Dokumente
zu Datenschutz
und Informationsfreiheit
2007

Impressum

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

Druck: Druckerei Feller

Stand: Januar 2008

Inhaltsverzeichnis

Vorwort

Wie in einem Brennglas bündeln sich die aktuellen Themen der datenschutzrechtlichen Diskussion in den Beschlüssen der Datenschutzbeauftragten und Aufsichtsbehörden auf nationaler und internationaler Ebene. So hat sich die Konferenz der Datenschutzbeauftragten 2007 mehrfach mit der Telekommunikationsüberwachung und Vorratsdatenspeicherung sowie mit der Online-Durchsuchung auseinandergesetzt. Aber auch der geplante elektronische Einkommensnachweis (ELENA), die Gefährdung der anonymen Fernsehnutzung durch neue technische Entwicklungen, der Arbeitnehmerdatenschutz, Zuverlässigkeitsüberprüfungen bei Großveranstaltungen und die auf Bundesebene vorgesehene zentrale Steuerdatei waren Themen, zu denen die Datenschutzkonferenz Stellung genommen hat.

Positiv hervorzuheben ist, dass die im Düsseldorfer Kreis zusammenarbeitenden Obersten Aufsichtsbehörden stärker als in der Vergangenheit öffentlich zu Entwicklungen des Datenschutzes im nicht-öffentlichen Bereich Stellung genommen haben. Dazu zählte das SWIFT-Verfahren, die RFID-Technologie, das Kreditscoring, der internationale Datenverkehr und die Anwendung des Bundesdatenschutzgesetzes auf Rechtsanwälte.

Auf europäischer und internationaler Ebene standen der Datenschutz in der sog. Dritten Säule (Justiz und Inneres) und der Transfer von Passagierdaten im Mittelpunkt des Interesses. Sowohl die Europäische als auch die Internationale Konferenz der Datenschutzbeauftragten haben sich zu diesen Problemen geäußert. Insgesamt ist auf europäischer Ebene eine Tendenz festzustellen, dass die Regierungen der Mitgliedstaaten den Datenaustausch untereinander in den Bereichen Justiz und Inneres immer mehr erleichtern, ohne zugleich für die notwendige rechtsstaatliche Kontrolle solcher Datenflüsse zu sorgen.

Schließlich hat die Konferenz der Informationsbeauftragten in Deutschland mehr Transparenz beim Umgang mit Betriebs- und Geschäftsgeheimnissen gefordert, was nur vordergründig paradox erscheint. Zu pauschal werden solche Begriffe nämlich häufig dazu verwandt, um über legitime Geheimhaltungsinteressen hinaus den Informationszugang zu erschweren.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 73. Konferenz vom 8./9. März 2007 in Erfurt

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten,

dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen . Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,

- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.

- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.

- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.

- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

2. Entschließung zwischen der 73. und der 74. Konferenz (vom 8. Juni 2007)

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben

hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

3. Entschließungen der 74. Konferenz vom 25./26. Oktober 2007 in Saalfeld

Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen

nicht von langer Dauer sein werden. So begründen z. B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche – teilweise sensible – Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektro-

nisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87 a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139 b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139 b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsauf-

träge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

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

1. Beschlüsse der Sitzung am 19./20. April 2007 in Hamburg

Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

Die Übermittlung von personenbezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4 a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Die Zulässigkeit einer Weitergabe von Kundendaten in dem genannten Umfang kann nicht auf § 28 BDSG gestützt werden, da sie nicht der Zweckbestimmung des Vertragsverhältnisses des Versandhandelsunternehmens mit dem Kunden dient (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und die schutzwürdigen Interessen der Kunden an dem Ausschluss der Weitergabe ihrer Daten an Auskunfteien überwiegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Die Kunden, die im Versandhandel bestellen, müssen nicht damit rechnen, dass ihr bisheriges Kundenverhalten gegenüber einem Versandhaus entscheidend dafür sein kann, ob sie Lieferungen von anderen Unternehmen erhalten, die bei einer Auskunftei Bonitätsauskünfte einholen. Die Kunden dürfen nicht zum Objekt wirtschaftlichen Handelns dadurch gemacht werden, dass der Handel selbst definiert, was für die Kunden bzw. ihre Daten gut ist. Sie haben daher ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Vermarktung ihrer positiven Bonitätsdaten.

Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen

(In der Fassung vom 26. Juni 2007)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4 a BDSG zulässig.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4 a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die „Verbraucherauskunfteien“.

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4 a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Mahnung durch Computeranruf

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

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

Kreditscoring / Basel II

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:

I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?

1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.

2. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Abs. 9 BDSG nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)

3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein

Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben.

Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist.

Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG herangezogen werden. § 10 Abs. 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personenbezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potentiellen) Kundinnen und Kunden. Die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen.

Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potentiellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.

II. Wie transparent müssen die Bewertungen für die Betroffenen sein?

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;

2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;

3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6 a BDSG zu beachten.

Internationaler Datenverkehr

Der Düsseldorfer Kreis beschließt das anliegende **Positionspapier** zum internationalen Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG „Internationaler Datenverkehr“ an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.

Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.

Der Düsseldorfer Kreis beschließt ferner die anliegende **Handreichung** zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

Anlage 1

Abgestimmte Positionen der Aufsichtsbehörden in der AG „Internationaler Datenverkehr“ am 12./13. Februar 2007
– Bezug: Protokoll der Sitzung mit Wirtschaftsvertretern am 23. Juni 2006 –

I. Bestimmung der „datenexportierenden Stelle“ nach §§ 4 b, 4 c BDSG

1. Faustregel: Wer öffnet die Tür zum Datenexport?
   Maßgebliches Entscheidungskriterium ist die Entscheidungsbefugnis über den Datenexport in das Drittland (z. B. Entscheidung über die Zuteilung/Vergabe von Zugriffsrechten). Die Befugnis verbleibt grundsätzlich beim Datenverarbeiter in Deutschland.

