumstößlich und können von der Artikel-29-Datenschutzgruppe zu einem späteren Zeitpunkt im Lichte neuerer Erkenntnisse überarbeitet wer-

[1] Unter Datenschutzbehörden sind die Datenschutzbehörden der EU-Mitgliedstaaten und der EWR-Länder zu verstehen.

den. Die Unternehmen werden aufgefordert, diese vorliegende Checkliste für die Vorlage von verbindlichen unternehmensinternen Datenschutzregelungen zur Prüfung durch die nationalen Datenschutzbehörden zu verwenden. Darüber hinaus ist von den Unternehmen zu bedenken, dass ihre Vorschläge ggf. der Ergänzung bedürfen, um die Vorgaben des jeweiligen einzelstaatlichen Rechtssystems einzuhalten – insbesondere hinsichtlich der Garantien, die vorgeschlagen werden, um sicherzustellen, dass betroffene Personen ihre Rechte im Rahmen der verbindlichen unternehmensinternen Regelungen wahrnehmen können.

Die Punkte, die in der Checkliste fehlen, werden von den genannten Behörden im Rahmen der üblichen Anhörungen im Zuge des Kooperationsverfahrens erörtert und behandelt. Es wurde versucht, in die Checkliste sämtliche im Arbeitsdokument WP 74[2] der Artikel-29-Datenschutzgruppe („WP 74“) formulierten Anforderungen aufzunehmen; dabei konzentriert sich die Liste auf die Punkte, die nach Maßgabe des Arbeitspapiers WP 74 von den Datenschutzbehörden bei der Bewertung der Angemessenheit zu prüfen sind.

1. Welchem Zweck dient die Checkliste?

2. Die vorliegende Checkliste soll Unternehmen Hilfestellung bieten, die einen Antrag auf Genehmigung ihrer verbindlichen unternehmensinternen Datenschutzregelungen stellen, und soll insbesondere den Nachweis der Einhaltung der im Arbeitspapier WP 74[3] gestellten Anforderungen durch das Unternehmen erleichtern.

3. An welche Datenschutzbehörde ist der Antrag zu richten?

3.1. Wenn es sich bei dem Mutterunternehmen oder der Zentrale Ihres Unternehmens um ein Unternehmen mit Sitz in einem Mitgliedstaat der EU handelt, ist der Antrag an die Datenschutzbehörde des betreffenden Mitgliedstaats zu richten.

3.2. Wenn nicht eindeutig zu bestimmen ist, wo das Mutterunternehmen oder die Zentrale Ihres Unternehmens seinen bzw. ihren Sitz hat, oder wenn sich dieser Sitz außerhalb der EU befindet, ist der Antrag an die nach den nachstehend genannten Kriterien am besten geeignete Datenschutzbehörde zu richten.

---

2 Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Regelungen für den internationalen Datentransfer. Angenommen am 3. Juni 2003.

3 In WP 74 sind die Anforderungen für verbindliche unternehmensinterne Regelungen festgelegt.

3.3. Im Antrag ist ausführlich zu begründen, weshalb es sich bei der Datenschutzbehörde, an die Sie den Antrag richten, Ihrer Meinung nach um die am besten geeignete Datenschutzbehörde handelt. Bei der Prüfung, ob Ihr Antrag an die am besten geeignete Datenschutzbehörde gerichtet wurde, werden u. a. folgende Faktoren berücksichtigt:

3.3.1. der Sitz der Zentrale des Unternehmens in Europa;

3.3.2. der Sitz des mit dem Datenschutz beauftragten Unternehmensteils[4];

3.3.3. der Sitz des Unternehmensteils, der am besten geeignet ist (hinsichtlich Managementfunktionen, Verwaltungsaufwand usw.), sich mit dem Antrag zu befassen und die verbindlichen unternehmensinternen Regelungen im Unternehmen durchzusetzen;

3.3.4. der Ort, an welchem die meisten Entscheidungen in Bezug auf Zweck und Mittel der Verarbeitung getroffen werden; und

3.3.5. die EU-Mitgliedstaaten, aus denen die meisten Übermittlungen nach außerhalb des EWR erfolgen werden.

3.4. Vorrang hat dabei der unter Punkt 3.3.1 genannte Faktor.

3.5. Hierbei handelt es sich nicht um formelle Kriterien. Die Datenschutzbehörde, an die Sie Ihren Antrag übermitteln, entscheidet im Rahmen ihres Ermessensspielraums, ob sie tatsächlich die am besten geeignete Datenschutzbehörde ist; in jedem Fall bleibt es den Datenschutzbehörden untereinander überlassen zu entscheiden, den Antrag einer anderen Datenschutzbehörde zuzuweisen als derjenigen, bei der Sie den Antrag gestellt haben.

4 Gemäß Arbeitsdokument WP 74 der Artikel-29-Datenschutzgruppe sollte das Unternehmen, wenn sich die Unternehmenszentrale nicht in der EU/dem EWR befindet, die Zuständigkeiten für den Datenschutz an einen in der EU ansässigen Unternehmensteil delegieren, der dafür verantwortlich ist zu garantieren, dass Unternehmensteile in Drittländern ihre Verarbeitung an die verbindlichen unternehmensinternen Regelungen anpassen, bei Bedarf mit der federführenden Behörde in Kontakt zu treten und Schadenersatz zu leisten für Schäden, die aus der Verletzung der verbindlichen unternehmensinternen Regelungen durch einen Unternehmensteil resultieren.

4. Welche Unterlagen werden für den Antrag benötigt?

4.1. Dem Antrag sind folgende Unterlagen beizufügen:

4.1.1. ein separates Dokument mit folgenden Angaben:

4.1.1.1. Kontaktdaten des zuständigen Mitarbeiters in Ihrem Unternehmen, an den Rückfragen gerichtet werden können;

4.1.1.2. alle einschlägigen Informationen, die die Wahl der Datenschutzbehörde begründen, u. a. Art und allgemeine Struktur der Verarbeitungsaktivitäten in der EU/dem EWR unter besonderer Berücksichtigung des Orts/der Orte, an welchem/welchen Entscheidungen getroffen werden, Sitz der angegliederten Unternehmen in der EU, Mittel und Zwecke der Verarbeitung, die Orte, von denen aus die Übermittlungen in Drittländer erfolgen, und die Drittländer, in welche die Daten übermittelt werden (diese Angaben werden von der als „Eintrittspunkt“ fungierenden Datenschutzbehörde zur Weitergabe an die betroffenen Datenschutzbehörden benötigt);

4.1.2. ein Hintergrundpapier, in dem übersichtsartig zusammengestellt ist, wie die geforderten Elemente von WP 74 (wie nachstehend festgelegt) erfüllt werden (diese Angaben erleichtern den Datenschutzbehörden das Auffinden der betreffenden Stellen in den von Ihnen vorgelegten Dokumenten);

4.1.3. alle einschlägigen Dokumente, welche die verbindlichen unternehmensinternen Regelungen enthalten, deren Annahme Ihr Unternehmen beabsichtigt (z. B. Unternehmenspolitiken, Verhaltenskodizes, Aktenvermerke, Verfahrensanleitungen und Verträge, die für den Antrag von Belang sein könnten). Außerdem eine allgemeine Grundsatzerklärung, aus der die Datenschutzbehörden ersehen können, wie der Datenschutz in Ihrem Unternehmen gehandhabt wird;

4.1.4. in diesem Zusammenhang ist zu beachten, dass zwar manche Datenschutzbehörden nach einzelstaatlichem Recht verpflichtet sind, Informationen, die sie von einem für die Verarbeitung von Daten Verantwortlichen im Rahmen des Genehmigungsvorgangs erhalten haben, nicht ohne rechtmäßige Vollmacht weiterzugeben, für andere Datenschutzbehörden hingegen auch Rechtsvorschriften zur Informationsfreiheit gelten. Wenn daher

die zusammen mit Ihrem Antrag auf Genehmigung von verbindlichen unternehmensinternen Regelungen eingereichten Unterlagen wirtschaftlich sensible Angaben enthalten, machen Sie bitte die entsprechenden Unterlagen kenntlich. Die Entscheidung über die Weitergabe der Informationen treffen jedoch die einzelnen beteiligten Datenschutzbehörden nach Maßgabe der einzelstaatlichen Rechtsvorschriften zur Informationsfreiheit. Auch müssen diejenigen Angaben, die von den übrigen beteiligten Datenschutzbehörden zur Bewertung der verbindlichen unternehmensinternen Regelungen benötigt werden, weitergegeben werden.

5. **Nachweis der Verbindlichkeit der Regelungen:**

5.1. Die Regelungen müssen verbindlich sein –

5.1.1. sowohl innerhalb des Unternehmens

5.1.2. als auch in Bezug auf die Außenwelt (rechtliche Durchsetzbarkeit).

5.2. Es gibt verschiedene Möglichkeiten, dieser Forderung nachzukommen; wie dies im Einzelnen geschieht, hängt von Größe und Struktur des Unternehmens und den Verfahren ab, die in Bezug auf andere, für Ihr Unternehmen maßgebliche rechtliche Vorschriften einzuhalten sind. Ein weiterer Faktor ist das einzelstaatliche Recht der Mitgliedstaaten, in denen Ihr Unternehmen ansässig ist.

5.3. **Verbindlichkeit innerhalb des Unternehmens**

5.4. **Wie wird garantiert, dass die Regelungen für die Unternehmensteile verbindlich sind?**

5.5. Die Einhaltung der verbindlichen unternehmensinternen Regelungen durch andere Unternehmensteile muss garantiert sein. Besonders wichtig ist dies in Fällen, in denen es entweder keine „Unternehmenszentrale“ gibt oder in denen die Unternehmenszentrale ihren Sitz außerhalb des EWR hat. Wie die Einhaltung garantiert wird, hängt von der Struktur des Unternehmens ab, aber auch von den einzelstaatlichen Rechtsvorschriften der Mitgliedstaaten, in denen Ihr Unternehmen ansässig ist.

5.6. Nachstehend einige Vorschläge dazu, wie garantiert werden kann, dass unternehmensinterne Regelungen innerhalb eines Unternehmens verbindlich sind; es ist allerdings durchaus möglich, dass andere Vorge-

hensweisen für die von Ihnen vorgeschlagenen Regelungen besser geeignet sind:

5.6.1. verbindliche unternehmensinterne oder vertragliche Regelungen, die gegenüber anderen Unternehmensteilen durchsetzbar sind;

5.6.2. einseitige Erklärungen oder Verpflichtungen seitens des Mutterunternehmens, die für die übrigen Unternehmensteile verbindlich sind;

5.6.3. die Aufnahme anderer Kontrollmaßnahmen, z. B. von in Gesetzesvorschriften enthaltenen Verpflichtungen, in einem festgelegten rechtlichen Rahmen, oder

5.6.4. die Aufnahme der Regelungen in die allgemeinen Unternehmensgrundsätze mit entsprechenden Verhaltensregeln, Audits und Sanktionen zu ihrer Durchsetzung.

5.7. Alle vorstehenden Vorschläge können in den einzelnen Mitgliedstaaten unterschiedliche Wirksamkeit haben, so gelten z. B. einfache einseitige Erklärungen in einigen Mitgliedstaaten nicht als verbindlich. Wenn Sie daher beabsichtigen, die Verbindlichkeit der Regelungen durch eine entsprechende Erklärung zu gewährleisten, sollten sie in dem betreffenden Mitgliedstaat Rechtsberatung in Anspruch nehmen.

Erläutern Sie bitte, wie garantiert wird, dass die Regelungen für alle Teile Ihres Unternehmens verbindlich sind.

5.8. **Wie wird garantiert, dass die Regelungen für die Mitarbeiter Ihres Unternehmens verbindlich sind?**

5.9. Die Regelungen müssen für die Mitarbeiter verbindlich sein. Erreicht werden kann dies beispielsweise durch diesbezügliche Verpflichtungen, die im Arbeitsvertrag festgelegt sind, und durch Disziplinarmaßnahmen bei Verstößen gegen die Regelungen. Daneben sollten geeignete spezielle Schulungsprogramme vorgesehen werden, das Engagement der Führungskräfte muss ersichtlich sein und die Funktion des letztendlich für die Einhaltung der Regelungen in Ihrem Unternehmen Verantwortlichen sollte im Antrag angegeben werden.

Führen Sie bitte aus, wie garantiert wird, dass die Regelungen für die Mitarbeiter Ihres Unternehmens verbindlich sind, und erläutern Sie die Disziplinarmaßnahmen bei Verstößen gegen die Regelungen.

5.10. **Wie wird garantiert, dass die Regelungen für Unterauftragnehmer, die die Daten verarbeiten, verbindlich sind?**

5.11. Sie müssen nachweisen, wie garantiert wird, dass die verbindlichen unternehmensinternen Regelungen Ihres Unternehmens für Unterauftragnehmer verbindlich sind. Legen Sie bitte anhand von Beispielen die diesbezüglichen Vertragsbestimmungen für Unterauftragnehmer dar und erläutern Sie die entsprechenden vertraglichen Regelungen bei Verstößen gegen die Regelungen.

Führen Sie bitte aus, wie garantiert wird, dass die Regelungen für Unterauftragnehmer verbindlich sind und erläutern Sie die Sanktionen bei Verstößen gegen die Regelungen.

5.12. **Wie wird die rechtliche Durchsetzbarkeit der Regelungen durch natürliche Personen garantiert?**

5.13. Natürliche Personen, die durch den Anwendungsbereich der verbindlichen unternehmensinternen Regelungen abgedeckt sind, müssen die Möglichkeit haben, die Einhaltung der Regelungen sowohl durch die Datenschutzbehörden als auch auf gerichtlichem Wege durchzusetzen.

5.14. Natürliche Personen müssen die Möglichkeit haben, Rechtsansprüche geltend zu machen im Gerichtsstand:

5.14.1. des Unternehmensteils, von dem die Übermittlung stammt, oder

5.14.2. der europäischen Zentrale oder des mit dem Datenschutz beauftragten in der EU ansässigen Unternehmensteils.

5.15. Aus dem Antrag muss hervorgehen, welche praktischen Schritte betroffene Personen ergreifen können, um Rechtsmittel gegen Ihr Unternehmen einzulegen, einschließlich eines Beschwerdeverfahrens.

5.16. Wenn z. B. die Unternehmenszentrale und die federführende Behörde in Belgien ansässig sind und ein Unternehmensteil in Italien gegen die unternehmensinternen Regelungen verstößt, muss für die betroffene Person klar sein, dass sie Rechtsansprüche gegen den Unternehmensteil, der die Regelungen verletzt hat, in Italien und/oder gegen die Unternehmenszentrale in Belgien geltend machen kann.

5.17. Ihr Antrag muss die Bestätigung enthalten, dass die europäische Zentrale des Unternehmens oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil in der EU über ausreichende Mittel verfügt

oder geeignete Vorkehrungen getroffen hat, um Schadenersatz für Verletzungen der verbindlichen unternehmensinternen Regelungen durch einen Unternehmensteil leisten zu können.

5.18. Im Antrag ist anzugeben, welcher Unternehmensteil für die Bearbeitung von Rechtsansprüchen zuständig ist und wie sich natürliche Personen Zugang zu den Beschwerdeverfahren verschaffen können.

5.19. Aus dem Antrag muss eindeutig hervorgehen, dass – unabhängig davon, wo der Rechtsanspruch geltend gemacht wird – die Beweislast in Bezug auf vermeintliche Verletzungen der Regelungen bei dem Unternehmensteil liegt, von dem die Übermittlung stammt, oder bei der europäischen Zentrale des Unternehmens oder bei dem mit dem Datenschutz beauftragten Unternehmensteil.

5.20. Aus dem Antrag muss hervorgehen, dass einer betroffenen Person die ihr nach Maßgabe der Richtlinie 95/46/EG gewährten Rechte zustehen.

5.21. Der Antrag muss eine Bestätigung dahingehend enthalten, dass das Unternehmen in Bezug auf alle Entscheidungen der Kontrollstelle mit den Datenschutzbehörden zusammenarbeiten und sich hinsichtlich der Auslegung von WP 74 an die Stellungnahme der Datenschutzbehörde halten wird.

Führen Sie bitte aus, wie garantiert wird, dass die Regelungen nach außen verbindlich sind.

6. Überprüfung der Einhaltung

6.1. In WP 74 ist festgelegt, dass die von dem Unternehmen angenommenen verbindlichen unternehmensinternen Regelungen entweder Eigenaudits und/oder eine externe Überwachung durch akkreditierte Auditoren vorsehen müssen.

6.2. Programm und Plan für das Datenschutzaudit müssen klar formuliert sein – entweder in einem Dokument, in dem die Datenschutzsstandards des Unternehmens festgelegt sind, oder in anderen Unterlagen zu internen Verfahrensanweisungen, und Audits sind der Datenschutzbehörde auf Verlangen vorzulegen. Die Datenschutzbehörde muss zu der Überzeugung gelangen, dass alle Aspekte der verbindlichen unternehmensinternen Regelungen von dem Auditprogramm abgedeckt werden – auch die Verfahren, mit denen sichergestellt wird, dass Abhilfemaßnahmen durchgeführt wurden. Im Auditplan muss der Kontrollstelle die Befugnis erteilt werden, im Bedarfsfall ein Datenschutzaudit durchzuführen.

6.3. Bei der Einsichtnahme von Auditergebnissen beschränken sich die Datenschutzbehörden auf Sachverhalte, die mit dem Datenschutz in Zusammenhang stehen. Mit Fragen der Unternehmensführung befassen sich die Behörden nur, insoweit diese die Einhaltung der Datenschutzvorschriften betreffen. Auch an sensiblen Geschäftsdaten haben die Behörden kein Interesse. Informationen müssen nur in dem zur Einhaltung der in WP 74 formulierten Forderungen nötigen Umfang zur Verfügung gestellt werden. Allerdings ist denkbar, dass Aspekte, die für die Einhaltung der Datenschutzvorschriften von Belang sind, auch in Berichten enthalten sein könnten, die ganz andere Informationen enthalten und dass es gelegentlich nicht möglich ist, diejenigen Elemente, die sich auf den Datenschutz beziehen, von anderweitigen Informationen zu trennen.

6.4. Geben Sie bitte eine zusammenfassende Darstellung der Auditregelungen für Datenschutzbelange in Ihrem Unternehmen und führen Sie aus, wie Auditberichte unternehmensintern gehandhabt werden (d. h. Angaben dazu, wem die Berichte vorgelegt werden und Stellung dieser Adressaten in der Unternehmensstruktur).

Machen Sie bitte detaillierte Angaben zu Datenschutz-Auditprogramm und –Auditplan Ihres Unternehmens.

7. Beschreibung der Verarbeitung und der Datenströme

7.1. Aus den verbindlichen unternehmensinternen Regelungen muss Folgendes hervorgehen:

7.1.1. die Art der Daten, d. h. ob sich die verbindlichen unternehmensinternen Regelungen nur auf einen Datentyp beziehen, z. B. Personaldaten, oder – wenn die Regelungen mehrere Arten von Daten betreffen – wie in den verbindlichen unternehmensinternen Regelungen auf diesen Aspekt eingegangen wird. In jedem Fall müssen die in dem Antrag gemachten Angaben so ausführlich sein, dass die Kontrollstelle beurteilen kann, ob die vorgesehenen Garantien der Art der durchgeführten Verarbeitung angemessen sind;

7.1.2. die Zwecke, zu denen die Daten verarbeitet werden;

7.1.3. der Umfang der Übermittlungen innerhalb des Unternehmens, die von den Regelungen erfasst werden. Hierzu sind folgende Detailangaben erforderlich:

7.1.3.1. alle Unternehmensteile in der EU, von denen aus Übermittlungen personenbezogener Daten erfolgen können, und

7.1.3.2. alle Unternehmensteile außerhalb des EWR, an die Übermittlungen personenbezogener Daten erfolgen können.

7.2. Außerdem ist nachzuweisen, ob sich die verbindlichen unternehmensinternen Regelungen ausschließlich auf Übermittlungen aus der EU beziehen oder ob sie für alle Übermittlungen zwischen Teilen des Unternehmens gelten. Die Datenschutzbehörden müssen sich ein Bild davon verschaffen können, auf welcher Grundlage Weiterübermittlungen (d. h. Übermittlungen von Daten von Unternehmensteilen außerhalb des EWR an Dritte) erfolgen.

Erläutern Sie bitte die Art der Daten, die Zwecke, für die diese Daten verarbeitet werden, und den Umfang der Übermittlungen innerhalb des Unternehmens.

8. **Garantien in Bezug auf den Datenschutz**

8.1. Aus den Regelungen muss eindeutig hervorgehen, welchen Standard die Datenschutzgarantien für die Daten nach Maßgabe der Richtlinie 95/46/EG bieten, und es muss ersichtlich sein, wie diese Anforderungen innerhalb des Unternehmens eingehalten werden.

8.2. Im Einzelnen müssen die verbindlichen unternehmensinternen Regelungen auf folgende Aspekte eingehen:

8.2.1. Transparenz und Fairness gegenüber den betroffenen Personen;

8.2.2. Beschränkung der Zweckbestimmung;

8.2.3. Gewährleistung der Datenqualität;

8.2.4. Sicherheit;

8.2.5. die Rechte natürlicher Personen in Bezug auf Zugriff, Berichtigung und Widerspruch gegen die Verarbeitung;

8.2.6. in den Regelungen formulierte Beschränkungen bezüglich der Weiterübermittlung an fremde Unternehmen (obwohl diese im Rahmen anderer Regelungen, die Übermittlungen erleichtern, möglich sein kann).