2. Rechtlich unselbständige Niederlassungen können übermittelnde Stellen i. S. v. §§ 4 b, 4 c BDSG sein.

3. Rechtlich unselbständige Niederlassungen sind nicht Antragsteller oder Adressat von Genehmigungsverfahren.

4. Ein Standardvertrag zwischen einem Unternehmen und seiner rechtlich unselbständigen Niederlassung ist nicht möglich, da dies ein In-Sich-Geschäft wäre. Eine (zugangs-, aber nicht empfangsbedürftige) Garantieerklärung (durch die ein Garantievertrag mit den betroffenen Personen zustande kommt) ist daher erforderlich.

5. Eine Zulässigkeitsprüfung in der 1. Stufe unabhängig von derjenigen in der 2. Stufe erfolgt in den Fällen, in denen deutsche Niederlassungen Daten an den europäischen Hauptsitz übermitteln (z. B. zum Abruf von dort durch den US-Konzernhauptsitz). Gleichwohl können Fragestellungen der 2. Stufe bei der Prüfung der 1. Stufe von Bedeutung sein.

II. Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ – Auswirkungen bzw. Bedeutung und Umsetzung der Ergebnisse beim Drittstaatentransfer

1. Die Verbindlichkeit von Betriebsvereinbarungen im Drittland wird durch „Unterwerfungserklärung“ des Datenimporteurs hergestellt.

2. Der alternative Standardvertrag ist grundsätzlich für Arbeitnehmerdaten nicht geeignet (und evt. ergänzungsbedürftig), da die Haftung und Auskunftspflicht des Datenexporteurs (des deutschen Arbeitgebers) einge-

schränkt sind. Wertungswidersprüche zum deutschen Recht (1. Stufe) sind zu vermeiden.

3. Bei allen Standardverträgen sind auch die Anforderungen nach nationalem Recht (1. Stufe) zu erfüllen, ggf. durch eine Zusatzvereinbarung (z. B. des Einwilligungserfordernisses statt Widerspruchsrecht). Wertungswidersprüche zum deutschen Recht (1. Stufe) sind zu vermeiden (vgl. Art. 2 der Kommissionsentscheidungen vom 15. Juni 2001 und 27. Dezember 2001).

4. Bei Änderung eines Standardvertrages, die eindeutig zugunsten des Betroffenen ausfällt, besteht u. U. keine Genehmigungspflicht nach § 4 c Abs. 2 BDSG, was durch Rückfrage bei der zuständigen Aufsichtsbehörde zu klären ist.

5. Die Antwort 4 zu FAQ 9 / Safe Harbor-Entscheidung hat nur deklaratorische Wirkung, kann also Rechte der betroffenen Arbeitnehmer gegen den Arbeitgeber in Deutschland / EU weder begründen noch beschränken, sondern gibt nur das Verständnis der US-Seite bezüglich des EU-(Arbeits-) Rechts wieder. Die Unternehmen tragen die Darlegungslast für die Arbeitnehmerrechte, die sicherzustellen sind.

III. Gelten bei der Datenweitergabe von einem in Deutschland befindlichen Datenverarbeitungsdienstleister an seinen im Drittstaat befindlichen Auftraggeber die Anforderungen der §§ 4 b, 4 c BDSG?

1. Der Auftraggeber (AG) im Drittland muss das BDSG nach § 1 Abs. 5 Satz 2 bei der Datenverarbeitung durch den deutschen Auftragnehmer (AN) berücksichtigen, wenn der AG auf automatisierte Mittel zur Datenverarbeitung in Deutschland zurückgreift.

2. Bei der (Rück-)Übermittlung durch den AN an den AG gelten die §§ 4 b, 4 c BDSG nicht (insofern neue Ansicht), unter anderem weil nach § 3 Abs. 8 Satz 3 BDSG der Auftragnehmer in Deutschland nicht Dritter im Verhältnis zur verantwortlichen Stelle ist und somit keine Übermittlung i. S. v. § 3 Abs. 4 Nr. 3 BDSG stattfindet. Die Rückausnahme, die § 3 Abs. 8 Satz 3 BDSG selbst impliziert, nämlich dass Auftragnehmer außerhalb des EWR Dritte sind, greift nicht für den Auftraggeber im Drittstaat.

3. Für die Verarbeitung in Europa und die Rückübermittlung durch deutsche AN an AG im Drittland gelten die technisch-organisatorischen sowie bestimmte materiell-rechtliche Regelungen des BDSG (d. h. nur §§ 28 ff, nicht §§ 4 b, 4 c BDSG). Adressat der Aufsichtsbehörde zur Durchsetzung

der materiell-rechtlichen Vorschriften ist weiterhin nur der Auftraggeber. Den AN trifft gegenüber dem AG eine „qualifizierte Remonstrationspflicht“ bei Kenntniserlangung von Umständen i. S .v. § 11 Abs. 3 Satz 2 BDSG.

4. Wegen § 1 Abs. 5 BDSG gilt materielles Datenschutzrecht, wenn die Daten in Deutschland verarbeitet werden (siehe 1.). Bei der Anwendung insbesondere des § 28 BDSG ist aber der besonderen Sachlage der Auftragsdatenverarbeitung Rechnung zu tragen. Einerseits ist das berechtigte Interesse des Auftraggebers, im Rahmen seiner Organisationsentscheidungen auch Datenverarbeitungsschritte auf Auftragnehmer (AN) zu verlagern, bei § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu betrachten. Die schutzwürdigen Interessen der Betroffenen sind andererseits entsprechend der jeweiligen Fallkonstellation zu gewichten. In diesem Zusammenhang sind grundsätzlich auch die Wertungen der Rechtsordnungen im Drittstaat von Bedeutung, sofern sie nicht gegen den „ordre public“ in Deutschland (z. B. bei Menschenrechtsverletzungen) verstoßen.

5. Deutsches materielles Recht gilt nicht, wenn der deutsche AN nicht auf die vom AG übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System / Black Box oder verschlüsselt erfolgt).

Anlage 2

Fallgruppen zur internationalen Auftragsdatenverarbeitung

Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung

Einleitung

Die folgende Darstellung beinhaltet die häufigsten Fallkonstellationen der internationalen Auftragsdatenverarbeitung und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Alle Grafiken stammen vom Regierungspräsidium Darmstadt, Dezernat Datenschutz.