Stellen Sie bitte zusammenfassend und mit entsprechenden Begleitunterlagen (z. B. einschlägige Unternehmenspolitiken) dar, wie in den von Ihrem Unternehmen angenommenen verbindlichen unternehmensinterne Regelungen auf diese Aspekte eingegangen wird.

9. **Instrumentarium für die Meldung und Erfassung von Änderungen**

9.1. In Ihrem Unternehmen muss ein System eingerichtet sein, mit dem andere Teile des Unternehmens und die Datenschutzbehörde gemäß Absatz 4.2 von WP 74 über Änderungen der Regelungen unterrichtet werden. Den Datenschutzbehörden müssen nur Änderungen gemeldet werden, die erhebliche Auswirkungen auf die Einhaltung der Datenschutzvorschriften haben. So müssen z. B. verwaltungstechnische Änderungen nur dann gemeldet werden, wenn sie sich auf die Anwendung der verbindlichen unternehmensinternen Regelungen auswirken. Die für Ihr Unternehmen zuständige federführende Behörde wird Sie über besondere Erfordernisse hinsichtlich der Unterrichtung oder Meldung von Aktualisierungen an Datenschutzbehörden in Kenntnis setzen.

Erläutern Sie bitte das in Ihrem Unternehmen vorgesehene Instrumentarium zur Meldung von Änderungen.

Geschehen zu Brüssel am 14. April 2005

Für die Arbeitsgruppe
Der Vorsitzende
Peter Schaar

Arbeitsdokument „Festlegung eines Kooperationsverfahrens zwecks Abgabe gemeinsamer Stellungnahmen zur Angemessenheit der verbindlich festgelegten unternehmensinternen Datenschutzgarantien“ (WP 107)

Angenommen am 14. April 2005

1. Ein Unternehmen das daran interessiert ist, einen Entwurf für verbindliche unternehmensinterne Regelungen mehreren Datenschutzbehörden zur Genehmigung vorzulegen, sollte eine Datenschutzbehörde als federführende Behörde für das Kooperationsverfahren vorschlagen[1]. Grundlage für die Entscheidung darüber, welche Datenschutzbehörde als federführende Behörde fungieren sollte, bilden die in diesem Arbeitsdokument formulierten Kriterien (siehe Punkt 2). Es ist Sache des Unternehmens zu begründen, weshalb eine bestimmte Datenschutzbehörde die federführende Funktion übernehmen soll.

2. Die Wahl der federführenden Behörde ist vom antragstellenden Unternehmen anhand aussagefähiger Kriterien zu begründen wie z. B.:

   a. dem Sitz der Zentrale des Unternehmens in Europa;

   b. dem Sitz des mit dem Datenschutz beauftragten Unternehmensteils[2];

   c. dem Sitz des Unternehmensteils, der am besten geeignet ist (hinsichtlich Managementfunktionen, Verwaltungsaufwand usw.), sich mit dem Antrag zu befassen und die verbindlichen unternehmensinternen Regelungen im Unternehmen durchzusetzen;

   d. dem Ort, an welchem die meisten Entscheidungen über Zweck und Art der Datenverarbeitung getroffen werden, und

   e. den EU-Mitgliedstaaten, aus denen die meisten Übermittlungen nach außerhalb des EWR erfolgen werden.

---

1 Unter Datenschutzbehörden sind hier die Datenschutzbehörden der EU-Mitgliedstaaten und der EWR-Länder zu verstehen.

2 Gemäß Arbeitsdokument WP 74 der Artikel-29-Datenschutzgruppe sollte das Unternehmen, wenn sich die Unternehmenszentrale nicht in der EU/dem EWR befindet, die Zuständigkeiten für den Datenschutz an einen in der EU ansässigen Unternehmensteil delegieren, der dafür verantwortlich ist zu garantieren, dass Unternehmensteile in Drittländern ihre Verarbeitung an die verbindlichen unternehmensinternen Regelungen anpassen, bei Bedarf mit der federführenden Behörde in Kontakt zu treten und Schadenersatz zu leisten für Schäden, die aus der Verletzung der verbindlichen unternehmensinternen Regelungen durch einen Unternehmensteil resultieren.

2.1. Vorrang hat dabei das unter Punkt 2(a) oben genannte Kriterium.

2.2. Hierbei handelt es sich nicht um formelle Kriterien. Die Datenschutzbehörde, der der Antrag übermittelt wird, entscheidet im Rahmen ihres Ermessensspielraums, ob sie tatsächlich die am besten geeignete Datenschutzbehörde ist; in jedem Fall bleibt es den Datenschutzbehörden untereinander überlassen zu entscheiden, den Antrag einer anderen als der von dem Unternehmen ausgewählten Datenschutzbehörde zuzuweisen.

2.3. Um die Weitergabe zu erleichtern, sind der vorgeschlagenen federführenden Behörde (Eingabestelle) vom Antragsteller sowohl in gedruckter als auch in elektronischer Form alle zweckdienlichen Informationen zur Verfügung zu stellen, die seinen Antrag begründen, u. a. Art und allgemeine Struktur der Datenverarbeitung in der EU/dem EWR unter besonderer Berücksichtigung des Orts/der Orte, an welchem/welchen Entscheidungen getroffen werden, Sitz und Art der angegliederten Unternehmen in der EU, Zahl der Beschäftigten oder betroffenen Personen, Mittel und Zwecke der Verarbeitung, die Orte, von denen aus die Übermittlungen in Drittländer erfolgen (unabhängig davon, ob der Verhaltenskodex für diese Länder gilt), und die Drittländer, in welche die Daten übermittelt werden.

3. Die Eingabestelle leitet die bei ihm eingegangenen Informationen über die Gründe, weshalb diese Datenschutzbehörde von dem Unternehmen als federführende Behörde ausgewählt wurde, an alle betroffenen Datenschutzbehörden (d. h. alle Datenschutzbehörden der Länder, aus denen nach Angaben der Antragsteller die Übermittlungen erfolgen sollen) weiter und gibt dazu an, ob sie einwilligt, die Funktion der federführenden Behörde zu übernehmen. Wenn sie sich bereit erklärt, als federführende Behörde zu fungieren, werden die übrigen beteiligten Datenschutzbehörden aufgefordert, etwaige Einwände innerhalb von zwei Wochen geltend zu machen (wobei diese Frist auf Antrag einer der betroffenen Datenschutzbehörden um weitere zwei Wochen verlängert werden kann). Gelangt die Eingabestelle zu der Auffassung, dass sie die Funktion der federführenden Behörde nicht übernehmen sollte, erläutert sie die Gründe für ihre Entscheidung und spricht eine Empfehlung aus, welche Datenschutzbehörde ihrer Meinung nach als federführende Behörde geeignet wäre. Die betroffenen Datenschutzbehörden bemühen sich, innerhalb eines Monats, nachdem ihnen die Unterlagen erstmals zugegangen sind, zu einer Entscheidung zu gelangen.

4. Sobald die Entscheidung über die federführende Behörde getroffen wurde, nimmt diese die Gespräche mit dem Antragsteller auf. Als Ergebnis dieser Gespräche sollte ein „konsolidierter Entwurf“ vorgelegt werden, der allen betroffenen Datenschutzbehörden zur Stellungnahme zugeleitet wird. In

der Regel soll die Frist für Stellungnahmen zu dem konsolidierten Entwurf einen Monat nicht überschreiten.

5. Die federführende Behörde übermittelt die Stellungnahmen zu dem „konsolidierten Entwurf" dem Antragsteller und kann ggf. erneute Gespräche aufnehmen. Ist die federführende Behörde der Auffassung, dass der Antragsteller in der Lage ist, den eingegangenen Stellungnahmen zur Zufriedenheit nachzukommen, fordert sie den Antragsteller auf, die „endgültige Entwurfsfassung" zu übermitteln und fordert dann die Datenschutzbehörden auf zu bestätigen, dass sie von der Angemessenheit der vorgeschlagenen Garantien überzeugt sind.

6. Diese Bestätigung wird von allen beteiligten Behörden und dem betroffenen Unternehmen als Übereinkunft verstanden, (im Bedarfsfall) auf einzelstaatlicher Ebene die notwendige Erlaubnis oder Genehmigung zu erteilen. Im Einzelfall kann es allerdings sein, dass in den einzelnen Ländern zusätzliche Anforderungen, z. B. in Bezug auf die Bekanntmachung oder Verwaltungsvorschriften, einzuhalten sind.

7. Der Vorsitzende der Artikel-29-Gruppe wird von der Entscheidung unterrichtet und gibt diese Information umgehend über CIRCA an die übrigen Datenschutzbehörden der EU/des EWR weiter.

8. Übersetzungen: Generell sind unbeschadet weiterer Übersetzungen, soweit diese erforderlich oder per Gesetz vorgeschrieben sind, der erste Entwurf und der konsolidierte Entwurf jeweils sowohl in der Sprache der federführenden Behörde als auch in englischer Sprache vorzulegen. Die endgültige Entwurfsfassung muss in die Sprachen der betroffenen Datenschutzbehörden übersetzt werden.[3]

Geschehen zu Brüssel am 14. April 2005

Für die Arbeitsgruppe
Der Vorsitzende
Peter Schaar

[3] Auf Grundlage der Erfahrungen mit den ersten genehmigten verbindlichen unternehmensinternen Regelungen kann die Artikel-29-Datenschutzgruppe zu einem späteren Zeitpunkt ein Dokument annehmen, in dem die erforderlichen Regelungen für die Zusammenarbeit in Bezug auf die Bearbeitung von internationalen Beschwerden und anderen damit zusammenhängenden Angelegenheiten festgelegt werden.

Arbeitspapier „Datenschutzfragen im Zusammenhang mit der RFID-Technik“ (WP 105)

Angenommen am 19. Januar 2005

1. Einführung

Der Einsatz von Radio Frequency Identification, gemeinhin bekannt als „RFID-Technik“, für unterschiedliche Zwecke und Anwendungen kann für die Wirtschaft, für Privatpersonen und für öffentliche Stelle (Regierungen eingeschlossen) von Vorteil sein. Wie im Folgenden ausgeführt wird, kann RFID Einzelhändlern bei der Verwaltung ihrer Lagerbestände helfen, das Einkaufserlebnis des Verbrauchers verbessern, die Sicherheit von Arzneimitteln erhöhen und den Zugang zu Sperrbereichen überwachen helfen.

Die Vorteile, die mit dem Einsatz der RFID-Technik verbunden sind, liegen auf der Hand, doch eine breite Nutzung der Technik birgt auch Nachteile. Aus der Sicht des Datenschutzes befürchtet die „Datenschutzgruppe“, dass einige Anwendungen der RFID-Technik die Menschenwürde und den Datenschutz verletzen könnten. Die Bedenken richten sich insbesondere auf die Möglichkeit für Unternehmen und Regierungen, mittels RFID in die Privatsphäre von Privatpersonen einzudringen. Die verdeckte Sammlung einer Vielzahl von Daten, die sich alle auf ein und dieselbe Person beziehen, die Lokalisierung von Personen, die sich an öffentlichen Plätzen (Flughäfen, Bahnhöfen, Geschäften) aufhalten, die Erstellung von Kundenprofilen durch Beobachtung des Verbraucherverhaltens in Geschäften, das Auslesen von Informationen über Kleidungsstücke und Accessoires, die gerade getragen, oder über Medikamente, die mitgeführt werden, sind Beispiele für das Nutzungspotenzial von RFID, das aus datenschutzrechtlicher Sicht Anlass zu Sorge gibt. Das Problem wird noch dadurch verschärft, dass die Technik aufgrund ihrer geringen Kosten nicht nur den großen Akteuren zur Verfügung stehen wird, sondern auch kleineren bis hin zum einzelnen Bürger.

Angesichts dieser neuen Risiken sah sich die Datenschutzgruppe veranlasst, die Auswirkungen der RFID-Technik auf die Persönlichkeitsrechte und andere Grundrechte näher zu untersuchen. Zu diesem Zweck hat sie die beteiligten Gruppen, darunter Hersteller und Anwender der Technik sowie Datenschützer befragt. Die sich daran anschließende Analyse mündete in das vorliegende Arbeitspapier, mit dem die Datenschutzgruppe im Wesentlichen zwei Ziele verfolgt: Zum einen will sie den Anwendern der RFID-Technik Leitlinien an die Hand geben für die Anwendung der Grundprinzipien der EG-Richtlinien, vor-

nehmlich der Datenschutzrichtlinie[1] und der Datenschutzrichtlinie für elektronische Kommunikation[2] , und zum zweiten möchte sie den Herstellern der technischen Bausteine, also der RFID-Tags, Lesegeräte und Anwendungen, sowie den RFID-Normungsstellen Empfehlungen geben im Hinblick auf ihre Verantwortung, eine datenschutzkonforme Technik zu entwickeln, damit die Anwender der Technik ihren Verpflichtungen aus der Datenschutzrichtlinie gerecht werden können.

Angesichts mangelnder Erfahrungen mit der RFID-Technik betrachtet die Datenschutzgruppe dieses Arbeitspapier als einen ersten Situationsbericht. Sie wird die Entwicklung weiter beobachten und mit zunehmender Erfahrung weitere Leitlinien vorschlagen. Dies wird umso wichtiger, als sich die RFID-Technik zu einem wesentlichen Baustein der künftigen „intelligenten Umgebung" (Ambient Intelligence) entwickeln dürfte. Kurz gesagt, mit diesem Papier soll ein Anfang gemacht werden, und die Datenschutzgruppe wird ihre Arbeit zu diesem Thema fortsetzen.

2. Funk-Erkennung (Radio Frequency Identification, RFID): Einführung in die Technik und ihre Verwendung[3]

1. Grundlagen der RFID-Technik

Die wichtigsten Bestandteile der RFID-Technik bzw. Infrastruktur sind der RFIDTransponder (auch Tag oder Etikett genannt), also ein Mikrochip (engl. *tag*), und das Lesegerät (engl. *reader)*. Der Transponder besteht aus einem elektronischen Schaltkreis zur Datenspeicherung und einer Antenne zum Empfangen und Senden von Funkwellen. Das Lesegerät besitzt eine Antenne und einen Demodulator, der die ankommenden analogen Informationen in digitale Daten umwandelt, die dann von einem Rechner verarbeitet werden können.

Wie im Folgenden dargestellt, kann die RFID-Technik je nach Art des Tansponders und des Lesegerätes in unterschiedlicher Weise eingesetzt werden. Die Anwender der Technik können je nach Bedarf zwischen unterschiedlichen technischen Möglichkeiten wählen. Es gibt „aktive" und „passive" RFID-Transponder. „Passive" Tags haben keine eigene Energieversorgung (Batterie) und bleiben daher jahrzehntelang funktionstüchtig. Sie beziehen ihre Energie aus den empfangenen Funkwellen. Ein RFID-Lesegerät sendet Funkwellen, die

[1] Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[2] Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

[3] Eine ausführlichere technische Beschreibung von RFID und der möglichen Einsatzbereiche ist diesem Papier als Anlage beigefügt.

den Tag innerhalb einer bestimmten Reichweite aktivieren, damit er die auf ihm gespeicherten Daten überträgt. „Aktive“ Tags haben eine eigene Batterie, wodurch sich ihre Lebensdauer allerdings verringert. Sie senden ihre Informationen selbsttätig oder bleiben im Ruhezustand, bis sie von einem Lesegerät aktiviert werden.

2. Vielfältige Einsatzmöglichkeiten – Beispiele

Die RFID-Technik hält in zahlreichen *Gebieten* Einzug, z. B. im Gesundheitswesen, in der Luftfahrt oder im Verkehr. Darüber hinaus wächst auch die Zahl der spezifischen *Funktionen*, die RFID-Tags in den einzelnen Bereichen erfüllen können, und die Möglichkeiten sind noch lange nicht ausgeschöpft. In diesem Abschnitt sollen die wichtigsten Funktionen und Anwendungsbereiche der RFID-Technik, wie beispielsweise Verkehr oder Gesundheitswesen, veranschaulicht werden. Einige der beschriebenen RFID-Anwendungen befinden sich noch in der Erprobung, andere sind jedoch schon Realität, manchmal ohne dass es den Betroffenen bewusst ist.

Verkehr und Handel. RFID-Systeme eignen sich gut für einige verkehrstechnische Anwendungen. Bei entsprechender Verteilung von RFID-Lesegeräten können Fahrzeuge, die mit einem RFID-Transponder ausgerüstet sind, auf dem Weg zu ihrem Ziel lokalisiert werden. Bereits jetzt beruhen viele Fahrkarten auf der RFIDTechnik. Nach Aussagen der Automobilindustrie sind außerdem bereits Millionen von Autoschlüsseln mit RFID-Technik ausgestattet.

Luftfahrt. Die RFID-Technik kann bei der Gepäckabfertigung eingesetzt werden. Beim Einchecken erhält jedes Gepäckstück einen Transponder, anschließend können Lesegeräte, die sich in verschiedenen Abschnitten der Flughäfen befinden, das Gepäckstück bei seiner Beförderung innerhalb eines Flughafens, aber auch zwischen verschiedenen Flughäfen verfolgen. Es gibt bereits Pläne, Bordkarten mit RFID-Tags zu versehen, um verspätete Passagiere ausfindig machen zu können.

Gesundheitswesen. Die Arzneimittelindustrie verwendet RFID-Systeme, um Arzneimittel leichter lokalisieren und Fälschungen und Diebstahlsverluste während des Transports vermeiden zu können. Bei der Herstellung erhält jedes Arzneimittel ein RFIDTag, das seine Herkunft bescheinigt. Apotheken oder Geschäfte, die Arzneimittel verkaufen, erhalten Lesegeräte, die überprüfen, ob das Arzneimittel auch wirklich von dem angeblichen Hersteller stammt. Die amerikanische Gesundheitsbehörde (FDA) hat bereits Leitlinien für das Anbringen von RFID-Tags auf Arzneimittelverpackungen veröffentlicht, um die Medika-

mente lokalisieren und Fälschungen vermeiden zu können[4]. Auch in Krankenhäusern kann RFID-Technik die Sicherheit der Patienten erhöhen und den Kliniken helfen, Kosten zu sparen; so können Tags auf dem Operationsmaterial verhindern, dass am Ende einer Operation etwas im Körper des Patienten vergessen wird. Auch die Patienten selbst können mit RFID-Transpondern ausgerüstet werden, um ihre Identität, ihren Aufenthaltsort und den genauen Behandlungsverlauf feststellen zu können. Das Klinikpersonal kann ebenso mit Transpondern ausgestattet werden, damit es in Notfällen schneller ausfindig gemacht werden kann. Die amerikanische Gesundheitsbehörde hat vor kurzem einem Unternehmen die Genehmigung für den Einsatz von RFID im Menschen erteilt: unter die Haut injiziert oder eingepflanzt soll der VeriChip den Ärzten bei Notfällen Auskunft über die Krankengeschichte des Patienten geben[5].

Sicherheit und Zugangskontrolle. Mit RFID-Systemen können die Bewegungen und die Verwendung wertvoller Gegenstände verfolgt werden, da die Transponder Informationen über den Aufenthaltsort dieser Gegenstände an Lesegeräte in angemessener Reichweite senden. In der Automobilindustrie wird die RFID-Technik bereits als Bestandteil einer Wegfahrsperre genutzt. In der Konsumgüterindustrie kann mit speziellen RFID-Tags die Herkunft bestimmter Waren festgestellt werden. Auf diese Weise können hochwertige Produkte auf Fälschung überprüft werden. Seit einigen Jahren ist das Anbringen von RFID-Tags auf Banknoten ein Forschungsschwerpunkt. Aus der Arbeit der ICAO[6] zu schließen, ist ein Einsatz von RFID auch für Pässe vorgesehen[7]. Der beschränkte Zugang von Personen zu bestimmten Bereichen kann ebenfalls mit Hilfe von RFID-Tags oder berührungslosen Smartcards kontrolliert werden, wie auf dem Weltgipfel Informationsgesellschaft oder bei einem Kongress der Kommunistischen Partei Chinas bereits geschehen.

Anwendungen im Einzelhandel. Einige Einzelhandelsketten haben die Hersteller ihrer Produkte bereits gebeten, die Waren mit RFID-Tags zu versehen. Solche „getagten“ Produkte bieten dem Händler vielfältige Vorteile. So kann er mittels RFID-Technik seine Lagerverwaltung verbessern. Jedes einzelne Produkt kann in den verschiedenen Phasen, die es durchläuft, also bei der Anliefe-

---

4 Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; Guidance for FDA Staff and Industry; Compliance Policy Guide; Sec. 400.210; Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; November 2004.

5 Department of Health and Human Services; Food and Drug Administration; 21 CFR Part 880; Docket No. 2004N–0477]; veröffentlicht im Federal Register / Vol. 69, No. 237 / 10. Dezember 2004 / Rules and Regulations.

6 International Civil Aviation Organisation – Internationale Zivilluftfahrt-Organisation

7 Im Jahr 2003 legte die ICAO die technischen Anforderungen für RFID-Technik fest, mit der elektronische Pässe ausgestattet werden sollen. Die Spezifikationen wurden im ICAO-Papier 9303 veröffentlicht.

rung, im Regal oder beim Verkauf identifiziert werden; so bietet die RFID-Technik dem Händler ein flexibles Werkzeug, um die Verfügbarkeit seiner Waren im Laden und im Lager zu regeln und zu überwachen. RFID kann auch die Effizienz innerhalb der Verkaufsräume erhöhen, was sowohl dem Händler als auch möglicherweise den Kunden zugute kommt. Lesegeräte im Kassenbereich könnten die Wartezeiten und somit die Aufenthaltsdauer des Kunden im Geschäft verkürzen. RFID kann die Lokalisierung von Produkten vereinfachen und somit Rückrufaktionen für fehlerhafte, unsichere oder Produkte mit abgelaufenem Haltbarkeitsdatum erleichtern. Im Zusammenhang mit der Anwendung von RFID-Technik im Einzelhandel sollten die Normungsarbeiten von EPCglobal nicht außer acht gelassen werden, die auf die Schaffung eines „Elektronischen Produktcodes" abzielen, mit dem jedes einzelne Produkt gekennzeichnet wird[8].

3. Eingriffe in den Datenschutz und die Persönlichkeitsrechte

Während einige RFID-Anwendungen keine datenschutzrechtlichen Probleme aufwerfen, bieten viele, wie nachfolgend beschrieben, sehr wohl Anlass zu Sorge. Dieser Abschnitt gibt einen Überblick über die wichtigsten datenschutzrechtlichen Folgen, die sich aus den unterschiedlichen Anwendungen der RFID-Technik ergeben.

3.1. Erhebung von Informationen, die mit personenbezogenen Daten verknüpft sind

Datenschutzrechtliche Bedenken kommen auf, wenn die RFID-Technik zur Erhebung von Informationen eingesetzt wird, die mittelbar oder unmittelbar mit personenbezogenen Daten verknüpft werden. Vorstellbar wäre ein Fall, in dem die RFIDNummer eines Produktes mit den Daten des Käufers verknüpft wird. So könnte beispielsweise ein Elektronikhändler seine Waren mit eindeutigen Produktcodes versehen, die dann systematisch mit dem bei der Kreditkartenzahlung erfassten Kundennamen kombiniert und später mit der Kundendatei des Händlers verknüpft werden, unter anderem für Garantiezwecke. Ferner ist eine Situation denkbar, in der ein Supermarkt Kundenkarten oder ähnliches, die die Kunden namentlich identifizieren, mit RFID-Transpondern versieht, um das Kundenverhalten in den Verkaufsräumen zu erfassen, z. B. die Zeit, die Kunden in bestimmten Abteilungen verbringen, die Zahl der Besuche ohne Einkauf usw.

In den oben genannten Fällen ist der Eingriff in die Persönlichkeitsrechte offensichtlich, da die mittels RFID-Technik erhobenen Informationen mit personenbezogenen Daten verknüpft werden. Mit Hilfe des Systems der Kundenkarten können schon heute Verbrauchergewohnheiten erfasst und individuelle Profile erstellt werden; die RFID-Technik erweitert diese Möglichkeiten noch: die Aus-

[8] Weitere Informationen über EPCglobal sind in Abschnitt 5.2 nachzulesen.

rüstung jedes einzelnen Produkts mit einem RFID-Tag („item-level tagging“) erhöht das Direktmarketingpotenzial, da die Kunden beim Betreten des Geschäftes identifiziert und ihr Verhaltensweisen im Geschäft beobachtet werden können. Darüber hinaus wird der großflächige Einsatz der Technik, sowohl was die Art als auch was die Zahl der Daten angeht, eine Datenflut auslösen, die von den unterschiedlichsten Verantwortlichen verarbeitet werden muss; auch dies gibt Anlass zu Sorge.

3.2. Speicherung personenbezogener Daten auf dem Transponder

Persönlichkeitsrechte werden aber auch verletzt, wenn personenbezogene Daten unmittelbar auf RFID-Tags gespeichert werden. Ein Beispiel für diese Nutzungsart sind Fahrkarten. Vorstellbar wäre der Fall eines Unternehmens, das beschließt, ein berührungsloses RFID-basiertes Fahrkartensystem für Monatskarten aufzubauen, bei dem Name, Anschrift, Telefonnummer usw. des Fahrkarteninhabers auf dem Tag gespeichert sind. Auf diese Weise könnte das Unternehmen jederzeit die Fahrstrecken des einzelnen Kunden nachvollziehen. Dies stellt einen offensichtlichen Eingriff in die Privatsphäre der Betroffenen dar. Doch nicht nur das Verkehrsunternehmen könnte über diese Informationen verfügen; auch Dritte könnten sich die Informationen verdeckt beschaffen, da jedes Standard-Lesegerät die Existenz bestimmte RFID-Tags erkennen kann. Es sei darauf hingewiesen, dass RFID-Systeme sehr angriffsanfällig sind. Da sie unsichtbar und berührungslos arbeiten, kann ein Angriff aus der Entfernung erfolgen und das passive Auslesen eines Tags ist für den Betroffenen nicht feststellbar.

3.3. Personenverfolgung ohne „traditionelle“ Kenndaten

Eine dritte Art von Datenschutzverletzungen ergibt sich aus dem Einsatz von RFID zur Verfolgung („Tracking“) einzelner Personen und zur Gewinnung personenbezogener Daten. Die nachfolgenden Beispiele zeigen, wie die RFID-Technik in die Persönlichkeitsrechte eingreifen kann.

Eine Handelskette gibt an ihre Kunden beispielsweise mit RFID-Tags versehene Pfandmünzen für Einkaufswagen aus, die bei jedem Einkauf wiederverwendet werden können. Mit Hilfe der auf der Pfandmünze gespeicherten Identifikationsnummer könnte eine Datei erstellt werden, aus der ersichtlich wäre, welche Produkte eine durch die Pfandmünze identifizierte Person kauft, wie häufig sie diese Produkte kauft und welche Filialen der Handelskette sie aufsucht. Die Filialen könnten Rückschlüsse auf das Einkommen, den Gesundheitszustand, den Lebensstil, die Einkaufsgewohnheiten usw. des Kunden ziehen. Diese Informationen wiederum könnten bestimmte Verkäuferentscheidungen beeinflussen, z. B. die Marketingstrategie oder gar eine dynamische Preispolitik. Da der Kunde mit Hilfe der Pfandmünze jedes Mal identifiziert würde, wenn er die Ver-

kaufsräume betritt, könnten seine gespeicherten Einkaufsgewohnheiten für individuelle Werbeaktionen genutzt werden. Neben den einzelnen Filialen könnten aber auch Dritte diese Angaben erhalten. Auf diese Weise könnten eine Reihe von Entscheidungen über die identifizierte Person getroffen werden, ohne dass diese hierzu in voller Kenntnis der Sachlage ihre Einwilligung gibt. Ähnlich wie bei der Verwendung von Cookies im Internetkontext lässt sich die betroffene Person, selbst wenn sie nicht sofort und unmittelbar anhand eines bestimmten Produkts identifiziert werden kann, auf der assoziativen Ebene problemlos identifizieren, und zwar über die Masse der sie umgebenden bzw. über sie gespeicherten Informationen. Die erhobenen Daten können sogar die Art beeinflussen, in der die betroffene Person behandelt oder beurteilt wird. Auch diese RFID-Anwendung löst schwerwiegende datenschutzrechtliche Befürchtungen aus.

Datenschutzrechtliche Bedenken ergeben sich auch in Situationen, in denen die Verwendung von RFID-Tags die Verarbeitung personenbezogener Daten nach sich zieht, selbst wenn keine weiteren eindeutigen Kenndaten verwendet werden. Angenommen die Person Z betritt das Geschäft C mit einer Tasche, in der sich „getagte“ Produkte aus den Geschäften A und B befinden. Geschäft C scannt diese Tasche, und die darin befindlichen Produkte (wahrscheinlich eher ein Wirrwarr an Zahlen) werden erfasst. Geschäft C speichert diese Zahlen. Kommt der Kunde Z am nächsten Tag wieder in das Geschäft, wird er wieder gescannt. Das Produkt Y, das bereits am Vortag gescannt wurde, wird wiedererkannt – die Nummer steht für die Armbanduhr, die der Kunde täglich trägt. Geschäft C erstellt eine Datei mit der Nummer des Produktes Y als „Schlüssel“. Nun kann der Kunde beim Betreten des Geschäfts anhand der RFID-Nummer der Armbanduhr erkannt werden. Geschäft C kann jetzt für den Kunden Z (dessen Name ihm nicht bekannt ist) ein Profil erstellen und verfolgen, was der Kunde bei späteren Besuchen in seiner Einkaufstasche hat. Auf diese Weise verarbeitet Geschäft C personenbezogene Daten, folglich findet das Datenschutzrecht Anwendung.

Schließlich wären da noch RFID-Transponder auf bestimmten Gegenständen, die Auskunft über die Art des Gegenstandes geben. Eigentumsgegenstände einer Person sind etwas sehr Persönliches und beinhalten Informationen, deren Kenntnis durch Dritte einen Eingriff in die Privatsphäre dieser Person darstellen würde. Folgende Beispiele veranschaulichen diese Aussage. Angenommen jeder, der ein Lesegerät besitzt, kann Banknoten, Bücher, Arzneimittel oder Wertgegenstände von Passanten ausfindig machen. Erhalten Dritte Kenntnis von diesen Informationen, stellt dies einen Eingriff in die Persönlichkeitsrechte des Eigentümers. Bedenklich wäre auch, wenn Terroristen in der Lage wären, in einer Menschenmenge Personen bestimmter Nationalitäten ausfindig zu machen. Noch schwerwiegender wäre der hier beschriebene Eingriff, wenn der Gegens-

tand selbst wichtige personenbezogene Daten enthielte, beispielsweise Ausweisdaten oder hochsensible Daten.

Diese Beispiele veranschaulichen einige der größten Gefahren der RFID-Technik für den Datenschutz und die Persönlichkeitsrechte, die darin bestehen, dass Personen verdeckt und ohne ihre Einwilligung ausspioniert werden, und zwar durch den unautorisierten Zugriff auf die von den RFID-Tags übertragenen Informationen.

In den folgenden Abschnitten wird erläutert, wie wichtig es ist, die oben beschriebenen Datenverarbeitungsverfahren an Leitlinien für die Anwendung der in den EG-Richtlinien, insbesondere der Datenschutzrichtlinie, verankerten Grundprinzipien zu knüpfen.

4. Anwendung des EU-Datenschutzrechts auf die Datenerhebung mittels RFID-Technik

4.1. Leitlinien für die Anwendung der Datenschutzrichtlinie auf die Sammlung und Weiterverarbeitung von Daten mittels RFID-Technik

Der Geltungsbereich der Datenschutzrichtlinie umfasst die Verarbeitung aller personenbezogenen Daten. Die Richtlinie enthält eine sehr weitgefasste Definition für „personenbezogene Daten“, die sich auf *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person“* erstreckt. Somit stellt sich die Frage, ob die Datenschutzrichtlinie damit zwangsläufig für die Datenerhebung mittels RFID-Technik gilt. Die Antwort wird immer von der jeweiligen Anwendung abhängen, insbesondere davon, ob die sie eine Verarbeitung personenbezogener Daten im Sinne der Datenschutzrichtlinie nach sich zieht.

Um zu beurteilen, ob die Erhebung personenbezogener Daten mittels einer bestimmten RFID-Anwendung unter die Datenschutzrichtlinie fällt, gilt es zu klären, a) inwieweit die verarbeiteten Daten sich auf eine betroffene Person *beziehen* und b) ob diese Daten eine Person betreffen, die *bestimmbar* oder bereits bestimmt ist. Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird. Um festzustellen, ob die Daten eine bestimmbare Person betreffen, ist Erwägungsgrund 26 der Datenschutzrichtlinie heranzuziehen; danach sollten „*alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen*“.

Somit fällt nicht jede Datenerhebung mittels RFID-Technik unter die Datenschutzrichtlinie, es ist aber auch nicht von der Hand zu weisen, dass es viele Situation geben wird, in denen personenbezogene Daten mittels RFID-Technik erhoben werden, deren Verarbeitung sehr wohl richtlinienrelevant ist.

Jeder, der Informationen verwenden will, die mittels RFID-Technik erhoben wurden, wird vorher prüfen müssen, ob die Informationen als „personenbezogene Daten" im Sinne der Datenschutzrichtlinie anzusehen sind. Enthalten die RFID-Informationen keine personenbezogenen Daten und werden auch nicht, wie oben beschrieben, mit personenbezogenen Daten verknüpft, findet die Datenschutzrichtlinie keine Anwendung. Werden also die Informationen auf dem RFID-Tag nicht mit anderem „Identifizierungsmaterial" verknüpft, beispielsweise mit einem Foto, dem Namen und der Anschrift der betreffenden Person oder einer wiederkehrenden Kennnummer, dann kommt die Datenschutzrichtlinie nicht zur Anwendung.

In den drei in Abschnitt 3 beschriebenen Fällen würde die Datenschutzrichtlinie Anwendung finden. Im ersten Fall, weil die mittels RFID-Technik erhobene Produktinformation direkt mit den auf einer Kredit- oder Kundenkarte gespeicherten personenbezogenen Daten verknüpft wird. Im zweiten Fall gilt die Datenschutzrichtlinie ab dem Zeitpunkt, an dem personenbezogene Daten, wie ein Name, im RFID-Transponder gespeichert werden. Schließlich gilt die Datenschutzrichtlinie auch dann, wenn mittels RFID-Technik Bewegungen einzelner Personen verfolgt werden, die zwar nicht bestimmt werden, angesichts der massiven Datenaggregation, der Speicher- und Verarbeitungsmöglichkeiten, aber bestimmt werden könnten.

4.2 Leitlinien für die Konformität mit den Datenschutzerfordernissen

Die Verantwortlichen für die Verarbeitung von mittels RFID-Technik erhobenen Daten sind an die Datenschutzrichtlinie gebunden (in dem vorliegenden Papier werden sie häufig als „Anwender der Technik" bezeichnet). Es kann zwar unmöglich festgelegt, wie diese Anforderungen in jedem einzelnen RFID-Szenario zu erfüllen sind, es ist aber möglich, einige allgemeine Leitlinien zu entwerfen, an die sich die für die Datenverarbeitung Verantwortlichen halten und die sie an die jeweiligen Umstände der Datenverarbeitung anpassen können. Wie in Abschnitt 5 näher erläutert wird, sind die Hersteller für die Bereitstellung einer datenschutzkonformen Technik direkt verantwortlich; diese soll dazu beitragen, dass die Verarbeiter ihren Verpflichtungen aus der Datenschutzrichtlinie nachkommen und dass die betroffenen Personen ihre Rechte wahrnehmen können.

Grundsätze:

Die Datenschutzgruppe weist darauf hin, dass Erwägungsgrund 2 der Datenschutzrichtlinie den Rahmen für die Anwendung der RFID-Technik, wie für jede andere Technik bildet: „*Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnortes der natürlichen Personen, deren Grundrechte und –freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen*."

Grundsätze der Datenqualität: Die für die Datenverarbeitung Verantwortlichen, die im Zuge von RFID-Anwendungen Daten erheben, müssen u. a. folgende **Datenschutzgrundsätze** einhalten:

Grundsatz der begrenzten Verwendung (Zweckbestimmung): Dieser Grundsatz, der teilweise in Artikel 6 Absatz 1 Buchstabe b der Datenschutzrichtlinie verankert ist, verhindert unter anderem eine Weiterverarbeitung, die mit dem Zweck (den Zwecken) der Datenerhebung unvereinbar ist.

Grundsatz der Datenqualität: Dieser ebenfalls in der Richtlinie festgeschriebene Grundsatz fordert, dass die personenbezogenen Daten für die Zwecke, für die sie erhoben werden, erheblich sind und nicht darüber hinausgehen. Demzufolge dürfen keine unerheblichen Daten erhoben werden; falls dies dennoch geschehen ist, müssen sie gelöscht werden (Artikel 6 Absatz 1 Buchstabe c). Darüber hinaus müssen die Daten sachlich richtig und auf dem neuesten Stand sein.

Aufbewahrungsgrundsatz: Diesem Grundsatz zufolge dürfen personenbezogene Daten nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Rechtsgrundlage für die Verarbeitung: Gemäß Artikel 7 der Datenschutzrichtlinie dürfen personenbezogene Daten nur verarbeitet werden, wenn eine der Voraussetzungen für eine rechtmäßige Datenverarbeitung erfüllt ist[9].

[9] Artikel 7 listet die folgenden Voraussetzungen auf, die eine Datenverarbeitung rechtfertigen: i) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben, ii) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, iii) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt, iv) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person, v) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, vi) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von der für die Verarbeitung verantwortlichen Partei wahrgenommen wird,

In der Mehrzahl der Fälle, in denen RFID-Technik eingesetzt wird, werden sich die für die Verarbeitung Verantwortlichen lediglich auf die Einwilligung der betroffenen Person als rechtmäßige Voraussetzung für die Datenerhebung mittels RFID stützen können. So wird ein Supermarkt, der seine Kundenkarten mit RFID-Tags versieht, entweder ausdrückliche vertragliche Vereinbarungen oder die Einwilligung der betroffenen Person benötigen, um die personenbezogenen Informationen, die er bei der Ausstellung der Kundenkarte erhalten hat, mit den Daten verknüpfen zu dürfen, die das RFID-Tag übermittelt. Die Einwilligung der betroffenen Person ist jedoch nicht immer die adäquate rechtliche Voraussetzung, um die Verarbeitung personenbezogener Daten, die im Rahmen von RFID-Systemen erhoben wurden, zu rechtfertigen. So bräuchte beispielsweise eine Klinik, die RFID in Operationsbestecken verwendet, um zu vermeiden, dass bei Beendigung einer Operation Instrumente im Körper des Patienten vergessen werden, nicht unbedingt das Einverständnis des Patienten, da diese Form der Verarbeitung mit den lebenswichtigen Interessen der betroffenen Person gerechtfertigt werden könnte, die gemäß Artikel 7 der Datenschutzrichtlinie[10]) einen anderen Rechtfertigungsgrund darstellen.

Basiert die Verarbeitung auf der Einwilligung der betroffenen Person, sind gemäß Artikel 2 und Artikel 7 Buchstabe a der Richtlinie bestimmte Erfordernisse zu erfüllen. (i) Die Einwilligung muss freiwillig gegeben werden, d. h. ohne „Täuschung oder Zwang". (ii) Sie muss spezifisch sein, d. h. sie muss sich auf einen bestimmten Zweck beziehen. (iii) Die Einwilligung muss Ausdruck des tatsächlichen Willens der betroffenen Person sein. (iv) Die Einwilligung muss in voller Kenntnis der Sachlage erfolgen. Schließlich muss sie „*ohne jeden Zweifel"* gegeben werden, d. h. eine Einwilligung, die mehr als eine Interpretation zulässt, gilt nicht als Einwilligung.

Informationserfordernisse: Gemäß Artikel 10 der Datenschutzrichtlinie müssen die für die Datenverarbeitung Verantwortlichen, die mittels RFID-Technik Daten verarbeiten, den betroffenen Personen folgende Informationen mitteilen: die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung sowie unter anderem Informationen über die Empfänger der Daten und das Bestehen eines Auskunftsrechts[11]. In dem in Abschnitt 4 ge-

---

sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

[10] Die Datenschutzgruppe weist darauf hin, dass die in Artikel 7 der Datenschutzrichtlinie aufgestellten rechtlichen Voraussetzungen, die eine bestimmte Datenverarbeitung rechtfertigen, letztlich von den besonderen Umständen dieser Verarbeitung abhängig sind.

[11] Informationen über die Empfänger der Daten, über die Antwortpflicht und über das Bestehen von Auskunfts- und Berichtigungsrechten müssen unter Berücksichtigung der jeweiligen Umstände, unter denen die Daten erhoben werden, bereitgestellt werden, sofern sie

schilderten Szenario müsste der Einzelhändler in Erfüllung dieser Verpflichtungen die betroffenen Personen mindestens über Folgendes informieren:

(i) die Existenz von RFID-Tags auf Produkten oder auf ihren Verpackungen und die Existenz von Lesegeräten;

(ii) die Folgen im Hinblick auf die Datenerhebung; insbesondere sollten die für die Verarbeitung Verantwortlichen die Betroffenen sehr genau darüber informieren, dass die RFID-Tags von den Lesegeräten zur Übertragung von Daten veranlasst werden können, ohne dass hierfür die betroffenen Personen in irgendeiner Weise tätig werden müssen.

(iii) die Zwecke, für die die Informationen bestimmt sind, einschließlich Angaben darüber a) mit welchen Daten die RFID-Informationen verknüpft werden und b) ob die Informationen Dritten verfügbar gemacht werden; ferner

(iv) die Identität des für die Verarbeitung Verantwortlichen. Darüber hinaus muss der für die Verarbeitung Verantwortliche je nach Art der RFID-Anwendung die betroffenen Personen darüber informieren,

(v) wie die Tags gelöscht, deaktiviert oder von den Produkten entfernt werden können, um zu verhindern, dass sie weitere Informationen übermitteln, und

(vi) wie die Betroffenen ihr Auskunftsrecht wahrnehmen können. Diese Auskünfte wären in den in Abschnitt 3.1 beschriebenen Szenarios erforderlich. Hinweise bei Gebrauchsgütern, wie z. B. die für EPCglobal vorgeschlagenen, dienen zwar der Bereitstellung der unter i) genannten Informationen; diese sollten aber um die oben aufgeführten Informationen ergänzt werden[12].

Gemäß dem in Artikel 6 Buchstabe a der Datenschutzrichtlinie verankerten Prinzip der Verarbeitung nach Treu und Glauben, müssen die Informationen für die betroffene Person klar und verständlich sein.

Schließlich möchte die Datenschutzgruppe darauf hinweisen, dass die betroffene Person durch die Bereitstellung der obigen Informationen in der Lage sein sollte, ohne Weiteres die Folgen der RFID-Anwendung zu verstehen.

---

notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

[12] Abschnitt 5.1 enthält einen Überblick über die Tätigkeiten von EPCglobal.