Fallgruppe A

Fallgruppe B

Erläuterung der Bewertung zur Fallgruppe B

Fallgruppe C

Fallgruppe D

Fallgruppe E

Erläuterung der Bewertung zu den Fallgruppen C, D, E

Fallgruppe F

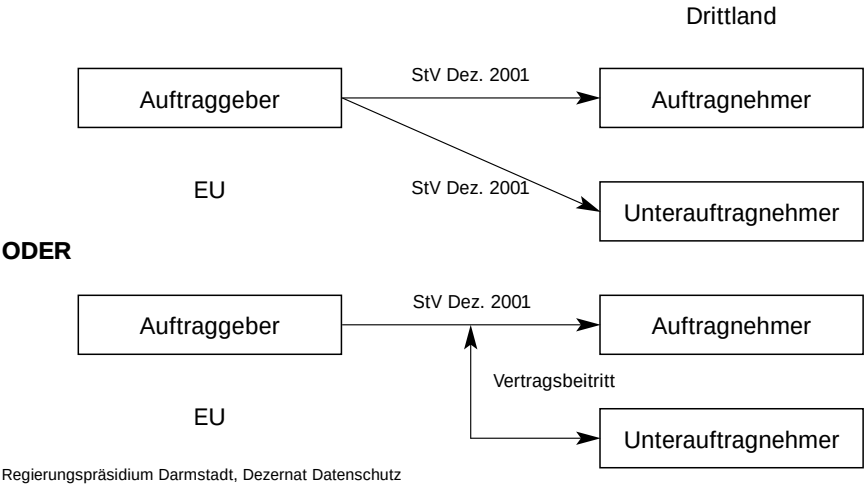
Fallgruppe G

Fallgruppe H

Fallgruppe I

Erläuterung der Bewertung zu den Fallgruppen F, G, H, I

Fallgruppe A



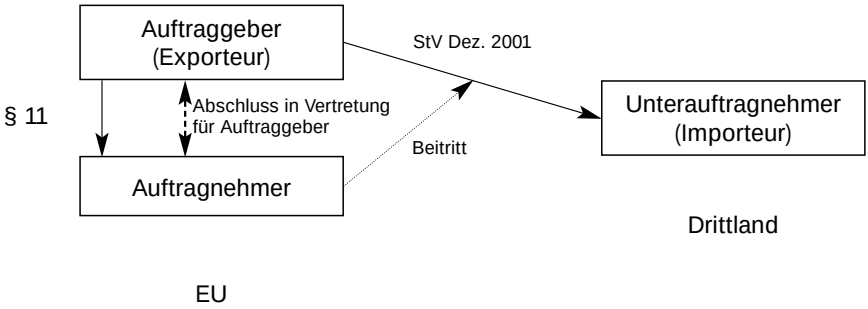
Regierungspräsidium Darmstadt, Dezernat Datenschutz

Konstellation:
Der Auftraggeber ist in der EU/EWR ansässig, während der Auftragnehmer und der von ihm beauftragte Unterauftragnehmer im Drittland ansässig sind.

Besonderheit:
Die Pflichten des Auftragnehmers sind an den Unterauftragnehmer „weiterzuleiten".

Bewertung:
Der Auftraggeber hat einen weiteren „Drittstaatenvertrag" mit dem Unterauftragnehmer zu schließen, oder der Unterauftragnehmer muss dem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer beitreten.

Fallgruppe B



Konstellation:
Der Auftraggeber und der Auftragnehmer sind in der EU/EWR ansässig. Es wird ein Unterauftragnehmer im Drittland eingeschaltet, der die Daten vom Auftragnehmer erhält.

Besonderheit:
Der Abschluss eines Standardvertrags zwischen Auftragnehmer in der EU/EWR und dem Unterauftragnehmer im Drittland ist nicht sachgerecht, weil der Auftragnehmer (anders als der Datenexporteur in den Standardverträgen) nicht verantwortliche Stelle ist. Der Auftragnehmer hat dann selbst keine vertraglichen Rechte oder Pflichten.

Bewertung:
Der Auftraggeber ist als Datenexporteur i. S. d. §§ 4 b, 4 c einzustufen, der Unterauftragnehmer als Datenimporteur. Beide müssen daher Vertragsparteien des Standardvertrages vom Dez. 2001 sein. Ein Beitritt des Auftragnehmers in der EU/EWR zum Vertrag ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

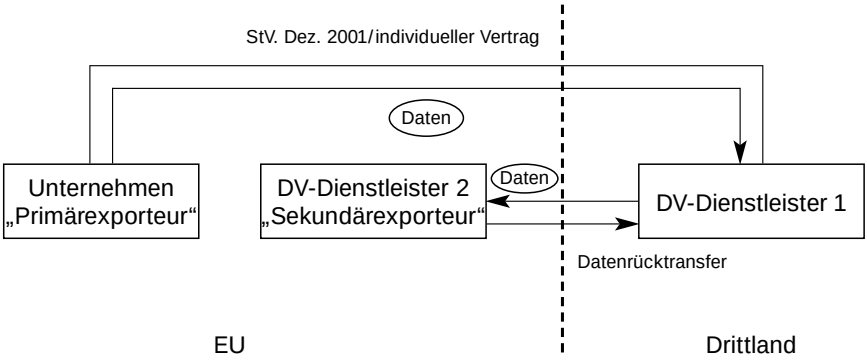
Erläuterung der Bewertung zur Fallgruppe B:

Da u. U. wegen der möglichen Vielzahl von Auftraggebern entsprechend viele Standardverträge mit den Unterauftragnehmern abgeschlossen werden müssten, ist es praktikabel und akzeptierbar, dass der Auftragnehmer im Auftrag (oder besser: in Vertretung) der Auftraggeber einen Standardvertrag (Auftragsdatenverarbeitung) mit dem Unterauftragnehmer abschließt. Dass auch der EU/EWR-Auftragnehmer dem Vertrag zwischen Auftraggeber und Drittstaaten-Unterauftragnehmer beitritt, ist jedenfalls sinnvoll. Bei einem Beitritt besteht keine Genehmigungspflicht nach § 4 c Abs. 2 BDSG, und zwar unabhängig davon, ob er durch eine gesonderte Vereinbarung erfolgt oder als Vertragsergänzung in den „Drittstaatenvertrag“ integriert wird.