Das Auskunftsrecht der betroffenen Person: Artikel 12 der Datenschutzrichtlinie gibt den betroffenen Personen die Möglichkeit, die Richtigkeit der Daten zu überprüfen und sicherzustellen, dass die Daten auf dem neuesten Stand sind. Diese Rechte gelten in vollem Umfang auch bei der Erhebung personenbezogener Daten mittels RFID-Technik. Für den Supermarkt, der Kundenkarten „tagt", bedeutet dies z. B., dass er im Rahmen des Auskunftsrechts *alle* Informationen offenlegen muss, die mit der betroffenen Person verknüpft sind, beispielsweise die Anzahl der Besuche in dem Geschäft, die Art der Einkäufe usw.

Enthalten RFID-Transponder personenbezogene Daten wie in Abschnitt 3.2 beschrieben, sollten die betroffenen Personen erfahren dürfen, welche Informationen auf den Transpondern gespeichert sind, und das Recht haben, mit einfachen Mitteln Berichtigungen vorzunehmen.

Sicherheitserfordernisse: Artikel 17 der Datenschutzrichtlinie verpflichtet die für die Verarbeitung Verantwortlichen, geeignete Maßnahmen zum Schutz gegen zufällige oder unrechtmäßige Zerstörung oder unberechtigte Offenlegung zu ergreifen. Die Maßnahmen können organisatorischer oder technischer Art sein. Auf dieses Erfordernis wird in Abschnitt 5 näher eingegangen, der sich mit der RFID-Technik und dem notwendigen Einsatz datenschutzfreundlicher Technik beschäftigt.

5. Technische und organisatorische Erfordernisse, die eine angemessene Verwirklichung der Datenschutzgrundsätze gewährleisten

Die Anwender von RFID-Technik müssen die oben genannten Grundsätze sowie das in Artikel 6 Absatz 1 der Datenschutzrichtlinie verankerte Prinzip der Datensparsamkeit einhalten.

Nach Auffassung der Datenschutzgruppe kann die Technik eine Schlüsselrolle übernehmen, wenn bei der Verarbeitung personenbezogener Daten, die mittels RFID erhoben wurden, die Einhaltung der Datenschutzgrundsätze gewährleistet werden soll. So könnte beispielsweise mit der Normung des Aufbaus von RFID-Tag, -Lesegeräten und - Anwendungen erreicht werden, dass personenbezogene Daten sparsam erhoben und verwendet werden, und dass jedwede unrechtmäßige Verarbeitung verhindert wird, indem ein unautorisierter Zugriff auf personenbezogene Daten technisch vereitelt wird.

In diesem Zusammenhang möchte die Datenschutzgruppe betonen, dass zwar die Anwender letztlich für die mittels einer RFID-Anwendung erhobenen personenbezogenen Daten verantwortlich sind, dass es aber Aufgabe der Hersteller und der Normungsgremien ist, den Anwendern eine datenschutzkonforme Technik zur Verfügung zu stellen, die Eingriffe in die Persönlichkeitsrechte verhindert. Es sollten Mechanismen entwickelt werden, die sicherstellen, dass solche

Normen bei der praktischen Anwendung weitgehend eingehalten werden. Datenschutzkonforme RFID-Normen müssen insbesondere gewährleisten, dass Verantwortliche, die personenbezogene Daten mittels RFID-Technik verarbeiten, über die Instrumente verfügen, die zur Einhaltung der Datenschutzrichtlinie erforderlich sind. Die Datenschutzgruppe ruft daher die Hersteller von RFID-Tags, -Lesegeräten und -Anwendungen sowie die Normungsgremien auf, die folgenden Empfehlungen bei ihrer Arbeit zu berücksichtigen.

5.1 Einfluss von Normung und Interoperabilität auf die Verwirklichung der Datenschutzgrundsätze

Bei jeder Technik ist die Normung normalerweise die wichtigste Voraussetzung für Interoperabilität, die wiederum für eine erfolgreiche Akzeptanz und Umsetzung neuer Techniken wichtig ist. Normung kann auch den Erlass von Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre erleichtern.

Alle Bestandteile eines RFID-Systems sind oder werden genormt, beispielsweise der Aufbau des Transponders und des Lesegeräts, die auf dem Tag gespeicherten Daten, das Kommunikationsprotokoll (Luftschnittstelle) zwischen Lesegerät und Transponder, die Verwaltung der vom Lesegerät ausgelesenen Daten usw. Die Normungsgremien und auch andere Stellen sind bereits im RFID-Bereich tätig geworden. Die RFID-Normung wird sich auf zahlreiche Märkte auswirken, insbesondere auf den Warenhandel.

Ursprünglich als Reaktion auf die BSE-Krise hat die Internationale Normungsorganisation (ISO) sektorspezifische Normen (Frachtbehälter, Transporteinheiten, Tiere usw.) für RFID-Transponder entwickelt, außerdem allgemeinere Normen für die Luftschnittstelle (ISO-Reihe 18000) und für das Artikelmanagement (ISO/EIC/15963:2004).

EPCglobal Inc.[13], ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC), wird geleitet von dem EPCglobal-Direktorium, in dem führende Unternehmen vertreten sind. Das Unternehmen arbeitet an einem „elektronischen Produkt-Code (EPC)“, mit dem jeder einzelne Artikel identifiziert werden kann. Jedes Produkt erhält einen Transponder auf dem die jeweilige Artikelnummer verzeichnet ist. Vorläufer dieses Systems ist der „Universal Product Code (UPC)“ oder Barcode, den der EPC ersetzen soll. Der Unterschied zwischen den beiden Systemen besteht darin, dass der UPC einen Produkttyp identifiziert, ohne dass jeder Artikel individuell nummeriert wird. Daneben entwickelt das EPCglobal-Netzwerk Normen für die Verbindung von Servern, die Informationen über mit EPC-Nummern identifizierte Artikel enthalten. Diese Server, auch EPC Information Services oder EPCIS genannt, sind über das In-

[13] http://www.epcglobalinc.org/

ternet zugänglich und über eine Reihe von Netzwerkdiensten verknüpft, autorisiert und zugänglich[14].

Bei den meisten RFID-Normungsinitiativen können Datenschutzmerkmale in die technischen Spezifikationen aufgenommen werden. So wurde beispielsweise kürzlich vorgeschlagen[15], die ISO-Norm für das Reader-to-Tag-Protokoll zu verändern, um die von der OECD ausgearbeiteten Fair Information Practices[16] mit einzubeziehen.

Vor kurzem hat das Europäische Institut für Telekommunikationsstandards (ETSI) eine neue europäische Norm für den Einsatz von RFID-Systemen angenommen, die die zulässige Leistung des Lesegerätes und die Zahl der verfügbaren Kanäle auf dem UHFBand erhöht, dem vielversprechendsten Band für die Artikelidentifizierung im Bereich des Einzelhandels. Diese Entwicklung wird insbesondere die Reichweite zwischen Lesegerät und RFID-Transponder vergrößern[17].

Die Interoperabilität von RFID-Systemen (Hardware, Software und erzeugte Daten) ergibt sich logischerweise aus der Normung. Die Unternehmen sehen die Interoperabilität von RFID-Systemen positiv. Natürlich sollte ein Einzelhändler im Hinblick auf ein nachhaltiges Geschäftsmodell nicht gezwungen sein, unterschiedliche Lesegeräte zu installieren, um die Transponder unterschiedlicher Hersteller auslesen zu können. Aus Sicht des Datenschutzes kann die Interoperabilität zwar die technische Qualität der Daten erhöhen und zur Einhaltung von Artikel 6 Absatz 1 Buchstabe d der Datenschutzrichtlinie beitragen, gleichzeitig kann sie aber auch negative Nebeneffekte auf den Datenschutz haben, sofern keine entsprechenden Maßnahmen ergriffen werden. So ist beispielsweise das Prinzip der Zweckbegrenzung schwieriger anzuwenden und zu kontrollieren. Wenn die Zahl der Akteure ansteigt, die die Daten verarbeiten, könnte darüber hinaus auch die Verwaltung der Zugriffsrechte aus datenschutzrechtlicher Sicht problematischer werden.

---

[14] Bis heute sind die Interessen der EU bei diesen Normungsinitiativen unterrepräsentiert, da dort im Wesentlichen Interessenträger der US-Industrie vertreten sind. Ferner steht noch nicht fest, ob die chinesische Seite eine der genannten Normen übernehmen oder möglicherweise eigene Normen entwickeln wird.

[15] Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), 8.-9. November 2004, Tokio, Japan.

[16] ISO 18000 Teil 6 Typ A

[17] Die Reichweite des Lesegeräts und seine Leistung können darüber entscheiden, inwieweit eine bestimmte RFID-Anwendung in die Privatsphäre betroffener Personen eindringt.

5.2 Technische und organisatorische Maßnahmen zur Information der Betroffenen über die Anwesenheit, Erkennbarkeit und Aktivierbarkeit von RFID-Geräten

Wie in Abschnitt 4 bereits erwähnt, müssen die Anwender der RFID-Technik die betroffenen Personen nicht nur über die Zweckbestimmungen der Datenverarbeitung informieren, sondern *auch* über die Anwesenheit von RFID-Geräten; dabei müssen sie folgende Anforderungen erfüllen:

Erstens müssen die Betroffenen über die Anwesenheit RFID-ähnlicher Geräte bzw. aktivierter RFID-Lesegeräte informiert werden. Zu diesem Zweck sind Piktogramme unerlässlich, wobei hier eine weltweite Norm erstrebenswert wäre, ferner weitere sachdienliche Informationsmittel, die diesen Zweck erfüllen. Die Bereitstellung dieser Information ist unverzichtbar, damit die unautorisierte und verdeckte Sammlung personenbezogener Daten mittels RFID-Technik verhindert werden kann. Gibt es beispielsweise in einem Geschäft oder in einer Klinik aktivierte Lesegeräte, sollten die betroffenen Personen darüber informiert werden.

Zweitens ist es aus den gleichen Gründen (Vermeidung verdeckter Datensammlung) wichtig, dass die betroffenen Personen *RFID-Tags in ihrer Umgebung* (beispielsweise in der Kleidung) erkennen können, da diese aufgrund ihrer Größe möglicherweise fast unsichtbar sind. Hier bieten sich vielfältige Möglichkeiten an, z. B. Standardhinweise oder auch technische Lösungen.

Drittens werden die Informationen über die bloße Anwesenheit von RFID in der Praxis nicht ausreichen; auch über die Aktivierbarkeit bzw. die *Echtzeitaktivierung* von RFIDs sollten die betroffenen Personen gemäß Datenschutzrichtlinie informiert werden. Dies bedeutet, dass einfache Verfahren zur Sichtbarmachung des Aktivierungszustands bzw. der Aktivierbarkeit benötigt werden. Für die Betroffenen leicht zugänglich sein sollten auch Informationen über die Existenz und die Art datenschutzfreundlicher Techniken, wie die Möglichkeit der vorübergehenden Deaktivierung oder physischen Entfernung des Tags, ferner Informationen über organisatorische Maßnahmen in einer bestimmten Umgebung.

Die Datenschutzgruppe betont, dass weitere Forschungs- und Entwicklungsanstrengungen zur Erfüllung dieser drei Erfordernisse für alle Beteiligten unabdingbar sind.

5.3 Technische und organisatorische Maßnahmen zur Wahrnehmung des Rechts auf Auskunft, Berichtigung und Löschung

Wie im Folgenden beschrieben, kann der Aufbau der RFID-Technik einen großen Einfluss darauf haben, inwieweit die Wahrnehmung des Rechts auf Auskunft, Berichtigung und Löschung im Sinne des Artikels 12 Datenschutzrichtlinie tatsächlich gewährleistet ist.

(a) Auskunft über den Inhalt des RFID-Tags (Artikel 12 Buchstabe a Datenschutzrichtlinie)

Technisch bedingt ist der Zugriff auf den Inhalt eines RFID-Transponders nur mit einem Lesegerät, das mit dem Tag über ein Protokoll kommuniziert, und einem Anzeigegerät möglich. In vielen Anwendungen enthält der Tag Aber lediglich eine ID-Nummer, deren Bedeutung nur über eine komplette IT-Anwendungsumgebung ermittelt werden kann. Unserer Kenntnis nach enthalten nur wenige RFID-Tags aussagekräftige Informationen (Beschreibung des Artikels, Kennung des für die Verarbeitung Verantwortlichen, Zweck der Datenerhebung usw.), aber selbst dann ist es für die betroffenen Personen schwierig, Auskunft über den Inhalt zu erhalten.

Eine Möglichkeit, diesen Informationen Aussagekraft zu verleihen, besteht darin, semantische Normen zu definieren, z.B. mit XML. Gleichwohl werfen diese semantischen Beschreibungen unabhängig von ihrer Form noch das Problem des Zugriffs durch unberechtigte Dritte auf (vgl. Abschnitt 3).

(b) Berichtigung des Inhalts (Artikel 12 Buchstabe b Datenschutzrichtlinie)

Im Gegensatz zum bloßen Zugriff auf den Inhalt sind für die Berichtigung ein Lesegerät, das mit dem Transponder-Protokoll kommunizieren kann, und ein interaktives IT-System erforderlich; auf diese Weise hat die betroffene Person die Möglichkeit, sowohl das Auslesen des Inhalts als auch seine Berichtigung zu überwachen.

Vorgeschlagen wurde bereits, in den Transponder eine Vorrichtung einzubauen, die die Artikelseriennummer löscht oder verschlüsselt, so dass lediglich die Objektklassenbeschreibung ganz oder teilweise lesbar ist; vorstellbar wäre auch die umgekehrte Möglichkeit, allerdings mit anderen Implikationen für die Privatsphäre.

(c) Löschen des Inhalts (Artikel 12 Buchstabe b Datenschutzrichtlinie)

Die Entscheidung, ob Vorrichtungen zur Deaktivierung der Tags eingeführt werden sollten oder nicht, mit denen die betroffenen Personen die Verarbeitung ihrer personenbezogenen Daten unterbinden können, wenn der Transponder in die Reichweite eines Lesegerätes kommt, hängt von der Rechtsgrundlage ab, auf der im jeweiligen Fall die Verarbeitung personenbezogener Daten beruht. Nicht sinnvoll wäre es beispielsweise bei RFID-Tags in Ausweisen, wohingegen es aus Datenschutzgründen bei RFID-Tags auf Konsumgütern durchaus erforderlich wäre. Diese Frage wurde auch auf der Konferenz der Datenschutzbeauftragten in Sydney erörtert und fand ihren Niederschlag in einer Erklärung zu RFID[18].

In den letzten Jahren wurden verschiedene Lösungen vorgeschlagen. Ein Vorschlag betraf die Einführung eines „Kill"-Befehls. Dies bedeutet, dass der Transponder dauerhaft oder vorübergehend über einen „Kill"-Befehl deaktiviert werden kann. Die permanente Deaktivierung kann mittels Durchbrennen einer Sicherung im Tag (fuse effect), Verschlüsselung des Speichers oder Entfernen des Transponders erfolgen. Die vorübergehende Deaktivierung kann mechanisch erfolgen oder mit Hilfe einer Softwaresperre. Allerdings geht bei diesem Ansatz der Vorteil eines Wiedereinsatzes der RFID-Geräte außerhalb des Geschäftes verloren. Daher wurden andere Varianten vorgeschlagen.

Eine besteht darin, die auf einem RFID-Tag gespeicherten Daten mit Nullen zu überschreiben. Der Transponder bleibt aktiv, sendet aber, wenn er „angefunkt" wird, nur Nullen anstatt einer Nummer. Mit diesem System wird der Transponder nicht wirklich deaktiviert. Er antwortet und sendet die Information, dass die betroffene Person einen „getaggten" Artikel bei sich trägt. Das kann mehrere Konsequenzen haben: Da erstens RFID-Tags, die lediglich Nullen übertragen, nicht sehr verbreitet sind, besteht die verwertbare Information in der reinen Existenz eines solchen Tags. Es zeigt, dass die betroffene Person in einem Geschäft eingekauft hat, das seine Artikel mit RFID-Tags versieht. Ein gut informiertes Unternehmen kann damit fundierte Vermutungen anstellen. Zweitens hat es den Anschein, als ob zunächst nur wertvolle Gegenstände mit RFIDTranspondern ausgestattet werden. Einige Jahre lang werden sich Diebe an der reinen Existenz eines RFID-Tags orientieren können (selbst wenn es lediglich Nullen oder unverständliche Daten überträgt), um wertvolle Gegenstände aus Garderoben oder Parkhäusern zu stehlen. Schließlich werden die Händler

[18] Entschließung zur Radio-Frequency Identification, 25. Konferenz der Datenschutzbeauftragen, Sydney 2003, http://www.privacyconference2003.org : „...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".

mit zunehmender Verbreitung der RFID-Tags, nicht unbedingt von Tags begeistert sein, die zwar antworten, dabei aber nur wertlose Daten übermitteln.

Eine andere Möglichkeit ist die physische Abschirmung des Transponders, die von der betroffenen Person bewusst eingesetzt werden kann. So können beispielsweise „getagte" Banknoten in abgeschirmten Geldbörsen nicht lokalisiert werden. Eine Alufolie in der Hülle eines RFID-Ausweises kann ausreichen, um den Inhalt zu schützen, es sei denn der Ausweis wird geöffnet. Eine Abschirmung eignet sich jedoch nicht für alle Anwendungen. So können beispielsweise Kleidungsstücke mit eingenähten RFID-Tags nicht in abschirmendes Material eingepackt werden, wenn sie getragen werden. Ferner dürfte ein solcher Ansatz einen unverhältnismäßigen Aufwand für die betroffenen Personen bedeuten, da sie letztlich allein dafür sorgen müssen, dass der Transponder keine Informationen preisgibt.

Wenn Normungsgremien, Hersteller und Anwender der RFID-Technik Verfahren zur Deaktivierung von Tags festlegen, sollten sie neben dem oben Gesagten auch berücksichtigen, dass betroffene Personen, die sich für das Entfernen des Transponders entscheiden, nicht bestraft werden sollten.

Auch in Bezug auf die oben angesprochene Problematik betont die Datenschutzgruppe, dass weitere Forschungs- und Entwicklungsanstrengungen zu diesen Problemen für alle Beteiligten unabdingbar sind.

5.4. Rechtsgrundlagen für die Verarbeitung

Deaktivierung der Transponder: Neben den in Abschnitt 5.3 genannten Gründen verlangen auch andere Bestimmungen der Datenschutzrichtlinie nach dieser Option. Wenn gemäß der Datenschutzrichtlinie die Einwilligung die einzige Rechtsgrundlage darstellt, die die Erhebung personenbezogener Daten mittels RFID-Technik rechtfertigt (vgl. Abschnitt 4.2), haben betroffene Personen natürlich immer die Möglichkeit, ihre Einwilligung zur Datenverarbeitung zu widerrufen (früher Artikel 7 Buchstabe a). Gibt es kein Gerät, mit dem eine betroffene Person den Transponder deaktivieren kann, wird sie, wenn sie die weitere Übermittlung ihrer Daten durch das Tag unterbinden will, an der Wahrnehmung ihres Rechts gehindert. Wenn auf RFID-Tags gespeicherte personenbezogene Daten auf einer anderen Rechtsgrundlage als der Einwilligung erhoben wurden, müssen diese Tags nicht unbedingt deaktivierbar sein. So wären beispielsweise für personenbezogene Daten auf Transpondern, die zur Überwachung des Zugangs zum Arbeitsplatz verwendet werden, keine Deaktivierungsvorrichtungen nötig, da die Datenverarbeitung aufgrund des Arbeitsverhältnisses gerechtfertigt ist.

Bei einigen RFID-Anwendungen, beispielsweise wenn die betroffene Person das Recht hat, ihre Einwilligung zu widerrufen oder Widerspruch gegen die Verarbeitung einzulegen (früher Artikel 14 Buchstabe a) und dementsprechend den Transponder zu deaktivieren, sollten Hersteller und Anwender der RFID-Technik sicherstellen, dass die Deaktivierung einfach durchzuführen ist. Mit anderen Worten: die betroffenen Personen sollte diese Aufgabe problemlos bewältigen können.

5.5 Datensicherheit

Verschlüsselung (Tags und Anwendungen): Enthalten RFID-Tags personenbezogene Daten müssen sie gemäß Artikel 17 Datenschutzrichtlinie über technische Maßnahmen verfügen, die eine unbefugte Offenlegung der Daten verhindern. Sonst könnte jeder, der über ein Lesegerät verfügt, einen Transponder aktivieren und die darin gespeicherten Informationen auslesen. Gemäß Datenschutzrichtlinie (früher Artikel 6 Absatz 1 Buchstabe d) sind solche Maßnahmen auch erforderlich, um die Integrität der auf dem Tag gespeicherten Daten zu gewährleisten und unautorisierte Veränderungen an den Daten zu verhindern.

Die Art der technischen Maßnahmen richtet sich nach der Art der Daten. Wie im Folgenden näher erläutert, dürfte es in den meisten Fällen genügen, dass die Daten *verschlüsselt* werden und das Lesegerät authentifiziert wird, um zu verhindern, dass Dritte mit Hilfe von Lesegeräten die Informationen auslesen. Das Beispiel der Patienten-Tags, auf denen die Identität des Patienten, des behandelnden Arztes und der vom Klinikpersonal durchzuführenden Behandlungsmethoden gespeichert sind, macht deutlich, dass die Klinik sicherstellen muss, dass diese Angaben nicht von Dritten ausgelesen werden. Daraus ergibt sich zwangsläufig die Notwendigkeit des Einsatzes technischer Maßnahmen wie der Verschlüsselung.