Folgender Text kann für einen derartigen Beitritt verwendet werden:

„Die vorstehenden Regelungen gelten mit folgender Maßgabe auch für den DV-Dienstleister in Europa [Name, Sitz], der insoweit dem Vertrag beitritt. Da der Datenexporteur einen Datenverarbeitungsdienstleistungsvertrag mit [Name des DV-Dienstleisters in Europa] geschlossen hat (als Auftragsdatenverarbeitung gemäß § 11 BDSG / Art. 2 e, 17 Abs. 3 EG-Datenschutzrichtlinie 95/46/EG und den hierzu erlassenen nationalen Vorschriften) und der Datenimporteur als „Unterauftragnehmer“ (oder: Subunternehmer) für [Name des DV-Dienstleisters in Europa] fungiert, ist der/die [Name des DV-Dienstleisters in Europa] gegenüber dem Datenexporteur primär verantwortlich, dass der Datenimporteur die Pflichten gemäß diesem Vertrag erfüllt. Der [Name des DV-Dienstleisters in Europa] hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber dem Datenimporteur und kann hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Datenexporteurs wahrnehmen. Dieser bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen, und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben.“

Fallgruppe C



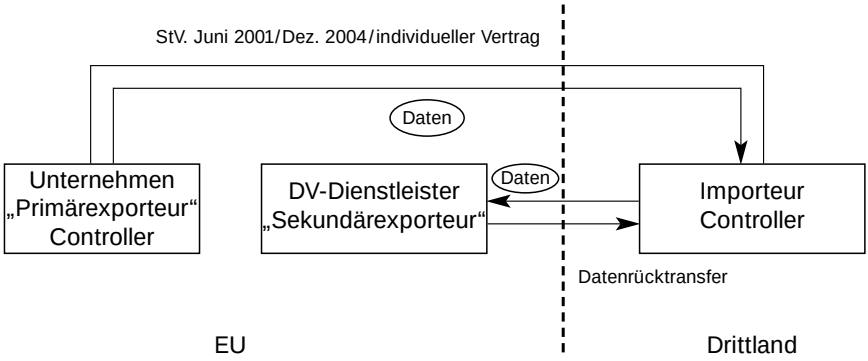
Konstellation:
Ein in der EU/EWR ansässiges Unternehmen beauftragt einen im Drittstaat ansässigen DV-Dienstleister mit der Verarbeitung personenbezogener Daten und schließt mit diesem den Standardvertrag vom Dezember 2001 (Controller – Processor) oder einen entsprechenden individuellen Vertrag. Der DV-Dienstleister im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-)transferiert.

Besonderheit:
Der Dienstleister in der EU (DV-Dienstleister 2) erhält Daten vom DV-Dienstleister im Drittland (DV-Dienstleister 1). Ein Vertrag besteht nur zwischen dem Unternehmen und dem DV-Dienstleister 1.

Bewertung:
Es besteht keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4 c Abs. 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittland-Unternehmen. Ein Beitritt des EU-/EWR-Dienstleisters zum „Drittstaatenvertrag“ ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

Fallgruppe D



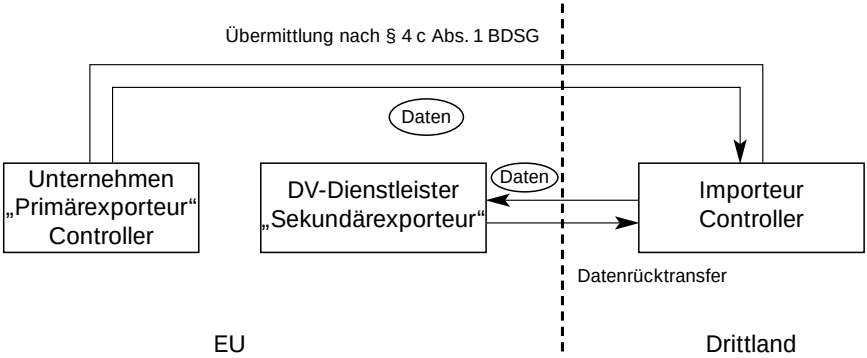
Konstellation:
Ein in der EU/EWR ansässiges Unternehmen übermittelt Daten an ein Unternehmen im Drittstaat und schließt mit diesem den Standardvertrag vom Juni 2001 oder Dezember 2004 (Controller – Controller) oder einen entsprechenden, individuellen Vertrag. Das Unternehmen im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-)transferiert.

Besonderheit:
Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:
Es besteht (wie bei Fallgruppe C) keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4 c Abs. 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen. Ein Beitritt zum „Drittstaatenvertrag“ ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

Fallgruppe E



Konstellation:
Wie in Fallgruppe D, aber zwischen dem in der EU/EWR ansässigen Unternehmen und dem Unternehmen im Drittstaat wird kein „Drittstaaten-Vertrag“ gemäß § 4c Abs. 2 BDSG abgeschlossen, weil eine der Katalogausnahmen des § 4 c Abs. 1 BDSG gegeben ist.

Besonderheit:
Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:
Es besteht (wie bei Fallgruppen C und D) keine Notwendigkeit einer eigenständigen vertraglichen Regelung zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen.

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen C, D und E:

Die Fallgruppen C, D und E sind dadurch gekennzeichnet, dass die Daten von einer verantwortlichen Stelle, die quasi der „Primär-Exporteur“ ist, in ein Drittland transferiert und hierbei die Voraussetzungen des § 4 c BDSG erfüllt wurden.

Der DV-Dienstleister in der EU/EWR ist quasi der „Sekundär-Exporteur“. Ungeachtet der grundsätzlichen Frage, inwieweit EU/EWR-Auftragnehmer überhaupt verantwortlich sind für das Vorliegen der Voraussetzungen der §§ 4 b, 4 c BDSG (s. hierzu Näheres zu den Fallgruppen F bis I), ist jedenfalls in den Fallgruppen C, D und E keine eigenständige vertragliche Regelung im Sinne des § 4 c Abs. 2 BDSG zwischen dem EU/EWR-Dienstleister und dem Drittstaaten-Unternehmen erforderlich.

Offensichtlich ist dies bei der **Fallgruppe C**, bei der sich der eigentliche Auftraggeber in der EU/EWR befindet. Da Zweck und Umfang der zulässigen Datenverarbeitung, die einzuhaltenden Datensicherheitsmaßnahmen etc. bereits in dem Vertrag zwischen dem EU/EWR-Auftraggeber und dem Drittstaaten-Auftragnehmer geregelt sind, besteht weder ein Erfordernis noch ein Spielraum für den EU/EWR-Unterauftragnehmer für eigenständige Vorgaben gegenüber dem Drittstaatenunternehmen bzgl. der dortigen Datenverarbeitung.

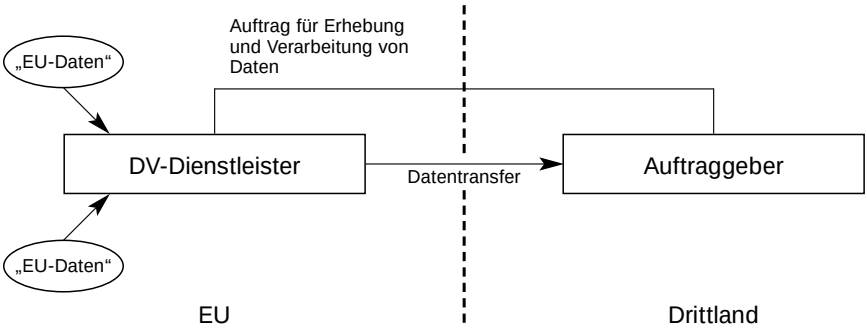
Würde man einen individuellen – genehmigungsbedürftigen – Vertrag mit dem EU/EWR-Unterauftragnehmer für erforderlich halten (die Standardverträge passen hier nicht), dann würde dies sogar die Gefahr bergen, dass Regelungen getroffen werden, die dem Vertrag zwischen dem EU-Auftraggeber und dem Drittstaaten-Unternehmen widersprechen.

Gleiches gilt für die **Fallgruppe D**. Wenngleich sich hier – im Unterschied zu C – der „Auftraggeber“ im Drittstaat befindet, wurden doch auch hier bereits umfassende Regelungen zur Gewährleistung ausreichender Datenschutzgarantien im Drittstaat getroffen, sodass für den EU/EWR-Auftragnehmer kein Erfordernis und kein Spielraum für eigene Vorgaben bestehen. Ein Beitritt des EU/EWR-Auftragnehmers zu dem Vertrag zwischen dem „Primär-Datenexporteur“ und dem Datenimporteur ist in den Fallgruppen C und D sinnvoll. Wenn kein DV-Dienstleistungsvertrag existiert, der den Vorgaben des § 11 BDSG entspricht, kann diese Lücke durch Beitritt zum Vertrag geschlossen werden.

In der **Fallgruppe E** besteht zwar kein Vertrag zwischen dem „Primär-Datenexporteur“ und dem Datenimporteur zur Gewährleistung ausreichender Datenschutzgarantien (ein Beitritt scheidet daher aus), allerdings wäre es nicht gerechtfertigt, an den „Sekundär-Datenexporteur“ strengere Anforderungen zu stellen als an den „Primär-Datenexporteur“.

Der Abschluss eines – genehmigungsbedürftigen – Vertrags im Sinnes des § 4 c Abs. 2 BDSG zwischen EU-Auftragnehmer und Drittstaatenunternehmen ist auch in der Fallgruppe E nicht erforderlich.

Fallgruppe F



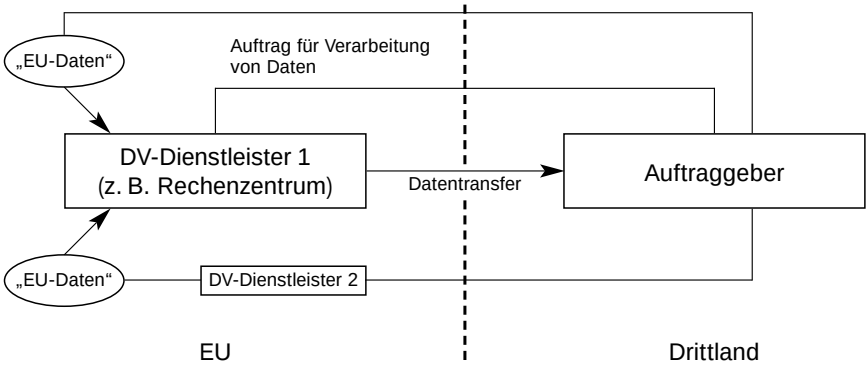
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister wird von einem in einem Drittland ansässigen Unternehmen beauftragt, in der EU/EWR personenbezogene Daten zu erheben und zu verarbeiten und dann an den Auftraggeber im Drittstaat zu transferieren.

Besonderheit:
Der Auftraggeber im Drittland beauftragt den DV-Dienstleister in der EU/EWR auch zusätzlich mit Datenerhebungen in der EU/EWR. Der DV-Dienstleister bleibt zwar auch Datenverarbeiter, kennt die Daten aber selbst (im Unterschied zur Fallgruppe G).

Bewertung:
Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i. V. m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4 b, 4 c BDSG. U. U. trifft ihn aber eine „Remonstrationspflicht“. Bezüglich der selbst erhobenen Daten muss er eine summarische Plausibilitätsprüfung vornehmen.

Näheres hierzu: s. Erläuterungen.