Die am weitesten verbreitete und sicherste Methode besteht in der Verwendung von Standard-Authentifizierungsprotokollen (z. B. ISO/IEC 9798). Sie finden bereits breite Verwendung in Netzwerken und bei Smartcards. In diesen Standardprotokollen werden kryptografische Grundelemente verwendet. Bei symmetrischen Authentifizierungsverfahren, bei denen die Schlüssel für Sender und Empfänger gleich sind, werden MACs (message authentication codes) oder symmetrische Verschlüsselungsalgorithmen wie DES oder AES verwendet. Bei den asymmetrischen Verfahren verfügt jede Partei über einen privaten (geheimen) und einen öffentlichen Schlüssel. Zum Einsatz kommen asymmetrische Verschlüsselungsalgorithmen, wie RSA oder ECC, oder Signaturen.

Einige kryptografische Authentifizierungsverfahren sind bereits in Wegfahrsperren oder bei Zugangskontrollsystemen implementiert. Sie beruhen jedoch häufig auf proprietären Algorithmen, da diese häufig einfacher und kostengünstiger zu

implementieren sind als Standardalgorithmen. Gleichwohl sollten in Fällen, in denen eine erhöhte Sicherheit erforderlich ist, wie beim Schutz sensibler Daten, Standardalgorithmen und -protokolle verwendet werden. Der Vorteil dieser Protokolle und Algorithmen besteht darin, dass sie weit verbreitet sind und von vielen Akteuren bereits getestet und erprobt wurden. Sie stoßen also in puncto Sicherheit auf breite Akzeptanz.

Einige Veröffentlichungen verweisen bereits auf symmetrische Algorithmen, wie AES, als geeignete Verschlüsselung für RFID-Etiketten[19]. Das Problem bei der Verwendung symmetrischer Authentifizierungsalgorithmen besteht darin, dass die Erzeugung und die Verwaltung des Schlüssels kompliziert sind. Asymmetrische Verfahren kennen dieses Problem nicht, sind aber teurer.

6. Fazit

Angesichts des zunehmenden Einsatzes von RFID für eine Vielzahl von Zwecken und Anwendungen von teilweise enormer Datenschutzrelevanz wählte die Datenschutzgruppe bewusst diesen Zeitpunkt, um mit diesem Arbeitspapier in die laufende Diskussion über die RFID-Problematik einzugreifen. Sie hofft, dass das Papier einen nützlichen Beitrag zu der Debatte um RFID leistet und fordert alle Interessenträger auf, sich den hier genannten Grundsätzen anzuschließen.

Das Arbeitspapier beruht auf den verfügbaren Informationen und berücksichtigt den aktuellen Stand der Technik, insbesondere die derzeitigen Einsatzgebiete in den verschiedensten Bereichen. Die Datenschutzgruppe ist sich jedoch darüber im Klaren, dass der Einsatz von RFID kontinuierlich weiterentwickelt wird: Es gibt immer wieder neue Entwicklungen und mit zunehmender Erfahrung nimmt auch das Wissen um die problematischen Aspekte zu. Aus diesem Grund wird die Datenschutzgruppe zusammen mit interessierten Gruppen die technischen Entwicklungen in diesem Bereich weiter beobachten. Einige der in dem Arbeitspapier angesprochenen Fragen müssen vielleicht im Lichte der Erfahrungen noch einmal diskutiert werden. Im Übrigen schließt die Datenschutzgruppe nicht aus, dass sie sich im Zuge der Entwicklung der RFID-Technik und ihrer Anwendungen zu einem späteren Zeitpunkt ausführlich mit spezifischen Bereichen oder Anwendungen beschäftigen und ergänzende Leitlinien zu bestimmten Anwendungen veröffentlichen wird.

---

[19] 20 Feldhofer M., Dominikus S., Wolkerstorfer J., "Strong Authentication for RFID Systems using the AES Algorithm", In the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004, 11.-13. August 2004, Boston, USA), Lecture Notes in Computer Science (LNCS) Vol. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, S. 357ff.
http://www.iaik.tugraz.ac.at/research/publications/2004/CHES2004_AES.htm

ANHANG

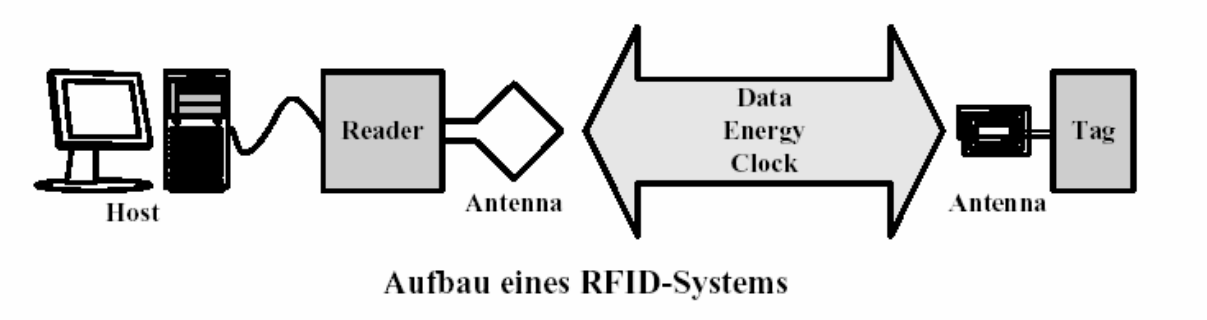
DIE RFID-TECHNIK

Die drahtlose Kommunikation schreitet immer weiter voran und ist bereits jetzt in einer Vielzahl von Anwendungen zu finden. Dazu gehören der Aufbau drahtloser lokaler Netze (WLAN) oder drahtlose Verbindungen niedriger Bandbreite zwischen einzelnen Geräten wie Laptops, PDAs, Handys usw. (Bluetooth).

In den vergangenen Jahren hat eine neue Technik immer mehr an Boden gewonnen: RFID - Radio Frequency Identification, übersetzt etwa: Funk-Erkennung. Dahinter steht vor allem die Idee, jedem Objekt, das mit einem RFID-Tag ausgestattet ist, eine eindeutige Kennung zu geben, die über Funkwellen an ein Lesegerät übermittelt werden kann. Damit ergeben sich vielfältige Anwendungsmöglichkeiten in der Lieferkette und in anderen gewerblichen Bereichen. Zunächst waren die RFID-Etiketten als Ersatz für Barcodes gedacht. Die Vorteile liegen auf der Hand: Da sie ohne Sichtkontakt funktionieren, ist eine automatische Erfassung möglich. Mit fortschreitender Entwicklung sind inzwischen noch andere, differenziertere Anwendungen denkbar. Vor der Diskussion möglicher Anwendungen soll ein Überblick über die Technik gegeben werden:

Das einfachste RFID-System besteht aus zwei Komponenten: einem Transponder (auch *Tag* oder *Etikett*), der an einem Objekt befestigt ist, und einem Lesegerät, das die Daten aus dem Transponder auslesen kann. Die beiden Komponenten kommunizieren miteinander über eine Funkverbindung. Transponder und Lesegerät besitzen eine Antenne und einen Demodulator (analoges Frontend). Dieses Frontend „übersetzt“ die per Funk ankommenden analogen Informationen in digitale Daten, die vom digitalen Teil des Lesegerätes oder des Transponders weiterverarbeitet werden können.

Im Transponder erfolgt die digitale Verarbeitung entweder mittels gezielt entwickelter Hardware oder mittels eines Mikroprozessors. Zur Verarbeitung der aus den Tags ausgelesenen Daten kann ein an das Lesegerät angeschlossener Server verwendet werden. Dieser Server muss unter Verwendung der Tag-Daten besondere Anwendungen ausführen können. Das Schaubild zeigt ein gängiges RFID-System:



Aufbau eines RFID-Systems

Ein RFID-System kann durch verschiedene technische Parameter beschrieben werden. Diese Parameter bestimmen die unterschiedlichen Anwendungsmöglichkeiten von RFID-Systemen.

Aktive/passive RFID-Tags. Einfache passive Tags beziehen ihre Energie und das Taktsignal zur Verarbeitung und Übermittlung der Daten über das elektromagnetische Feld des Lesegerätes. Die Stärke dieses Feldes ist durch nationale und internationale Vorschriften begrenzt. Daher muss der Energieverbrauch des Tags begrenzt werden, um ein einwandfreies Funktionieren zu gewährleisten. Die Feldstärke nimmt mit der Entfernung zum Lesegerät ab. Kommt der Tag mit weniger Energie aus, hat das Lesegerät folglich eine größere Reichweite, sprich: Lesegerät und Tag können über eine größere Entfernung miteinander kommunizieren. Aktive Tags übermitteln Daten, auch wenn kein Lesegerät vorhanden oder in Reichweite ist. Aus diesem Grund besitzen sie eine Batterie. Der Vollständigkeit halber sollte erwähnt sein, dass einige Tags Prüf- oder Messschaltungen enthalten können, die bestimmte Werte aufnehmen; das kann beispielsweise ein Thermometer sein, das die Unterbrechung der Kühlkette feststellen soll; in diesen Fällen ist ebenfalls eine Batterie erforderlich, die allerdings unabhängig von der Art des Tags (aktiv oder passiv) ist.

Betriebsfrequenz: RFID-Systeme können mit unterschiedlichen Frequenzen, Reichweiten und Kopplungsarten arbeiten. Diese Parameter hängen stark voneinander ab. Die Frequenzen reichen von 135 kHz bis 5,8 GHz. Hier sind internationale Beschränkungen sowie physikalische Erfordernisse zu berücksichtigen. Die Kopplungsverfahren können elektrisch, magnetisch oder elektromagnetisch sein. Die Kopplung beeinflusst die Reichweite, die sich zwischen wenigen Millimetern bis zu 15 Metern und mehr bewegen kann. Insbesondere können unterschieden werden:

- ✓ So genannte „Close-Coupling-Systeme“ mit einer kurzen Reichweite von maximal einem Zentimeter. Ihre Arbeitsfrequenz reicht vom Niederfrequenzbereich bis 30 MHz. Tags dieser Art müssen in oder auf das Lesegerät gelegt werden, damit sie kommunizieren können. Diese Systeme können mit hohem Energieverbrauch und hoher Datenübertragungsrate arbeiten.

- ✓ „Remote-Coupling-Systeme“ mit einer Reichweite von bis zu einem Meter. Die meisten RFID-Systeme arbeiten mit Remote-Coupling auf Frequenzen zwischen 135 kHz und 13,56 MHz.

- ✓ „Long-Range-Systeme“ mit einer Reichweite von mehr als einem Meter. Sie arbeiten auf Frequenzen zwischen 868 MHz und 5,8 GHz.

  RFID-Systeme können andere Funkeinrichtungen stören. Daher müssen sie auf anderen Frequenzen arbeiten als Hörfunk, Fernsehen oder mobile Funkstationen. Vorwiegend arbeiten RFID-Systeme auf Frequenzen zwischen 0 und 135 kHz, ferner auf den ISMFrequenzen (Industrial, Scientific, Medical) von 6,78 MHz, 13,56 MHz, 27,125 MHz, 40,68 MHz, 869,0 MHz, 2,45 GHz, 5,8 GHz und 24,125 GHz.

Lese-/Schreibfunktion: Die Komplexität von RFID-Systemen variiert und ist häufig begrenzt durch die Leistungsfähigkeit des Tags.

- ✓ So genannte „Low-end-Systeme“ haben lediglich lesbare Tags. Das Lesegerät kann nur den Inhalt des Tags auslesen, der normalerweise aus einer Seriennummer mit wenigen Bytes besteht. Diese Tags werden häufig eingesetzt, weil sie kostengünstig sind und nur einen kleinen Chip benötigen. Sie können Barcode-Systeme ersetzen, wo immer Objekte lokalisiert werden müssen, üblicherweise bei der Lagerlogistik oder beim Produkt-Routing in einem Produktionsprozess. Auch die Lokalisierung von Tieren ist mit solchen Tags möglich.

- ✓ RFID-Systeme mittlerer Leistungsfähigkeit können Tags mit wieder beschreibbarem Speicher haben. Die Speicherkapazität schwankt derzeit zwischen wenigen Bytes und einigen zehn oder hundert Kilobyte EEPROM[20] für passive und SRAM[21] für aktive Transponder. In diesem Leistungsspektrum können auch (Temperatur-, Druck- usw.) Sensoren in die Transponder integriert werden, die dann Umweltunfälle erfassen, die der Transponder aufzeichnet. Darüber hinaus können solche Tags für Zugangskontrollen eingesetzt werden. Ein weiteres, bereits erprobtes Einsatzgebiet ist das Gepäck-Routing auf Flughäfen. Der Bestimmungsort des Gepäckstückes wird auf dem Tag gespeichert und das Gepäckstück wird automatisch weitergeleitet. Auch im Gesundheitswesen ist der Einsatz von Transpondern vorstellbar. Im Klinikbetrieb können Einzelheiten der Behandlung oder bestimmte Werte über den Gesundheitszustand des Patienten auf dem Tag gespeichert werden.

[20] Electrically Erasable Programmable Read Only Memory (digitaler Festwertspeicher, in dem Daten gelöscht und neu geschrieben werden können).

[21] Static Random Access Memory (statischer Speicher mit wahlfreiem Zugriff).

- ✓ Berührungslose Smartcards mit einem Mikroprozessor und einem Betriebssystem bilden so genannte High-End-Systeme. Sie verfügen über eine gewisse Speicherkapazität, die im Allgemeinen höher ist als bei RFID-Transpondern des mittleren Leistungsspektrums. Auf der Karte können komplexe Funktionen implementiert werden. Im Transponder können Programme gespeichert und dann vom Mikroprozessor ausgeführt werden. Aufgrund des hohen Energieverbrauchs dieser Karten ist die Reichweite solcher Systeme derzeit noch auf wenige Zentimeter begrenzt. Mit diesen Karten können komplexere Anwendungen realisiert werden. Eine typische Smartcard-Anwendung ist beispielsweise die Zugangskontrolle. Ferner können Sie als Ausweis oder als Krankenversicherungskarte verwendet werden. Diskutiert wird auch der Einsatz solcher High-End-RFID-Systeme in Reisepässen mit IC-Chip[22], wie von der Internationalen Zivilluftfahrtorganisation (ICAO) definiert, oder als Visa und Aufenthaltsgenehmigungen mit IC-Chip.

Brüssel, 19. Januar 2005

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR

[22] Integrated Circuit Chip

Arbeitspapier „Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten“ (WP 104)

Angenommen am 18. Januar 2005

I. Hintergrund

Die Datenschutzgruppe stellt fest, dass der aufgrund der Entwicklung des Internet zunehmende Informationsaustausch immer stärker die heikle Frage der Kontrolle über die Nutzung urheberrechtlich geschützten Materials berührt. Dabei geht es insbesondere um die Rechte und Pflichten von Akteuren, die ein Interesse an urheberrechtlich geschütztem Material haben und mit der Verwaltung digitaler Rechte befasst sind.

Die Datenschutzgruppe weiß einerseits um die Notwendigkeit von Maßnahmen, mit denen die berechtigten Interessen der Inhaber von Immaterialgüterrechten (Rechte des geistigen Eigentums) vor mutmaßlichem Betrug geschützt werden können. Andererseits hat die Datenschutzgruppe festgestellt, dass einige dieser Maßnahmen, die von den Urheberrechtsinhabern auf verschiedenen Ebenen ergriffen wurden, um den unrechtmäßigen Austausch urheberrechtlich geschützten Materials wirksam zu verhindern, die Verarbeitung personenbezogener Daten beinhalten. Zuerst möchte sich die Datenschutzgruppe mit der digitalen Rechteverwaltung (*Digital Rights Management – DRM*) befassen, die sich derzeit entwickelt; dabei geht es ihr konkret darum, dass DRM die Identifizierung und Nachverfolgung von Einzelpersonen ermöglichen, die über das Internet auf gesetzlich geschütztes Material zugreifen (zum Beispiel auf Musikaufnahmen oder Software). Anschließend geht die Datenschutzgruppe auf die Möglichkeiten der Urheberrechtsinhaber ein, ihre Rechte gegenüber Einzelpersonen durchzusetzen, die im Verdacht der Urheberrechtsverletzung stehen.

Dieses Papier beleuchtet die unterschiedlichen Niveaus, auf denen sich Datenschutzfragen ergeben; es fasst die wesentlichen Rechtsgrundsätze zusammen, die nicht nur von den Urheberrechtsinhabern bei der Ausübung ihrer Rechte zu beachten sind, sondern auch von anderen Akteuren, die in besonderer Weise mit der digitalen Rechteverwaltung zu tun haben, beispielsweise die betroffenen Wirtschaftszweige und Dienstanbieter, die Technologie zur digitalen Rechteverwaltung anbieten.

a. Digitale Rechteverwaltung

Zur Entwicklung der digitalen Rechteverwaltung merkt die Datenschutzgruppe an, dass sich neue Technologien zur Identifizierung und/oder Nachverfolgung von Benutzern sowohl auf der Informationsaustauschebene als auch auf der Plattformebene durchsetzen (d. h. Überprüfung von Hardware/Software).

Beim Austausch bzw. Herunterladen urheberrechtlich geschützten Materials im Internet wird der Zugang zu diesem Material immer häufiger von einer vorherigen Überprüfung der Identität des Benutzers abhängig gemacht; außerdem wird die Nutzung des Materials anschließend mittels Etiketten (*tags*) oder digitalen Wasserzeichen weiterverfolgt. Beispiel: Ein Benutzer muss sich häufig identifizieren, bevor er ein Musikstück eines offiziellen Anbieters herunterladen kann; sein Profil wird dabei um Informationen aus der eindeutigen Kennung ergänzt, die in jedem heruntergeladenen Musikstück enthalten ist. Neben dem erklärten Zweck der Kontrolle der individuellen Nutzung des Materials im Einklang mit DRM wird die Kennzeichnung oft auch zur Erstellung von Benutzerprofilen und zur gezielten Werbung verwendet. Die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation stellte dazu fest: „Elektronische Copyright-Management-Systeme (ECMS), die zur allgegenwärtigen Überwachung von Nutzern digitaler Werke führen könnten, werden entwickelt und angeboten. Einige ECMS überwachen jede einzelne Handlung des Lesens, Anhörens und Betrachtens im Internet durch individuelle Nutzer, wobei hoch sensible Informationen über die Betroffenen gesammelt werden“[1].

Auf der Plattformebene verfolgt die Datenschutzgruppe bereits eingehend die Entwicklung einiger Industrieprojekte, z. B. TCG, die darauf abstellen, die Vertrauenswürdigkeit von Informationen zu gewährleisten, die in einer Computerplattform enthalten sind bzw. auf die von einer Computerplattform aus zugegriffen wird. Wenngleich solche Systeme sich sehr positiv auf den Grad der Informationssicherheit auswirken können, was die Datenschutzgruppe bereits eingeräumt hat, so sind deren Anwendungsmöglichkeiten doch sehr vielfältig. Die Bestandteile von Computerplattformen könnten durchaus von außen auf die Beachtung von Urheberrechten hin überprüft werden. Die Datenschutzgruppe hat in ihrem Arbeitspapier WP 86 vom 23. Januar 2004 bereits darauf hingewiesen, dass TPM-basierte Anwendungen z. B. auch von der Contentindustrie eingesetzt werden könnten, „um die Kontrolle über Verbreitung und Nutzung von digitalem Content (einschließlich Software) zurückzugewinnen, die sie mit dem Aufkommen von Internet und Peer-to-Peer-Anwendungen verloren hat“. Derartige Kontrollen könnten bei jeder Kontaktaufnahme zwischen Plattformen routine-

[1] Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: „Gemeinsamer Standpunkt - Datenschutz und Urheberrechts-Management“, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000.

mäßig erfolgen, denn „der von einer derart starken Vertretung der Industrie propagierte TPM-Einsatz dürfte zum De-facto-Standard werden, zu einer notwendigen Voraussetzung für die Teilhabe an der Informationsgesellschaft".

b. Durchsetzung von Urheberrechten

Einerseits wird an der Quelle auf Kontrolle und Nachverfolgung gesetzt in dem Bestreben, jeden Benutzer, der Material rechtmäßig aus dem Internet herunterlädt, „im Vorfeld" zu überprüfen; andererseits führt der Urheberrechtsschutz dazu, dass die meisten betroffenen Akteure auch Maßnahmen „im Nachfeld" ergreifen und Ermittlungen gegen mutmaßliche Rechtsverletzer durchführen.

Die Rechteinhaber setzen dabei unterschiedliche Instrumente ein; die Folgenden möchte die Datenschutzgruppe besonders hervorheben:

Häufig wird auf Internet-gestützte Peer-to-Peer-Instrumente zurückgegriffen, um Informationen über Einzelpersonen zu gewinnen, die geschütztes Material online bereitstellen oder herunterladen.

Die Rechteinhaber erfassen bei ihren Recherchen in der Regel die IP-Adressen der Benutzer[2]. Diese Informationen werden dann mit den Benutzerdaten der Internetdienstanbieter (*ISP*) verknüpft. In manchen Fällen verlangen die Rechteinhaber von den Internetdienstanbietern direkt die Preisgabe der Benutzeridentität, um die Benutzer schriftlich abzumahnen. In anderen Fällen fordern die Rechteinhaber die Internetdienstanbieter auf, die betreffenden Benutzer schriftlich zur Entfernung des mutmaßlich rechtsverletzenden Materials aufzufordern oder ihnen den Netzzugang zu sperren.

In welchem Umfang Rechteinhaber Zugang zu detaillierten Benutzerinformationen erhalten, ist von Land zu Land unterschiedlich. In Belgien fordern die Rechteinhaber die Internetdienstanbieter auf, Warnungen an die Benutzer zu richten. In den Vereinigten Staaten wurden die Internetdienstanbieter aufgefordert, der Musikindustrie die Identität ihrer Kunden ohne richterliche Anordnung *direkt* mitzuteilen[3]. In anschließenden Gerichtsentscheidungen (siehe Rechtssache Ve-

[2] Noch vor wenigen Jahren wurden vielen Benutzern dynamische Adressen zugewiesenen, die sich beim Aufbau einer Internetverbindung stets änderten. Kabelanschlüsse und ADSL bringen mit sich, dass den Benutzern permanente IPAdressen zugewiesen werden. Permanente IP-Adressen, die mit dem neuen Internetprotokoll IPv6 zum Standard werden könnten, machen die Nachverfolgung von Internetnutzern noch einfacher (siehe dazu die Stellungnahme 2/2002 der Datenschutzgruppe vom 30. Mai 2002: „Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6", 10750/02/DE, WP 58).

[3] Dabei beriefen sich die Rechteinhaber auf Section 512 der Digital Millennium Copyright Act bezüglich Haftungseinschränkungen im Zusammenhang mit Online-Material. Diese

rizon vom Dezember 2003) stellten die Gerichte allerdings fest, dass die direkte Übermittlung von Daten an Rechteinhaber als rechtswidrig anzusehen ist. Ein anderes Beispiel liefert das australische Recht mit der als „*Anton Piller Order*" bekannten Verfügung; diese ermöglicht die Erhebung von Beweismitteln, einschließlich Hausdurchsuchungen, durch private Akteure, beispielsweise die Inhaber von Immaterialgüterrechten.

Um mutmaßliche Rechtsverletzungen auf die verantwortlichen Benutzer zurückführen und die Profile der Benutzer ergänzen zu können, versuchen die Rechteinhaber, bestehende öffentliche Register wie „Whois"-Datenbanken zu nutzen, in denen Angaben zu Personen gespeichert sind, die einen Domainnamen haben registrieren lassen. Sie enthalten vornehmlich Informationen über den dem Domainnamen zugehörigen Ansprechpartner, darunter Name, Telefonnummer, E-Mail- Adresse und sonstige personenbezogene Daten. Auf einige Angaben kann direkt online zugegriffen werden, andere sind offline gespeichert und müssen somit bei der für die Datenbank verantwortlichen Stelle abgerufen werden.

Schließlich sei noch Folgendes angemerkt: Die Erhebung personenbezogener Daten durch Rechteinhaber ist an bestimmte Datenschutzgrundsätze gebunden; vor diesem Hintergrund stellt die Datenschutzgruppe fest, dass Erörterungen mit Interessenträgern in mehreren Ländern im Gange sind, die darauf abzielen, ihnen mehr Spielraum bei der Verarbeitung personenbezogener Daten einzuräumen. So enthält das französische Datenschutzgesetz beispielsweise jetzt eine Ausnahmeregelung, die einigen gesetzlich bestimmten[4] Rechteinhabern erlaubt, unter gewissen Voraussetzungen und mit vorheriger Genehmigung der französischen Datenschutzbehörde[5] Strafverfolgungsdaten zu verarbeiten.

Vorschriften ermöglichen es einem Urheberrechtsinhaber oder seinem Vertreter, bei einem Bundesgericht eine Verfügung gegen einen Internetdienstanbieter zu erwirken, der dann die Identität eines Benutzers preisgeben muss, der urheberrechtsverletzender Handlungen verdächtigt wird. Dieses Verfahren ist recht flexibel, da auf diesem Wege personenbezogene Daten des Benutzers beschafft werden können, ohne ein ordentliches Gerichtsverfahren einleiten zu müssen.

4 Die Ausnahme gilt für die in Artikel L 321-1 und L 331-1 des Urheberrechtsgesetzes erschöpfend aufgeführten Rechtspersönlichkeiten und dient dem Interessenschutz der Rechteinhaber.

5 Die Nationale Kommission für Informatik und Freiheiten (CNIL) hat die Art der in den Dateien enthaltenen Strafverfolgungsdaten sowie deren Speicherfrist genauer auszuführen. Ferner muss sie sicherstellen, dass eine derartige Verarbeitung angemessen ist und nicht über das zur Bekämpfung betrügerischer Nachahmung unbedingt nötige Maß hinausgeht (Entscheidung des „Verfassungsrats" Nr. 2004-499 DC, 29. Juli 2004). Der Verfassungsrat vertritt übrigens die Auffassung, dass das Identifizieren von Benutzern mittels ihrer IP-Adresse nur im Rahmen eines gerichtlichen Verfahrens zulässig ist.

Die Datenschutzgruppe muss in diesem sich wandelnden Kontext an die wesentlichen Datenschutzgrundsätze erinnern und darlegen, in welchem Maße sie für die digitale Rechteverwaltung und die Durchsetzung von Urheberrechten gelten.

II. Die Verwaltung von Immaterialgüterrechten

Wenn Rechteinhaber den berechtigten Zweck verfolgen, den Missbrauch urheberrechtlich geschützten Materials zu verhindern, bringt dies häufig die Nachverfolgung von Benutzern und die Überwachung ihrer Präferenzen mit sich. Vor allem die Verwendung eindeutiger Kennungen in Verbindung mit den gesammelten personenbezogenen Daten mündet in die Verarbeitung detaillierter personenbezogener Daten. Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten stellten mehrere Grundsätze auf, die von einem Rechteinhaber beachtet werden müssen, wenn personenbezogene Daten verarbeitet werden. Artikel 2 Absatz 3 Buchstabe a der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums verweist darauf, dass sie die Richtlinie 95/46/EG nicht berührt und folglich die Datenschutzgrundsätze zu beachten sind.

Dieses Papier konzentriert sich auf den Grundsatz der Notwendigkeit, ferner auf die Notwendigkeit des anonymen Zugangs zu Netzdiensten, auf den Grundsatz der Transparenz, die Vereinbarkeit der Zweckbestimmungen und die Beschränkungen hinsichtlich der Speicherung von Daten.

- Grundsätze der Notwendigkeit und der Anonymität

Die Datenschutzgruppe bekräftigt erneut die Notwendigkeit, Transaktionen im Internet anonym oder pseudonym durchführen zu können. Diesen Grundsatz hat die Datenschutzgruppe mehrfach ausgeführt[6], erstmalig in ihrer Empfehlung vom 3. Dezember 1997, worin die Datenschutzgruppe bereits feststellte, dass die Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten im Internet ebenso einzuhalten seien wie bei der Offline-Verarbeitung. Auch die Internationale Arbeitsgruppe vertritt die Ansicht, „dass die Nutzer generell die Möglichkeit haben sollten, auf das Internet ohne Preisgabe ihrer Identität zuzugreifen, sofern personenbezogene Daten nicht für die Erbringung eines bestimmten Dienstes erforderlich sind“[7]. Dieser Grundsatz wird von dem Notwendigkeitsgrundsatz in Artikel 6 Buchstabe c der Datenschutzrichtlinie untermauert; da-

[6] Empfehlung 3/97 „Anonymität auf dem Internet“, angenommen am 3.12.1997, WP 6; Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet, angenommen am 23. Februar 1999, 5013/99/DE/endg., WP 16; Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware, angenommen am 23. Februar 1999, 5093/98/DE/endg., WP 17;

[7] Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation, a.a.O., S. 2.

nach muss sichergestellt werden, dass die personenbezogenen Daten „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“

Diesbezüglich betont die Datenschutzgruppe, dass bei der Verwendung von DRM-Technologien zum Schutz eines bestimmten Materials Instrumente eingesetzt werden sollten, die die Anonymität des Benutzers wahren. Daher sollten datenschutzfreundliche Technologien bei der Entwicklung dieser neuen Instrumente größere Beachtung finden.

- Verwendung eindeutiger Kennungen

Die Verwendung eindeutiger Kennungen ermöglicht die Verknüpfung von Daten zu einer bestimmten Person und erleichtert das Erstellen von Profilen. Bei der digitalen Rechteverwaltung ermöglichen diese Kennungen die Erstellung von Benutzerprofilen anhand von Art und Menge des abgerufenen Materials. Beispiel: Ein Anbieter von Rechtsinhalten kann den Weg von Dateien, die ein digitales Wasserzeichen in Form einer eindeutigen Kennung tragen, innerhalb von Peer-to-Peer-Netzen verfolgen und den Benutzer ausfindig machen, der das Material ursprünglich rechtmäßig heruntergeladen und gegebenenfalls anschließend mutmaßlich rechtswidrig weiterverwendet hat. Auch am Arbeitsplatz hätte die Musik- oder Filmwirtschaft die Möglichkeit, die Benutzung des angebotenen urheberrechtlich geschützten Materials durch ihre Mitarbeiter nachzuverfolgen. Die Datenschutzgruppe stellt die Nutzung von Kennungen ernstlich in Frage, die der Verfolgung aller Benutzer im Vorfeld dient und darauf abstellt, im Falle eines mutmaßlichen Urheberrechtsmissbrauchs eine bestimmte Person herauszufiltern. Die Etikettierung von Material sollte nicht mit der Identität einer Einzelperson verknüpft werden, es sei denn, die Verknüpfung ist zur Erbringung der Dienstleistung erforderlich oder die Einzelperson wurde darüber informiert und hat dem zugestimmt.

- Information des Betroffenen

Wie die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation betont hat, sollte für größtmögliche Transparenz beim Betrieb der Copyright-Management-Systeme gesorgt werden. Gemäß Artikel 10 der Richtlinie 95/46/EG dürfen personenbezogene Daten nur dann erhoben werden, wenn der betroffenen Person bestimmte Auskünfte erteilt werden, dazu zählen vornehmlich die Identität des für die Verarbeitung Verantwortlichen, der Verarbeitungszweck, die Empfänger oder Empfängerkategorien der Daten sowie das Bestehen von Auskunfts- und Berichtigungsrechten.

Diese Informationen sollten gut sichtbar angezeigt werden, bevor der Benutzer personenbezogene Daten bereitstellt oder gekennzeichnetes Material herunterlädt[8].

- Zweckbindungsgrundsatz (Vereinbarkeit)

Personenbezogene Daten, die beim Benutzer auf freiwilliger Basis erhoben wurden oder die zur Erbringung der Dienstleistung erforderlich sind, sollten grundsätzlich nur zum angegebenen Zweck verwendet werden, so wie es in Artikel 6 Absatz 1 Buchstabe b der Richtlinie ausgeführt wird. Beispiel: Bei einer Kreditkartentransaktion ist es nicht zulässig, Name und Adresse des Benutzers zu erfassen, um die Daten anschließend für das Direktmarketing zu verwenden, nachdem sie mit Benutzerpräferenzen verknüpft wurden, die aus heruntergeladenem, digital gekennzeichnetem Material gewonnen wurden. Auch gemäß Artikel 13 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sind derartige Profile und die Vermarktung personenbezogener Daten nur bei vorheriger Einwilligung der Betroffenen gestattet. Derselbe Grundsatz gilt auch für die etwaige Übermittlung der personenbezogenen Daten an Dritte. Die Datenschutzgruppe unterstreicht ferner, dass die Sammlung von Daten über Konsumgewohnheiten die Verarbeitung sensibler Daten nach sich ziehen kann, wenn Benutzerprofile aus der Art der abgerufenen Informationen zusammengestellt werden (z. B. beim Herunterladen eines Buches über religiöse oder politische Fragen). Eine derartige Verarbeitung darf nur unter strenger Einhaltung der Bestimmungen von Artikel 8 der Richtlinie 95/46/EG erfolgen.

- Befristete Speicherung personenbezogener Daten

Gemäß Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG müssen personenbezogene Daten in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Alle personenbezogenen Daten, die bei der Lieferung urheberrechtlich geschützten Materials oder bei der Erbringung einer urheberrechtlich geschützten Dienstleistung erfasst wurden, müssen daher unverzüglich gelöscht werden, sobald der Bedarfszweck entfallen ist, dieser Bedarfszweck kann die Rechnungsstellung sein oder die Erfüllung eines Zwecks, in den der Benutzer eingewilligt hat, z. B. die Pflege einer Geschäftsbeziehung. Es wäre mit diesem Rechtsgrundsatz unvereinbar, wenn grundsätzlich alle Benutzerdaten gespeichert würden, weil die

[8] Siehe Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, angenommen am 17. Mai 2001, 5020/01/DE/endg, WP 43.

Möglichkeit besteht, dass ein bestimmter Benutzer urheberrechtlich geschütztes Material missbräuchlich verwendet.

III. Ausmaß der Ermittlungsbefugnisse

Abgesehen von der Entwicklung technischer Schutzvorkehrungen, die auf die Etikettierung und die Nachverfolgung urheberrechtlich geschützten Materials abstellen, leiten Urheberrechtsinhaber seit einigen Jahren auch konkrete rechtliche Schritte gegen mutmaßliche Urheberrechtsverletzer ein. Dazu müssen - wie in Abschnitt I b dargelegt - Daten über Verdächtige gesammelt werden, was mit unterschiedlichen Mitteln und unter Verwertung unterschiedlicher öffentlich oder nicht öffentlich zugänglicher Quellen geschehen kann.

Zwar ist eine derartige Verarbeitung von Daten zweifellos rechtlich zulässig, wenn sie im Rahmen eines eigenen Rechtsstreits erfolgt, die Verfahren zur Datensammlung und die Art der erfassten Daten unterliegen aber datenschutzrechtlichen Regelungen; diesbezüglich sind folgende Grundsätze zu beachten:

- Grundsatz der Vereinbarkeit

Rechteinhaber konzentrieren sich bei ihren Nachforschungen in erster Linie auf online gewinnbare Fakten, z. B. die Darstellung urheberrechtlich geschützten Materials in Peer-to-Peer-Netzen. Auf Angaben wie das Datum und die Uhrzeit einer etwaigen Rechtsverletzung, die Art des geschützten Materials und auf indirekte Identifikationsmerkmale, z. B. Pseudonyme des möglichen Rechtsverletzers, lässt sich zugreifen. Somit ist die Versuchung groß, diese Sammlung personenbezogener Daten um weitere Angaben zu ergänzen, die sich unter Mithilfe des Internet- Dienstanbieters oder aus anderen Datenbanken, z. B. den Whois-Datenbanken mit Angaben über die Inhaber von Domänennamen, gewinnen lassen.

Die Datenschutzgruppe weist nachdrücklich auf die rechtlichen Beschränkungen hin, denen die Weiterverwendung personenbezogener Daten unterliegt. Der Inhalt von Datenbanken darf – unabhängig davon, ob sie öffentlich und nicht öffentlich sind, – nur für Zwecke verarbeitet und weiterverwendet werden, die mit der ursprünglichen Zweckbestimmung vereinbar sind. Zur Whois-Datenbank stellte die Datenschutzgruppe bereits in ihrer Stellungnahme vom 13. Juni 2002[9] fest: „Aus dem Blickwinkel des Datenschutzes muss unbedingt klar festgelegt werden, was die eigentliche Zweckbestimmung von Whois ist und welche Zwecke als rechtmäßig anzusehen sind und als mit der eigentlichen Zweckbestimmung vereinbar. […] Dies ist eine außerordentlich heikle Angelegenheit, da es

[9] Stellungnahme 2/2003 zur Anwendung der Datenschutzgrundsätze auf die Whois-Verzeichnisse, 10972/03/DE endg., WP 76.

nicht angehen kann, dass die Zweckbestimmung der Whois-Verzeichnisse einfach nur deshalb auf andere Zwecke ausgedehnt wird, weil dies von einigen potenziellen Benutzern der Verzeichnisse als wünschenswert angesehen wird. Einige Zwecke, die Datenschutzprobleme (Vereinbarkeit) hervorrufen könnten, sind beispielsweise die Nutzung der Daten durch privatwirtschaftliche Akteure bei der Selbstkontrolle im Zusammenhang mit mutmaßlichen Verstößen gegen ihre Rechte, z. B. auf dem Gebiet der Verwaltung digitaler Rechte (Digital Rights Management)."

Der Vereinbarkeitsgrundsatz und die Beachtung des Vertraulichkeitsgrundsatzes der Richtlinien 2002/58/EG und 95/46/EG verbieten, dass Datenbestände der Internetdienstanbieter, die zu bestimmten Zwecken verarbeitet werden und im Wesentlichen auch die Leistung eines Telekommunikationsdienstes betreffen, an Dritte weiterübermittelt werden, z. B. an Rechteinhaber; davon ausgenommen sind unter klaren gesetzlichen Voraussetzungen die Strafverfolgungsbehörden.

- Aufgaben der Internetdienstanbieter

Die Datenschutzgruppe erinnert daran, dass die Internetdienstanbieter gemäß Artikel 15 der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr nicht systematisch zur Überwachung oder Zusammenarbeit verpflichtet sind.

Internetdienstanbieter müssen außerdem nur in bestimmten Fällen, in denen eine Verfügung der Strafverfolgungsbehörden vorliegt, für eine generelle vorherige Speicherung urheberrechtlich relevanter Verkehrsdaten sorgen. Dazu stellte die Datenschutzgruppe mehrfach[10] fest: „Wenn in besonderen Fällen Verkehrsdaten aufbewahrt werden sollen, muss eine beweisbare Notwendigkeit vorliegen und die Zeitdauer der Aufbewahrung muss so kurz wie möglich sein; weiterhin muss die diesbezügliche Praxis gesetzlich in einer Weise klar geregelt sein, die ausreichenden Schutz gegen unrechtmäßigen Zugang und anderweitigen Missbrauch bietet."

- Verarbeitung von Strafverfolgungsdaten

Gemäß Artikel 8 Absatz 5 der Datenschutzrichtlinie darf die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, nur unter strengen, von den Mitgliedstaaten festgelegten Voraussetzungen erfolgen. Wenngleich dem Einzelnen zweifelsohne das Recht zusteht, Strafverfolgungsdaten im Rahmen eines eigenen Rechtsstreits zu verarbeiten, so

[10] Vgl. 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, 11818/02/DE/endg., WP 64.

geht der Grundsatz doch nicht so weit, dass er die gründliche Ermittlung, Erfassung und Zentralisierung personenbezogener Daten durch Dritte erlauben würde, wozu auch generelle systematische Ermittlungen wie das Durchforsten des Internet (Internet-Scanning) zählen oder die Anforderung personenbezogener Daten aus den Beständen anderer Akteure, z. B. Internetdienstanbieter oder Stellen, die für die Verarbeitung von Wohis-Verzeichnissen verantwortlich sind. Derartige Ermittlungen sind Sache der Strafverfolgungsbehörden.

Diesbezüglich stellt die Datenschutzgruppe fest, dass die kürzlich verabschiedete Richtlinie 2004/48/EG vom 28. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums Bedingungen nennt, unter denen personenbezogene Daten von den Strafverfolgungsbehörden angefordert werden. Diese Behörden können auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag hin anordnen, dass Auskünfte über den Ursprung und die Vertriebswege von immaterialgüterrechtsverletzenden Waren oder Dienstleistungen erteilt werden, wenn die Rechtsverletzung in gewerblichem Ausmaß erfolgte und wenn dabei die Grundsätze beachtet werden, die die Vertraulichkeit der Informationsquellen oder die Verarbeitung personenbezogener Daten betreffen. Es gilt, einen gerechten Ausgleich zwischen den legitimen Interessen der betroffenen Urheberrechtsinhaber und Einzelpersonen zu finden. Das Kriterium des wirtschaftlichen Vorteils aus der Rechtsverletzung kann in dieser Hinsicht entscheidend sein.

IV. Fazit

Die Datenschutzgruppe stellt mit Besorgnis fest, dass die rechtmäßige Nutzung von Technologien zum Schutz urheberrechtlich geschützter Werke den Schutz personenbezogener Daten beeinträchtigen könnte. Die Anwendung der Datenschutzgrundsätze auf die digitale Rechteverwaltung lässt erkennen, dass der Schutz des Einzelnen in der Offline-Welt und der Schutz des Einzelnen in der Online-Welt immer stärker auseinanderklaffen, besonders vor dem Hintergrund genereller Nachverfolgung und Profilerstellung. Die Datenschutzgruppe fordert die Entwicklung datenschutzgerechter technischer Instrumente, und ganz allgemein die transparente und begrenzte Nutzung eindeutiger Kennungen, die dem Benutzer eine Wahlmöglichkeit zugestehen.

Im Hinblick auf die Ermittlungsbefugnisse muss die Datenschutzgruppe daran erinnern, dass sich private Akteure, z. B. Urheberrechtsinhaber, bei Ermittlungen wie oben erläutert in einem klaren Rechtsrahmen bewegen müssen; dies gilt in besonderem Maße für die Frage, welche Informationen rechtmäßig erfasst werden dürfen und welche Durchsetzungsbefugnisse diesen Akteuren eingeräumt werden können.

Brüssel, den 18. Januar 2005

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR

IV. Internationale Konferenz der Datenschutzbeauftragten

Entschließungen der 27. Konferenz vom 14. - 16. September 2005 in Montreux (Schweiz)

Erklärung von Montreux: „Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. Entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung,

2. Erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschließung über den Datenschutz und die internationalen Organisationen,

3. Stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmassnahmen beherrscht wird,

4. Sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt,

5. Verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien,

6. Sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt,

7. Sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten

überhaupt werden können, und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt,

8. Erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen,

9. Anerkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann,

10. Sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft ist,

11. Sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist,

12. Sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen,

13. Sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen,

14. Erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat,

15. Erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten Zehn Geboten zum Schutz der Privatheit Rechnung zu tragen,[1]

[1] http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm

16. Anerkennen, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC),

17. Erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:

    - Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
    - Prinzip der Richtigkeit,
    - Prinzip der Zweckgebundenheit,
    - Prinzip der Verhältnismäßigkeit,
    - Prinzip der Transparenz,
    - Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
    - Prinzip der Nicht-Diskriminierung,
    - Prinzip der Sicherheit,
    - Prinzip der Haftung,
    - Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,3
    - Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierungen und den internationalen und supranationalen Organisati-

onen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragten

a. die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;

b. sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäß den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;

c. den Europarat, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern;

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16.-18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a. die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzuhalten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;

b. die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von

Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;

c. die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten.