Fallgruppe G



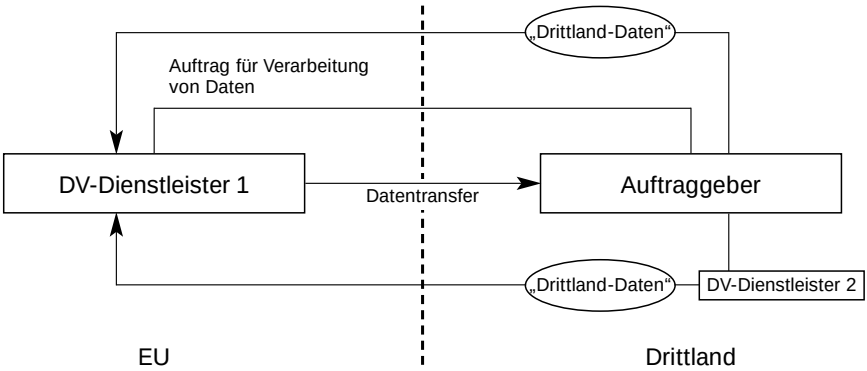
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister 1 wird von einem in einem Drittland ansässigen Unternehmen beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu transferieren. Die Daten stammen aus der EU / dem EWR. Sie wurden hier entweder vom Auftraggeber selbst oder in dessen Auftrag von einem DV-Dienstleister 2 erhoben.

Besonderheit:
Die Daten für den DV-Dienstleister 1 in der EU/EWR kommen vom Auftraggeber aus dem Drittland sowie vom europäischen DV-Dienstleister 2.

Bewertung:
Der DV-Dienstleister 1 ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i. V. m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister 1 hat selbst keine Verantwortung im Sinne der §§ 4 b, 4 c BDSG. U. U. trifft ihn aber eine „Remonstrationspflicht“.

Näheres hierzu: s. Erläuterungen.

Fallgruppe H



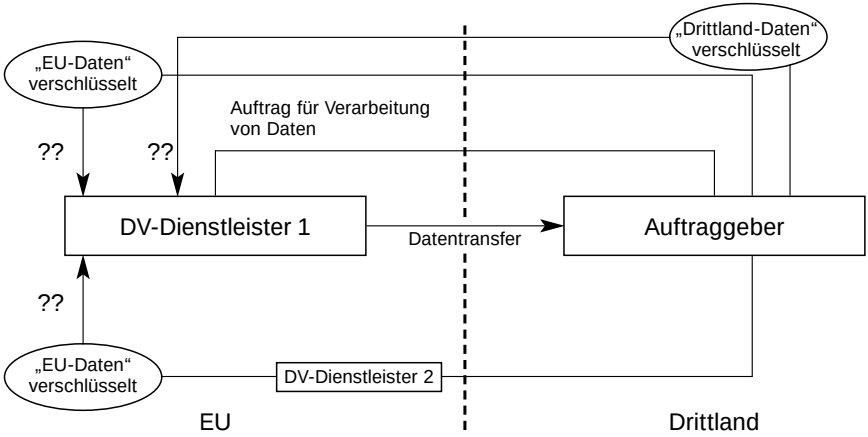
Konstellation:
wie Fallgruppe G, aber die Daten stammen nicht aus der EU/EWR, sondern aus dem Drittland. Sie werden in der EU/EWR nur verarbeitet und dann zurückübermittelt.

Besonderheit:
Die aus dem Drittland stammenden Daten wurden nach dortigem Recht zulässig erhoben. Nach deutschem Recht wäre die Erhebung unzulässig gewesen.

Bewertung:
Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i.V.m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U. U. trifft ihn aber eine „Remonstrationspflicht".

Näheres hierzu: s. Erläuterungen.

Fallgruppe I



Konstellation:
Wie Fallgruppe G oder H, aber der EU/EWR-Dienstleister erhält die Daten in verschlüsselter Form und kann von dem Inhalt keine Kenntnis nehmen.

Besonderheit:
Der DV-Dienstleister in der EU/EWR kennt die Daten aus dem Drittland nicht (Black Box-Konstellation).

Bewertung:
Deutsches materielles Recht gilt weder für die DV-Dienstleister noch für den Auftraggeber, wenn der deutsche AN nicht auf die vom AG übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System oder verschlüsselt erfolgt, ohne dass der AN über den Schlüssel verfügt).

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen F, G, H, I:

Nach § 1 Abs. 5 Satz 2 BDSG findet dieses Gesetz Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Für die Verarbeitung durch den DV-Dienstleister in Deutschland gilt somit das BDSG. Der DV-Dienstleister ist grundsätzlich nur für

die Datensicherheit der von ihm durchgeführten Datenverarbeitung nach Maßgabe der Regelungen in § 11 i. V. m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie verantwortlich. Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich.

Bei den Fallgruppen F, G, H und I gibt es keine „Primär-Datenexporteure", die für das Vorliegen der Voraussetzungen des § 4 c BDSG beim Drittstaaten-Auftraggeber zu sorgen haben. Die Frage der eigenen Verantwortlichkeit des EU/EWR-Auftragnehmers wird hier also besonders virulent. Fraglich ist, ob ihn weitere (über die vorgenannten hinausgehenden) Pflichten treffen.

Hinsichtlich der **Fallgruppen F bis I** ist zu fragen, ob sich für den Auftragnehmer aus § 1 Abs. 5 Satz 2 BDSG die Pflicht ergibt zu prüfen und sicherzustellen, dass beim (Rück-) Transfer der Daten die Voraussetzungen des § 4 c BDSG (bzw. des § 4 b BDSG) erfüllt werden. Würde man eine solche Pflicht annehmen, müsste der Auftragnehmer eine umfassende Prüfung der gesamten Datenverarbeitung vornehmen, also eine umfassende Prüfung des Zwecks der gesamten Datenverarbeitung sowie des Kontextes und der Umstände der Datenverarbeitung. Die bloße Vereinbarung mit dem Auftraggeber im Drittstaat, dass die Daten von jenem nur zu dem Zweck weiterverarbeitet werden dürfen, zu dem der Auftragnehmer die Daten erhalten hat, würde keinesfalls reichen. Eine Verantwortung gemäß §§ 4 b, 4 c BDSG würde vielmehr eine eigenständige umfassende Prüfung durch den Auftragnehmer erfordern. Dieser kennt aber höchstwahrscheinlich nur einen kleinen Ausschnitt der Datenverarbeitung und des Verwendungszusammenhanges. Die Rechtmäßigkeit der Verarbeitung von Daten im Konzernzusammenhang etwa wird er oft nur schwerlich beurteilen können. Er kann im Unterschied zu den Fallgruppen A – E gerade nicht auf einen vorhandenen Regelungsrahmen verweisen oder Bezug nehmen.

Deshalb ist zu konstatieren, dass es in den meisten Fällen für den Auftragsverarbeiter in Deutschland (EU/EWR) unmöglich sein dürfte, eine umfassende Prüfung i. S. d. §§ 4 b, 4 c BDSG vorzunehmen, um beurteilen zu können, ob eine Katalogausnahme gegeben ist, oder um vertragliche Regelungen i. S. d. § 4 c Abs. 2 BDSG treffen zu können. Bezüglich etwaiger vertraglicher Regelungen i. S. d. § 4 c Abs. 2 BDSG wäre im übrigen unklar, welche konkrete Rolle mit welchen Pflichten der Auftragsverarbeiter hierin übernehmen sollte (Einstandspflicht für Betroffenenrechte wie Auskunfts- und Haftungsanspruch?).

Aus alledem ergibt sich, dass der Auftragsverarbeiter in Deutschland (EU/EWR) keine Verantwortung i. S. d. §§ 4 b, 4 c BDSG hat. Der Gesetzgeber hat in § 1 Abs. 5 BDSG der Stelle im Drittstaat selbst die umfassende Verantwortung für die Vereinbarkeit der Datenverarbeitung mit dem BDSG zugewiesen, nicht dem Auftragsverarbeiter, dessen sich der Auftraggeber im Drittstaat bedient.

Den Auftragnehmer in Deutschland trifft aber eine qualifizierte Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG sowie unter Umständen eine Pflicht zur materiellen Plausibilitätsprüfung bezüglich der von ihm selbst in Deutschland vorgenommenen Datenerhebungen, -verarbeitungen und -nutzungen.

Daraus ergeben sich folgende Konsequenzen:

a) **Fallgruppe F**
Wenn der DV-Dienstleister die Daten selbst zu erheben hat, so ist damit in aller Regel eine inhaltliche Kenntnisnahme der Daten verbunden. Daher hat der DV-Dienstleister summarisch auf Plausibilität zu prüfen, ob die Datenerhebung und -verarbeitung und die diesbezüglichen Weisungen des Auftraggebers mit dem BDSG vereinbar sind. Wenn nein, gelten die unter b) genannten Anforderungen.

b) **Fallgruppe G**
Die DV-Dienstleistung wird häufig in der Rechenzentrums-Dienstleistung bestehen, so dass eine inhaltliche Kenntnisnahme der Daten durch den Auftragsverarbeiter nicht vorgesehen ist. Der Auftragsverarbeiter hat lediglich für die Datensicherheit zu sorgen, er hat keine Prüfungspflicht bzgl. der Vereinbarkeit der Datenverarbeitung mit dem BDSG.

Soweit ihm jedoch (aufgrund besonderer Hinweise Dritter o. ä.) bekannt wird, dass die Datenverarbeitung gegen das BDSG verstößt, hat er eine qualifizierte Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG. Gleiches gilt in den Einzelfällen, bei denen dem Auftragsverarbeiter bekannt wird, dass offensichtlich (eindeutig) kein angemessenes Datenschutzniveau (ausreichende Datenschutzgarantien) beim Auftraggeber besteht und auch eindeutig kein Ausnahmetatbestand i. S. d. § 4 c Abs. 1 BDSG gegeben ist.

In diesen Fällen, in denen der Auftraggeber einen gravierenden Missstand trotz Hinweisen des Auftragsverarbeiters nicht abstellt, ist eine Hinweis-/Anzeigepflicht des Auftragsverarbeiters gegenüber der Datenschutzaufsichtsbehörde gegeben. Gegebenenfalls besteht somit unter Umständen die Pflicht des Auftragsverarbeiters, die weitere Ausführung des Auftrages einzustellen. Dann entscheidet die Aufsichtsbehörde, wie weiter zu verfahren ist.

c) Die **Fallgruppe H** bedarf besonderer Betrachtung:
In Drittstaaten können bestimmte Verarbeitungen personenbezogener Daten explizit vorgeschrieben sein, die in Deutschland unzulässig wären (z. B. die Verarbeitung der Sozialversicherungsnummern von Kunden, die die Funktion eines Personenkennzeichens haben). Zwar gilt das BDSG grundsätzlich unabhängig davon, ob die Betroffenen Personen in Deutschland ansässig sind oder

nicht. Allerdings wird mit der Sondervorschrift des § 1 Abs. 5 Satz 2 BDSG der reguläre Anwendungsbereich des BDSG ohnehin ausgedehnt, so dass hier eine Relativierung möglich erscheint. Ob der Gesetzgeber bzw. die Europäische Datenschutzrichtlinie bei der Regelung des § 1 Abs. 5 Satz 2 BDSG (bzw. Art. 4 Abs. 1c) Richtlinie) einen „EU/EWR-Bezug" der Daten stillschweigend unterstellt hat, bleibt unklar.

Die Lösung besteht darin, dass zwar aus § 1 Abs. 5 Satz 2 BDSG keine umfassende Geltung des deutschen Datenschutzrechts abzuleiten wäre, aber Verarbeitungen, die eindeutig gegen unseren „ordre public" verstoßen (z. B. bei Menschenrechtsverletzungen), unzulässig sind, auch wenn die Daten keinerlei EU/EWR-Bezug aufweisen. Demzufolge besteht die qualifizierte Remonstrationspflicht des Auftragsverarbeiters (s. o. b)) nur bei derartigen Verstößen.

d) **Fallgruppe I**
Hier muss der Auftraggeber nicht die Regelungen des BDSG beachten, weil die Situation vergleichbar ist mit der Transitregelung des § 1 Abs. 5 Satz 4 BDSG. Es besteht auch keine weitere (über die technisch-organisatorische hinausgehende) Verantwortlichkeit des EU/EWR-Auftragnehmers. Der Grundsatz lautet hier: Deutsches materielles Datenschutzrecht gilt nicht, wenn der deutsche Auftragnehmer nicht auf die vom Auftraggeber übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System / Black Box oder verschlüsselt erfolgt).