Die Datenschutzbeauftragten kommen außerdem überein

a. namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschließungen der Konferenz zu verstärken;

b. die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;

c. den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;

d. mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;

e. eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschließt:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zur Zeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

Wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

Unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

Im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar" machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

1. wirksame Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technische Beschränkung der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

Resolution zur Verwendung von Personendaten für die politische Kommunikation

Die Konferenz

In Erwägung, dass politische Kommunikation ein grundlegendes Instrument für die Beteiligung der Bürgerinnen und Bürger, der politischen Kräfte und der Kandidatinnen und Kandidaten am Leben einer Demokratie ist, und in Anerkennung der Wichtigkeit der Freiheit der politischen Meinungsäußerung als ein Grundrecht;

In Erwägung, dass gelebte Staatsbürgerschaft das Recht der Bürgerinnen und Bürger voraussetzt, im Rahmen von Wahlkampagnen von Politik und Verwal-

tung Informationen zu erhalten und angemessen informiert zu werden; in Erwägung, dass diese Rechte auch geeignet sind, um bei weiteren Themen, Ereignissen und politischen Positionen in Kenntnis der Sachlage seine Wahl zu anderen Themen des politischen Lebens treffen zu können, sei es bei Referenden, bei der Wahl von Kandidatinnen und Kandidaten oder beim Zugang zu Informationen innerhalb politischer Organisationen oder von gewählten Amtsträgern;

In Erwägung, dass sich die politischen Kräfte und politische Organisationen im Allgemeinen sowie gewählte Abgeordnete verschiedener Formen der Kommunikation und der Geldmittelbeschaffung bedienen und Informationsquellen und neue Technologien nutzen, um direkte und persönliche Kontakte mit verschiedensten Kategorien von betroffenen Personen zu knüpfen;

In Erwägung, dass in einer wachsenden Zahl von Ländern ein Trend hin zu immer stärkerer institutioneller Kommunikation gewählter Kandidatinnen und Kandidaten und Körperschaften zu beobachten ist, ebenfalls auf lokaler Ebene und mittels E-Government; in der Erwägung, dass diese Aktivitäten, die die Verarbeitung von Personendaten voraussetzen können, in Einklang stehen mit dem Recht der Staatsbürgerinnen und -bürger, über die Tätigkeiten der gewählten Kandidatinnen und Kandidaten und Körperschaften informiert zu werden;

In Erwägung, dass in diesem Rahmen von politischen Organisationen fortlaufend eine große Menge von Personendaten gesammelt und manchmal in aggressiver Art und Weise verwendet werden, unter Anwendung verschiedener Techniken wie Umfragen, Sammlung von E-Mail-Adressen mittels geeigneter Software oder Suchmaschinen, flächendeckender Stimmenwerbung in Städten oder Formen politischer Entscheidbildung durch interaktives Fernsehen oder Computerdateien, die die Herausfilterung einzelner Stimmenden erlauben; in Erwägung, dass in diesen Daten – zusätzlich zu elektronischen Adressen, Telefonnummern, E-Mail-Konten, Informationen über berufliche Tätigkeiten und familiäre Verhältnisse – zuweilen unrechtmäßig auch sensible Daten enthalten sein können wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten;

In Erwägung, dass von verschiedenen Personen invasive Profile erstellt und sie klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen, ihr angehören oder gar Parteimitglieder sind, um so mit bestimmten Gruppen von Bürgerinnen und Bürgern vermehrt persönlich kommunizieren zu können;

In Erwägung, dass diese Aktivitäten gesetzeskonform und ordnungsgemäß ausgeübt werden müssen;

In Erwägung, dass es nötig ist, die Grundrechte und Grundfreiheiten der betroffenen Personen zu schützen und mit geeigneten Maßnahmen zu verhindern, dass diese Personen ungerechtfertigtes Eindringen in ihre Privatsphäre erfahren, Schaden erleiden oder ihnen Kosten entstehen, dass sie namentlich negative Auswirkungen und mögliche Diskriminierungen erleiden oder auf die Ausübung bestimmter Formen der politischen Beteiligung verzichten müssen;

In Erwägung, dass es möglich sein sollte, das Schutzziel zu erreichen, indem sowohl die Interessen der Öffentlichkeit an bestimmten Formen politischer Kommunikation als auch angemessene Modalitäten und Garantien in Bezug auf die Kommunikation mit Parteimitgliedern und mit andern Bürgerinnen und Bürgern in Betracht gezogen werden;

In Erwägung, dass in diesem Sinne ein verantwortungsbewusstes Marketing gefördert werden kann, ohne dass der Austausch politischer Ideen und Vorschläge behindert zu werden braucht, und dass die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten hat, die sie vom kommerziellem Marketing unterscheiden;

In Erwägung, dass Datenschutzgesetze bereits in vielen Gerichtsbarkeiten auf politische Kommunikation anwendbar sind;

In Erwägung, dass es nötig ist, die Einhaltung der Datenschutzgrundsätze zu garantieren und dazu einen weltweiten Minimalstandard zu schaffen, der dazu beitragen könnte, das Schutzniveau für Personen, von denen Daten gesammelt werden können, zu harmonisieren, indem zum einen nationale und internationale Verhaltensregeln zur Grundlage genommen und zum andern spezifische Lösungen und Regelungen einzelner Länder berücksichtigt werden;

In Erwägung, dass die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen könnten, auch in Zusammenarbeit mit anderen Aufsichtsbehörden in den Bereichen der Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren;

verabschiedet

folgende Resolution

Jede Aktivität politischer Kommunikation, die die Verarbeitung von Personendaten voraussetzt – auch diejenige, die nicht im Zusammenhang mit Wahlkampagnen steht – muss die Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen respektieren, einschließlich des Rechts auf Schutz der persönlichen Daten, und muss im Einklang stehen mit den anerkannten Grundsätzen des Datenschutzes, namentlich:

Datenminimierung

Personendaten sollen nur so weit verarbeitet werden, als es zur Erreichung des spezifischen Zwecks, zu welchem sie gesammelt werden, erforderlich ist.

Erhebung auf rechtmäßige Weise und nach Treu und Glauben

Personendaten sollen aus erkennbaren Quellen rechtmäßig erhoben werden und sie sollen nach Treu und Glauben verarbeitet werden. Es soll sichergestellt werden, dass die Quellen, im Einklang mit dem Gesetz, entweder öffentlich zugänglich sind, oder dass andernfalls respektiert wird, dass sie nur zu bestimmten Zwecken, unter bestimmten Modalitäten, für einen begrenzten Anlass oder Zeitraum genutzt werden dürfen.

Besondere Aufmerksamkeit soll jenen Fällen geschenkt werden, in denen aggressive Methoden für die Kontaktaufnahme mit den betroffenen Personen gewählt werden.

Datenqualität

Bei der Verarbeitung sollen die anderen Grundsätze zur Sicherung der Datenqualität beachtet werden. Die Daten müssen insbesondere richtig, relevant und auf das notwendige Minimum beschränkt sein und à jour gehalten werden im Hinblick auf den bestimmten Zweck, zu dem sie erhoben wurden, besonders wenn sich die Informationen auf gesellschaftliche oder politische Anschauungen oder ethische Überzeugungen der betroffenen Person beziehen.

Zweckmäßigkeit

Personendaten aus privaten oder öffentlichen Informationsquellen, Institutionen oder Organisationen dürfen für die politische Kommunikation verwendet werden, wenn ihre Weiterverarbeitung im Einklang steht mit dem Zweck, zu dem sie ursprünglich erhoben wurden, und den betroffenen Personen zur Kenntnis gebracht wird; dies gilt insbesondere für sensible Daten. Gewählte Abgeordnete müssen diese Grundsätze beachten, wenn sie Daten, die zur Ausübung der amtlichen Funktionen gesammelt wurden, für die politische Kommunikation benützen wollen.

Personendaten, die ursprünglich mit aufgeklärter Einwilligung der betroffenen Person zu Marketingzwecken erhoben wurden, dürfen für die politische Kommunikation verwendet werden, wenn der Zweck der politischen Kommunikation in der Zustimmungserklärung ausdrücklich genannt wird.

Verhältnismäßigkeit

Personendaten dürfen nur auf die Art und Weise verarbeitet werden, die dem Zweck der Datensammlung entspricht, insbesondere wenn es um Daten zu potenziellen Wählerinnen und Wählern oder um den Vergleich von Daten geht, die aus verschiedenen Archiven oder Datenbanken stammen.

Personendaten, insbesondere solche, die über den Anlass hinaus, zu dem sie erhoben wurden, aufbewahrt werden, dürfen weiter verwendet werden, bis die Ziele der politischen Kommunikation erreicht sind.

Information der betroffenen Person

Den betroffenen Personen muss eine dem gewählten Kommunikationsmittel entsprechende Informationsnotiz zugestellt werden, bevor von ihnen Daten gesammelt werden; die Notiz hat den für die Datensammlung Verantwortlichen zu bezeichnen (die einzelne kandidierende Person; den externen Kampagnenleiter; die lokale Unterstützungsgruppe; lokale oder assoziierte Vereinigungen; die Partei insgesamt) sowie den zu erwartenden Datenaustausch zwischen diesen Instanzen.

Die Person, von der Daten gesammelt werden, muss informiert werden, wenn diese Daten ohne ihr Zutun gesammelt werden, zumindest wenn die Daten nicht nur vorübergehend aufbewahrt werden.

Einwilligung

Es muss sichergestellt sein, dass die Verarbeitung von Personendaten auf der Einwilligung der betroffenen Person oder auf einen anderen gesetzlich vorgesehen Grund beruht. Die Verarbeitung muss die im jeweiligen Staat geltenden, den spezifischen Informationsquellen und –mitteln entsprechenden Regelungen beachten, namentlich im Falle von E-Mail-Adressen, Faxnummern, SMS oder andern Text/Bild/Video-Mitteilungen oder von aufgezeichneten Telefonkontakten.

Datenaufbewahrung und Datensicherheitsmassnahmen

Jede für eine Datensammlung verantwortliche Person, sei es eine politische Gruppierung oder eine einzelne kandidierende Person, muss alle technischen und organisatorischen Maßnahmen treffen, die nötig sind, um die Integrität der Daten zu schützen und um zu verhindern, dass die Daten verloren gehen oder von unbefugten Personen oder Stellen benutzt werden.

Rechte der betroffenen Person

Die betroffene Person hat das Recht auf Zugang, Berichtigung, Sperrung und Löschung ihrer Daten; sie hat das Recht, sich gegen unerwünschte Kommunikation zu wehren und – kostenlos sowie auf einfache Weise – zu verlangen, keine neuen Mitteilungen mehr zu erhalten. Diese Rechte müssen in der an sie gerichteten Informationsnotiz ausdrücklich genannt werden.

Für den Fall, dass diese Rechte verletzt werden, sind angemessene Maßnahmen und Sanktionen vorzusehen.

V. Arbeitspapiere der internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 37. Sitzung am 31. März / 1. April 2005 in Madeira (Portugal)

Zweites Arbeitspapier zum Datenschutz bei Online-Wahlen in Parlamentswahlen und Wahlen zu anderen staatlichen Gremien

– Übersetzung –

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat bei ihrer 30. Sitzung am 28. August 2001 in Berlin ein Arbeitspapier zum Datenschutz bei Online-Wahlen in Parlamentswahlen und Wahlen zu anderen staatlichen Gremien angenommen.[1]

Seitdem sind in mehreren Ländern e-voting-Projekte (Projekte mit elektronischen Abstimmungsverfahren) durchgeführt worden. Diese Projekte haben neue Erkenntnisse und Analysewerkzeuge aufgrund ihrer Auswertung erbracht.

Die Arbeitsgruppe gibt deshalb die folgenden zusätzlichen Empfehlungen:

Elektronische Abstimmungssysteme müssen das Wahlgeheimnis, die Privatsphäre der Wählenden und die Vertraulichkeit des Wahlverfahrens garantieren. Die elektronische Wahl im Wahllokal, ohne dass Daten der Wählenden oder abgegebene Stimmen über eine elektronische Infrastruktur übermittelt werden, muss die Vertraulicheit, Integrität und Verfügbarkeit des Systems durch folgende Vorkehrungen sicherstellen:

- Die Hard- und Software sollte einer technischen und organisatorischen Vorabkontrolle unterworfen werden, die unter der Aufsicht der zuständigen Wahlbehörde/des zuständigen Wahlamtes (oder einer von dieser/diesem bestimmten unabhängigen Stelle) durchzuführen ist, und

- das System (Hard- und Software) sollte der zuständigen Wahlbehörde angezeigt werden; auch sollte die Software mit einer elektronischen Signatur zertifiziert werden, um seine Integrität und Transparenz zu gewährleisten.

Die Übermittlung personenbezogener Daten über die wählenden Personen und die abgegebenen Stimmen über ein Netz, das Online-Wahlbüros verbindet, ent-

[1] S. <http://www.datenschutz-berlin.de/doc/int/iwgdpt/online_voting.htm>

hält nicht genügend Sicherheitsgarantien, wenn die Übermittlung nicht in einem virtuellen privaten Netz (Virtual Private Network) stattfindet.

Die Arbeitsgruppe empfiehlt als Grundlage der weiteren Diskussion die Terminologie der Empfehlung R (2004) 11 des Ministerkomitees des Europarates an die Mitgliedstaaten über rechtliche, verfahrensmäßige und technische Standards für elektronische Abstimmungen (e-voting) vom 30. September 2004[2].

Anhang[3]

In dieser Empfehlung werden die folgenden Begriffe mit folgender Bedeutung verwandt:

- Authentifizierung: die Vergewisserung/Überprüfung der behaupteten Identität einer Person oder eines Datensatzes;
- Abstimmung/Wahl: das rechtlich anerkannte Verfahren, in dem ein Wähler oder eine Wählerin seine Wahlentscheidung ausdrücken kann;
- Kandidat: eine zur Wahl stehende Person und/oder Gruppe von Personen und/oder politische Partei;
- Stimmabgabe: Einwurf des Stimmzettels in die Wahlurne;
- e-Wahl oder e-Referendum: eine politische Wahl oder ein Referendum, bei der oder dem elektronische Verfahren in einer oder mehreren Phasen eingesetzt werden;
- Elektronische Wahlurne: das elektronische Verfahren, in dem Stimmen vor der Auszählung gespeichert werden;
- e-voting: eine elektronische Abstimmung oder ein elektronisches Referendum, bei dem zumindest die Stimmabgabe automatisiert erfolgt;
- Netzbasiertes e-voting: e-voting, bei dem die Stimmabgabe mit einem Gerät erfolgt, das nicht von einem Wahlvorstand kontrolliert wird;

---

2 Die Empfehlung ist abrufbar unter <http://www.coe.int/T/e/integrated_projects/democracy/02/_Activities/02_e-voting/>

3 Zit. nach der Empfehlung des Europarates, vgl. FN 2.

- Versiegelung: der Schutz von Informationen dergestalt, dass sie nicht ohne Zusatzinformationen oder Mitteln genutzt oder interpretiert werden, die nur bestimmten Personen oder Stellen zugänglich sind;
- Stimme: der Ausdruck einer Wahlentscheidung;
- Wähler oder Wählerin: ein Person mit Stimmrecht bei einer bestimmten Wahl oder in einem bestimmten Referendum;
- Abstimmungskanal: die Methode/das Verfahren, in dem der Wähler oder die Wählerin abstimmen kann;
- Wahlmöglichkeiten: die Alternativen, zwischen denen durch die Stimmabgabe bei einer Wahl oder einem Referendum gewählt werden kann;
- Wählerverzeichnis: Liste der wahlberechtigten Personen.

2. 38. Sitzung am 6./7. September 2005 in Berlin

Web Browser Caching („Zwischenspeicherung") von personenbezogenen Daten bei öffentlichen Internet-Zugängen (z. B. Internet-Cafes)[4]

– Übersetzung –

1. Einleitung

In Internet-Cafes besteht die Möglichkeit, gegen Entgelt oder kostenlos Zugang zum Internet zu erhalten. Als Gratisdienstleistung wird dies mitunter auch in öffentlichen Bibliotheken und Schulen angeboten. In diesen von mehreren Personen genutzten Umgebungen kommunizieren die Nutzer mit ihrer Familie oder Freunden, nehmen berufliche oder andere Verpflichtungen wahr und führen online Bankgeschäfte aus. Dies macht Internet-Cafes zu einem Ziel für Kriminelle, die personenbezogene Daten „stehlen". Mit dem steigenden Bewusstsein für die Auswirkungen des „Identitätsdiebstahls" (ID theft), erhält die Rolle der Betreiber von Internet-Cafes bei der Bekämpfung dieses Problems eine immer größere Bedeutung.

[4] Wegen Besonderheiten in der nationalen Gesetzgebung kann das Papier von Italien nicht mitgetragen werden.

2. Probleme

Jüngste Veröffentlichungen über Identitätsdiebstahl und seine Auswirkungen auf die Betroffenen unterstreichen Folgendes:

- Risiken bei der Nutzung des Internet für persönliche Kommunikation
- Datensicherheitsaspekte in Internet-Cafes
- Mangelhafte Betriebsorganisation von Internet-Cafes, die persönlichen Informationen der Nutzer gefährden können.

Die clientseitige Zwischenspeicherung von Webseiten-Informationen ist seit langem als Sicherheits- und mögliches Datenschutzproblem erkannt. Die clientseitige Zwischenspeicherung führt zu einer temporären Speicherung der Kopien von Webseiten durch die Webbrowser Software auf der Festplatte des Nutzerrechners. Alle üblicherweise installierten Webbrowser nutzen diese Technik, z. B. ermöglicht sie die Verwendung des „Zurück"-Buttons eines Browsers. Sie sichert auch die Rückkehr zur Quelle einer früher heruntergeladenen Webseite, wenn diese Seite unverändert bleibt.

Ein Sicherheitsproblem tritt auf, wenn personenbezogene Daten Bestandteil einer Webseite sind, die vom Webbrowser zwischengespeichert wird. Die zwischengespeicherte Seite wird gleichwohl auf dem Computer des Nutzers verbleiben und kann für andere Nutzer mittels des „Zurück"-Buttons, des „History"-Verzeichnisses oder mittels direkter Suche auf der Festplatte des PCs zugänglich sein.

In Internet-Cafes entsteht ein Sicherheitsproblem am Ende der Internet-Sitzung eines Nutzers. Nachfolgende Nutzer sind in der Lage, die Seiten aufzusuchen, die im Zwischenspeicher des Browsers enthalten sind, und auf diese Informationen zu zugreifen. Hier besteht das Risiko, dass angesichts jüngster Veröffentlichungen über Spyware und andere bösartige Programme, die Sicherheitsrisiken, die durch den Browser Cache entstehen, übersehen werden.

3. Empfehlung

Cyber-Cafes sollten sicherstellen, dass alle personenbezogenen Daten, die während einer Internet-Sitzung eines Nutzers gesammelt werden, nach dem Ende der Sitzung (logout) vollständig entfernt werden. Weiterhin sollte der Nutzer selbst die Möglichkeit haben, den Inhalt des „History"-Ordners zu löschen, bevor ein anderer Nutzer Zugang zum System erhält. Es sollte ein Warnhinweis oder -signal (z. B. ein Popup-Fenster) vorgesehen werden, das den Nutzer auf die Löschungsmöglichkeit aufmerksam macht, bevor er sich abmeldet.

Netzwerkbasierte Telemedizin

Arbeitspapier

- angenommen auf der 31. Sitzung am 26./27. März 2002 in Auckland (Neuseeland)

- aktualisiert auf der 38. Sitzung am 6./7. September in Berlin

– Übersetzung –

Telemedizin ist das Praktizieren von Medizin aus der Entfernung. Der Begriff ist weit genug gefasst, um den australischen „Flying Doctor Service", Fernuntersuchungen über Video nach Unfällen auf Bohrinseln und medizinische Ratgeber-Sendungen im Fernsehen oder im Radio zu umfassen. Dieses Papier beschäftigt sich mit netzwerkbasierten Gesundheitsdiensten und ihren Implikationen für den Datenschutz.

Die „American Medical Association" hat festgestellt, dass „der Zugang zu medizinischer Information über das Internet das Potenzial besitzt, die Beziehung zwischen Arzt und Patient von der ärztlichen Autorität, die Behandlungen und Beratung verabreicht zu einem gemeinsamen Entscheidungsprozess zwischen Patient und Arzt zu beschleunigen".[1] Andere mögen nicht so optimistisch sein. Die Zunahme von Informationsangeboten zur Gesundheit im Internet[2], Online-Selbsthilfe- und Diskussionsgruppen[3] und die elektronische Übermittlung von Gesundheitsdaten über das Internet erweckt den Eindruck, dass das Internet ein integraler Bestandteil der Gesundheitsversorgung werden wird.

Das Angebot von Gesundheitsdiensten über das Internet findet gegenwärtig in drei Umgebungen statt:

1 American Medical Association, „Guidelines for Medical and Health Information Sites on the Internet", http://www.ama-assn.org/ama/pub/category/1905.html

2 vgl. www.medscape.com, ein Portal, das an Ärzte und interessierte Laien gerichtet ist.

3 vgl. die Untersuchung über medizinische Internetnutzung www.hon.ch/Survey/FebMar2001/survey.html

1. Das Internet als ein Forum für die Diskussion von Gesundheitsfragen

Dies schließt Internet-basierte Diskussionsgruppen und Mitteilungsdienste ein. Die Veröffentlichung kann anonym sein und die Diskussionen werden entweder moderiert oder nicht. Informationen, die in diesen Foren veröffentlicht werden, tendieren dazu, eher anekdotischer als verlässlicher Natur zu sein und schließen normalerweise nicht die Bezahlung einer Gebühr oder eines Abonnements oder die Begründung einer klinischen Beziehung zwischen dem Informationsanbieter und dem Informationssuchenden ein. Auf der professionellen Ebene existieren private Diskussionsgruppen, für die eine Gebühr erhoben wird und bei denen die Aufnahme auf eine bestimmte Untergruppe der Internetnutzer wie z. B. Ärzte beschränkt ist.

2. Internet-basierte Erbringung von Gesundheitsdiensten von Ärzten für Patienten (e-Ärzte)

Es hat einige Versuche gegeben, die traditionelle Arzt-Patient-Beziehung in der virtuellen Welt abzubilden. Patienten, die sich unter Umständen zu einem bestimmten Zeitpunkt für Abrechnungszwecke identifizieren müssen, übermitteln private Anfragen mit der Beschreibung ihrer Symptome an Ärzte. Der Arzt, dessen Name und Qualifikation in dem Internetangebot verfügbar ist, kann durch e-Mail oder gesicherte Internetverbindungen antworten, berät und schlägt eine Behandlung vor. Obwohl es dem Arzt nicht möglich sein wird, seinen Patienten zu berühren, könnte eine visuelle Untersuchung durch die Nutzung einer Webcam möglich sein (obwohl dies bisher nicht üblich ist). Nationale Gesetze werden typischerweise fordern, dass Rezeptverordnungen die Unterschrift des Arztes tragen, und es mag in manchen Fällen unethisch sein, Medikamente zu verschreiben, ohne den Patienten persönlich untersucht zu haben.[4]

3. Das Internet als Aufbewahrungsort für Patientenakten

In manchen Fällen existiert als Teil des unter 1. und 2. Beschriebenen ein elektronisches Archiv personenbezogener Gesundheitsdaten, zu denen der Betroffene und sein autorisierter Behandler Zugang haben.

Dieses Papier beschäftigt sich mit der Internet-basierten Erbringung von Gesundheitsdiensten.

[4] Apotheker dürfen Medikamente verkaufen, solange sie eine Verordnung erhalten (sie brauchen den Betroffenen dafür nicht sehen zu können). Als Beispiel eines Internet-basierten Verkäufers vgl. „CyberChemist“ unter www.chemist.co.nz/pm/index.cfm.

Eine Auswahl von Datenschutzproblemen bei Internet-basierter Telemedizin

Ethische Verpflichtungen und gesetzliche Pflichten zur Vertraulichkeit

Ein eingeführter Bestandteil der normalen Beziehung zwischen Arzt und Patient ist die Vertraulichkeit. Vertraulichkeit zwischen Arzt und Patient verpflichtet den Arzt im Hinblick auf die persönlichen Informationen des Patienten. Wenn ein zugelassener Arzt Gesundheitsdienstleistungen erbringt, gelten gleichzeitig ethische Beschränkungen, unabhängig davon, ob die Arztpraxis tatsächlicher oder virtueller Natur ist. Allerdings müssen einige spezifische Probleme in Bezug auf den Datenschutz der Nutzer von online-Gesundheitsdiensten bei der Nutzung des Internet betrachtet werden.

Probleme können sich aus der Nutzung von Verbindungsdaten ergeben, die im Zuge einer Interaktion zwischen Arzt und Patient entstehen. Verbindungsdaten können unter bestimmten Umständen mit Daten über andere Nutzungen des Internet und personenbezogenen Daten zusammengeführt werden. Daten über Verordnungen sind z.B. für Hersteller von Medikamenten von Interesse. Ein weiteres Anliegen ist Grundvertrauen. Nutzer müssen überzeugt sein, dass eine Webseite ein vertrauenswürdiger Aufbewahrungsort für ihre medizinischen Daten ist.

Wenn Internet-Angebote dieser Art Erfolg haben sollen, muss das Internet zunächst als ein akzeptabler Weg für die Erbringung von Gesundheitsdiensten angesehen werden. Datenschutz ist eines der wichtigsten Bedenken der Nutzer im elektronischen Geschäftsverkehr und die Sensibilität von Gesundheitsinformationen vergrößert diese Bedenken. Es sind einige Versuche unternommen worden, gute Praktiken und dadurch das Vertrauen der Öffentlichkeit zu fördern. Ein Beispiel ist der "Health On-Line Code of Conduct", der verlangt, dass Internetangebote „die gesetzlichen Anforderungen hinsichtlich des Datenschutzes bei medizinischer oder Gesundheits-Information beachten, die in demjenigen Land oder Bundesstaat gelten, in dem das Internet-Angebot und gespiegelte Angebote angesiedelt sind oder darüber hinausgehen"[5]. Ein anderes Beispiel bilden die AMA „Guidelines for Medical and Health Information Sites on the Internet[6]. Solche Initiativen werden in manchen Fällen durch selbstregulierende Datenschutz-Gütesiegel-Programme mit externer Zulassung und Beschwerde-Verfahren unterstützt.

[5] vgl. www.hon.ch. Ein Artikel aus dem „Journal of Medical Internet Research", der diesen Code kritisiert, ist verfügbar unter www.jmir.org/2000/1/37.

[6] s. Fußnote 1

Erhebung, Nutzung und Übermittlung

Die Erhebung von Daten während einer telemedizinischen Untersuchung kann – anders als bei einer „physikalischen" Untersuchung – indirekt oder sogar „unsichtbar" erfolgen. Internetangebote veröffentlichen oft Datenschutzerklärungen, die Aussagen darüber enthalten, welche Daten erhoben werden[7], aber diese decken nur selten die Nutzung von „Third Party Cookies" ab, die durch Werbeunternehmen platziert werden. Die Weiterverwendung von Verbindungsdaten, besonders wenn diese mit anderen personenbezogenen Daten kombiniert werden, würde ein ernsthaftes Problem darstellen. Es ist unwahrscheinlich, dass Probleme im Zusammenhang mit Verbindungsdaten oder Cookies durch herkömmliche ethische Regelung angemessen geregelt werden. Dies könnte verstärkt werden durch eine enge Partnerschaft, die zwischen praktischen Ärzten und Medikamentenherstellern existieren könnte.

Ethische Probleme und Datenschutzprobleme können auch entstehen, wenn Verbindungsdaten zu Forschungszwecken mit personenbezogenen Daten der Patienten zusammengeführt werden.

Angemessenheit

Es kann Aspekte medizinischer Beratung geben, für die Internet-basierte Anwendungen für die vorhersehbare Zukunft unangemessen sind. Dies gilt z. B. in Fällen, in denen eine Diagnose ohne weitere Informationen durch den Patienten nicht sicher vorgenommen werden kann (obwohl die Einholung einer „zweiten Meinung" möglich sein wird, solange der untersuchende Arzt die Symptome und den Zustand bereits sorgfältig aufgezeichnet hat).

Sicherheit

Sicherheitsprobleme existieren bei der Speicherung medizinischer Daten, so dass Ärzte und Patienten über das Internet darauf zugreifen können. TCP/IP ist ein in sich unsicheres Medium[8] und Methoden zur Beseitigung dieser Unsicherheit verlangen Maßnahmen und finanziellen Aufwand in dem Internetangebot, in dem die Daten gespeichert werden. Während die Online-Speicherung von medizinischen Informationen eine gute Nutzung der Allgegenwärtigkeit des Web darstellt, entsteht durch sie auch die Möglichkeit eines Fernzugriffs von unsicheren Orten wie Internet-Cafes.

---

[7] Eine Studie, nach der eine Inkonsistenz zwischen den veröffentlichten Datenschutzerklärungen von Angeboten zur Gesundheit im Internet und deren tatsächlicher Praxis besteht, kann abgerufen werden unter www.ehealth.chcf.org/view.cfm?itemID=12497.

[8] Für eine kurze Erläuterung der Hintergründe s. www.itsecurity.com/tutor/tcpip.htm.

Die Vertraulichkeit medizinischer Informationen wird von den Nutzern als sehr wichtig eingeschätzt und wirksame Sicherheitsmaßnahmen gegen unautorisierten Zugriff stellen eine unverzichtbare Maßnahme dar, um den Bruch der Vertraulichkeit zu verhindern. Sie können gleichzeitig auch einen Wettbewerbsvorteil für jegliches Internetangebot zur Telemedizin bilden.

Vorteile

Wie nicht anders zu erwarten, hat sich dieses Papier auf die Problembereiche konzentriert. Bevor Empfehlungen gegeben werden, soll auf Aspekte Internet-basierter Telemedizin hingewiesen werden, die zu einer Verbesserung des Datenschutzes führen können:

- Der Einzelne kann in die Lage versetzt werden, selbst auf Informationen zugreifen zu können; sowohl auf die eigenen Patientenakten als auch auf Gesundheitsratgeber, und zwar zu praktisch jeder Zeit und an jedem Ort in der Welt;

- Internet-basierte Telemedizin eröffnet die anonyme Möglichkeit, eine „zweite Meinung“ einzuholen – manche Betroffenen hatten Hemmungen oder es war ihnen peinlich, eine zweite Meinung in der traditionellen Weise durch ihren eigenen Arzt zu verlangen;

- Cyber-Apotheken bilden das moderne Äquivalent der Katalogbestellung und können die Verlegenheit beim Ausfüllen von Verordnung für Medikamente gegen sexuell übertragbare Krankheiten etc. – besonders in Kleinstädten – verringern.

Empfehlungen

Aus der Sensitivität medizinischer Daten folgt, dass die gesetzlichen Bestimmungen zum Datenschutz von Anbietern Internet-basierter Telemedizin genauestens eingehalten werden müssen. Wo solche gesetzlichen Regelungen nicht anwendbar sind, sollten die allgemein anerkannten Prinzipien des fairen Umgangs mit Informationen beachtet werden und jegliche Erhebung, Nutzung und Übermittlung von Daten sollte mit der informierten Einwilligung des Betroffenen erfolgen. Zusätzlich zu den üblichen Datenschutzerwägungen werden folgende Empfehlungen gegeben:

1. Internetangebote zur Telemedizin müssen ihren Umgang mit personenbezogenen Informationen für die Nutzer transparent machen. Dies bedeutet unter anderem die Veröffentlichung einer klaren und aussagekräftigen Datenschutzerklärung. Besondere Aufmerksamkeit sollte der Information der Betroffenen über Aspekte der Telemedizin gewidmet werden, die von der nor-

malen „face-to-face“-Medizin abweichen. Idealerweise sollte die Einhaltung der Datenschutzerklärung verifiziert werden können (z. B. durch periodische Auditierung oder durch ein Gütesiegelprogramm).

2. Internet-basierte Angebote zur Telemedizin sollten keine personenbezogenen Daten von den Nutzern durch aktive Elemente oder Cookies heimlich erheben. Wo das anwendbare Recht die Anwendung aktiver Elemente oder von Cookies erlaubt, sollten diese nur mit der Einwilligung des Betroffenen aktiviert werden und ihre Nutzung sollte für die Betroffenen, die um medizinische Beratung nachsuchen, nicht verpflichtend sein. Jedes Internetangebot zur Telemedizin, das aktive Elemente oder Cookies verwendet, sollte darauf in seiner Datenschutzerklärung hinweisen.

3. Verbindungsdaten, die personenbezogene Daten der Besucher eines Internet-Angebots zur Telemedizin enthalten, sollten nicht an Dritte weitergegeben werden. Insbesondere sollten die erhobenen medizinischen Daten nicht für kommerzielle Zwecke genutzt werden.

4. Traditionelle ethische Verpflichtungen für Ärzte und Gesundheitsdienstleister dürfen durch das Angebot dieser Dienste über das Internet nicht gemindert werden. Standesorganisationen sollten die Ergänzung ihrer ethischen Richtlinien in Erwägung ziehen, um sicherzustellen, dass vorbildliche Praktiken in der neuen Umgebung eingehalten werden.

5. Internet-basierte Angebote zur Telemedizin sollten die anwendbaren Richtlinien zum Verbraucherschutz und professionelle Standards einhalten, um sicherzustellen, dass jegliche personenbezogene Daten, die erhoben, empfangen, genutzt oder übermittelt werden, in fairer Weise verarbeitet werden. Die AMA bietet z. B. wertvolle Richtlinien in Bezug auf den Inhalt von Internet-Angeboten, Werbung, Sponsoring und elektronischen Geschäftsverkehr, die in Betracht gezogen werden sollten.

6. Wirksame Sicherheitsmaßnahmen sollten ergriffen werden, um gespeicherte medizinische Informationen (ebenso wie personenbezogene Daten während der Übertragung) in einem Internet-Angebot zur Telemedizin zu schützen. Solche Maßnahmen sollten Verschlüsselung einschließen.

7. Die Standesorganisationen von Ärzten und ähnlichen Berufsgruppen sollten angemessene Richtlinien verabschieden. Überprüfungsmechanismen (z. B. Gütesiegel) sollten geschaffen werden, um die Umsetzung dieser Empfehlung zu verifizieren.

B Dokumente zur Informationsfreiheit

I. Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID)

1. Entschließung der 10. Sitzung am 27. Mai 2005 in Potsdam

„Jetzt nicht kneifen – das Informationsfreiheitsgesetz endlich verabschieden!“

Nachdem die zweite und dritte Lesung des Entwurfs für das Informationsfreiheitsgesetz im Deutschen Bundestag auf Anfang Juni 2005 verschoben wurde, fordert die Arbeitsgemeinschaft der Informationsbeauftragten, die Verabschiedung des Gesetzes nicht länger hinauszuzögern. Mit seinem überkommenen Amtsgeheimnis bleibt Deutschland sonst europäisches und internationales Schlusslicht in Sachen Transparenz.

Seit die Bundesregierung 1998 angekündigt hatte, ein Informationsfreiheitsgesetz für Bundesbehörden auf den Weg zu bringen, haben die Gegnerinnen und Gegner einer transparenten Verwaltung das Gesetzesvorhaben kontinuierlich torpediert. Jüngst befürchteten die Krankenkassen unter anderem Wettbewerbsverzerrungen durch Offenlegungspflichten und Überschneidungen mit bestehenden Informationsansprüchen. Die berechtigten Interessen der Krankenkassen an der Geheimhaltung ihrer Geschäftsgeheimnisse sowie der Sozialdaten ihrer Patientinnen und Patienten werden von dem vorgelegten Gesetzentwurf jedoch wirksam geschützt; ebenso regelt der Entwurf das Verhältnis zu vergleichbaren Informationsansprüchen klar und eindeutig. Es gibt also keinen Grund für eine Verschiebung der Diskussion im Parlament. Die Informationsbeauftragten fordern daher, dass der Deutsche Bundestag – trotz der aktuellen Debatte um vorgezogene Neuwahlen – dieses wichtige Gesetz noch verabschiedet, damit es spätestens Anfang 2006 in Kraft treten kann. Das Informationsfreiheitsgesetz soll den Bürgerinnen und Bürgern endlich freien Zugang zu öffentlichen Informationen auch bei Bundesbehörden verschaffen.

2. Entschließungen der 11. Sitzung am 14. November in Düsseldorf

Transparenz in öffentlichen Unternehmen gefordert

Private, börsennotierte Aktiengesellschaften sind seit kurzem verpflichtet, die Vergütungen der Vorstandsmitglieder offen zu legen. Aktionärinnen und Aktio-

näre können somit erfahren, ob der Vorstand einer Aktiengesellschaft angemessene Bezüge erhält. Dieselben Rechte sollen auch Bürgerinnen und Bürger gegenüber öffentlichen Unternehmen geltend machen können.

Die Bürgerinnen und Bürger haben einen Anspruch darauf, zu wissen, wie hoch die Vergütungen für die einzelnen Mitglieder der Verwaltungsräte, Aufsichtsräte und Geschäftsführungen von privatrechtlichen Gesellschaften sind, die sich mehrheitlich aus Vertretern des Bundes, der Länder oder der Kommunen zusammensetzen. Eine Veröffentlichung der Bezüge in den Jahresabschlüssen und in den Beteiligungsberichten der öffentlich-rechtlichen Körperschaften verbessert die Transparenz über die Verwendung von Steuergeldern und stärkt die Akzeptanz öffentlicher Unternehmen.

Die Arbeitsgemeinschaft der Informationsbeauftragten fordert die Gesetzgeber des Bundes und der Länder daher auf, eine entsprechende Offenlegungspflicht auch für öffentlich kontrollierte Unternehmen festzulegen. Die Regelungen des jüngst verabschiedeten Vorstandsvergütungs-Offenlegungsgesetzes für private Aktiengesellschaften können hierfür als Maßstab dienen.

Offenlegung von Aktivitäten und Bezügen der Mitglieder öffentlicher Organe und Gremien

Ob ein Mitglied einer kommunalen Vertretung oder einer Landesregierung den Vorsitz in einer bestimmten Organisation führt oder in einem Aufsichtsrat eines Unternehmens sitzt, kann von erheblichem Einfluss auf die Entscheidungsfindung der Kommune oder des Landes sein. Ohne Kenntnis solcher Aktivitäten öffentlicher Entscheidungsträger ist Verwaltungshandeln häufig gar nicht nachvollziehbar. Insbesondere Informationen über die Höhe der zusätzlichen Vergütung können Aufschluss über die Motivation für ein bestimmtes Abstimmungs- oder Entscheidungsverhalten geben. Derzeit werden solche Informationen allerdings noch geheim gehalten.

Die Transparenz von „nebenamtlichen“ Aktivitäten und Bezügen öffentlicher Entscheidungsträger ist ein wichtiges Kontrollinstrument, das auch in Geschäftsordnungen von Landtagen, in Haushaltsordnungen oder Gemeindeordnungen sowie in Korruptionsbekämpfungsgesetzen mehr und mehr Eingang findet. Die Verpflichtung, solche Aktivitäten und Bezüge offen zu legen, erhöht zudem die Akzeptanz der Entscheidungen öffentlich Bediensteter.

Die Arbeitsgemeinschaft der Informationsbeauftragten fordert daher die Gesetzgeber in den Ländern auf, eine allgemeine Offenlegungspflicht für „nebenamtliche“ Aktivitäten und Vergütungen öffentlicher Entscheidungsträger gesetzlich festzulegen.

II. Gründung der Europäischen Konferenz der Informationsbeauftragten am 24./25. November 2005 in Berlin

Erklärung der Zusammenarbeit

– Übersetzung –

Am 7. April 2003 wurde die Internationale Konferenz der Informationsbeauftragten (ICIC) in der Europäischen Akademie für Informationsfreiheit und Datenschutz gegründet.

14 Delegationen aus aller Welt erklärten:

„Teilhabe am Wissen der öffentlichen Verwaltung ist ein Bürgerrecht in der Informationsgesellschaft. Jede Person muss ohne Diskriminierung Zugang zu Dokumenten staatlicher Einrichtungen erhalten. Eine transparente öffentliche Verwaltung, die offen ist für eine Beteiligung der Bürgerinnen und Bürger an ihren Entscheidungen, ist Voraussetzung einer modernen, demokratischen Gesellschaft.

Die Informationsbeauftragten und Ombudspersonen, die in ihren Heimatländern die Informationsfreiheit wahren, sind diesen Grundprinzipien verpflichtet."

Um ein breiteres, weltweites Bewusstsein für Informationsfreiheit zu entwickeln, zur weiteren Untersuchung und Bestimmung ihrer entscheidenden Elemente und um vom gegenseitigen Erfahrungsaustausch zu profitieren, vereinbarten die Teilnehmer eine ständige Zusammenarbeit. Diese Verpflichtung wurde bekräftigt bei den folgenden Zusammenkünften der ICIC in Kapstadt/Südafrika 2004 und Cancún/Mexiko 2005.

In Anbetracht der Tatsache, dass es aufgrund der Gesetzgebung der Europäischen Union, ihrer Mitgliedstaaten und aller anderen europäischen Länder als wünschenswert betrachtet wird, zu einem gemeinsamen Standpunkt zu den speziellen Fragen der Förderung der Informationsfreiheit in Europa und zur Harmonisierung der entsprechenden Gesetzgebung zu gelangen, vereinbaren die Unterzeichner eine ständige Zusammenarbeit in der

Europäischen Konferenz der Informationsbeauftragten.

Berlin, 25. November 2005

Parlamentarischer Beauftragter
für Datenschutz und Informationsfreiheit
Republik Ungarn

Beauftragte für den Zugang
zu öffentlichen Informationen
Republik Slowenien

Schwedischer Parlamentarischer Ombudsman

Bundesbeauftragter für den Datenschutz
(und die Informationsfreiheit), Deutschland

Berliner Beauftragter
für Datenschutz und Informationsfreiheit,
Deutschland

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht,
Brandenburg, Deutschland

Der Landesbeauftragte
für den Datenschutz
Mecklenburg-Vorpommern,
Deutschland

Die Schriftenreihe „Dokumente zu Datenschutz und Informationsfreiheit“ wird gemeinsam von der 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 und zur Informationsfreiheit veröffentlicht.

Der vorliegende Band mit Dokumenten aus dem Jahr 2005 enthält die relevanten 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,
- Europäischen Konferenz der Informationsbeauftragten.