2. Beschlüsse der Sitzung am 8./9. November 2007 in Hamburg

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.

Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring-Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.

Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen.

Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) – auch hinsichtlich mandatsbezogener Daten – auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43 a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

III. Europäische Konferenz der Datenschutzbeauftragten

Zypern, 10./11. Mai 2007

Erklärung von Zypern

Im Rat der Europäischen Union ist ein Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Gegenstand von Beratungen.

Die Schaffung eines harmonisierten und hohen Standards für den Datenschutz bei polizeilichen und justiziellen Maßnahmen in der Union ist in der Tat ein entscheidender Bestandteil der Achtung und des Schutzes von Grundrechten, wie des Rechts auf den Schutz personenbezogener Daten, bei der Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts.

Die Initiativen in der Europäischen Union zur Verbesserung der Bekämpfung von schweren Straftaten und Terrorismus haben das Ziel gemeinsam, nationale Grenzen innerhalb der Union zunehmend unwichtiger werden zu lassen, wenn es um die Bedingungen für den Austausch von Daten zwischen zuständigen Behörden geht. Daten für die Strafverfolgung sollen auf verschiedenen Wegen zugänglich gemacht werden, inklusive der Möglichkeit des direkten Zugriffs auf nationale Datenbestände.

Diese Initiativen zeigen deutlich, dass die Verpflichtung der Union zur Hilfe beim Kampf gegen schwere Straftaten und Terrorismus nicht auf die Schaffung der Bedingungen für den Informationsaustausch zwischen den Mitgliedstaaten beschränkt ist; klar erkennbar haben die Initiativen auch Auswirkungen auf die Datenverarbeitung auf nationaler Ebene, die jedem möglichen Austausch vorangeht. Es ist klar, dass jede Entwicklung auf diesem Gebiet abgewogen werden muss mit angemessenen und harmonisierten Datenschutzrechten und -verpflichtungen, wobei das gegenseitige Vertrauen in diese ein entscheidender Bestandteil ist.

Innerhalb der Europäischen Union unterscheidet sich die Datenschutz-Gesetzgebung für Maßnahmen der Strafverfolgung sowohl der Natur als auch der Sache nach. Sie gewährleistet somit sicherlich keinen harmonisierten Ansatz zum Datenschutz für Strafverfolgungs-Informationen, für die Rechte des Betroffenen sowie für eine effektive unabhängige Kontrolle.

Im Hinblick auf den zunehmenden Rückgriff auf die Verfügbarkeit („availability“) von Informationen als Konzept zur Verbesserung des Kampfes gegen schwere Straftaten, sowohl auf nationaler Ebene wie zwischen den Mitgliedstaaten, führt das Fehlen eines harmonisierten und hohen Standards für den Datenschutz in der Union zu einer Situation, in der das Grundrecht auf den Schutz personenbezogener Daten nicht mehr ausreichend gewährleistet wird.

Mit Bezugnahme auf ihr Positionspapier zu Strafverfolgung und Informationsaustausch in der EU (April 2005) und an ihre Erklärungen von Krakau (2005), Budapest (2006) und London (2006) erinnernd, ruft die gesamte Europäische Datenschutzkonferenz daher die im Rat der Europäischen Union und im Europäischen Parlament vertretenen Mitgliedstaaten dazu auf, einen solchen harmonisierten und hohen Standard des Datenschutzes in der Europäischen Union zu schaffen.

Die Europäische Datenschutzkonferenz ist sich über die Grundsatz-Diskussion im Rat über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses bewusst: sollte er nur auf Daten anwendbar sein, die zwischen Mitgliedstaaten ausgetauscht werden oder auf jegliche Verarbeitung durch Polizei- und Justizbehörden?

Die Europäische Datenschutzkonferenz weist wiederholt darauf hin, dass Initiativen der Union Auswirkungen auf nationaler Ebene haben und darauf, dass eine Begrenzung des Anwendungsbereiches auf Daten, die zwischen den Mitgliedstaaten ausgetauscht werden oder werden könnten, das Risiko besonderer Unsicherheiten und Unwägbarkeiten über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses mit sich bringen würde. Sie **betont, dass nur ein umfassender Anwendungsbereich unter Einschluss aller Arten der Verarbeitung personenbezogener Daten den notwendigen Schutz der Individuen gewährleisten kann**.

Die Europäische Datenschutzkonferenz **betont weiter, dass die von der deutschen Ratspräsidentschaft am 13. März 2007 vorgelegte Fassung des Entwurfs des Rahmenbeschlusses auch bezüglich anderer Datenschutz-Grundsätze keine verlässliche und strenge Datenschutzordnung enthält** und dass sie weder die Stellungnahme der Europäischen Datenschutzkonferenz vom 24. Januar 2006 noch die Stellungnahme des EP vom 18. Mai 2006 einbezogen hat.

Während der Entwurf einige Verbesserungen im Hinblick auf die Erreichung eines harmonisierten Rahmens für die Verarbeitung gebracht hat, ist er bislang unbefriedigend bei den Vorkehrungen zur Gewährleistung des Schutzes der Privatsphäre der Bürger. Dies muss besonders gelten, wenn man die bereits bestehende europäische Gesetzgebung zum Datenschutz berücksichtigt, insbesondere

den rechtlichen Rahmen, der von den nationalen Gesetzgebern bei der Umsetzung der Richtlinie 95/46/EG geschaffen wurde und der ebenfalls auf die Verarbeitung personenbezogener Daten in dem fraglichen Bereich anwendbar ist. Darüber hinaus wiederholt die Europäische Datenschutzkonferenz, dass es notwendig ist, die auf nationaler Ebene bestehenden Schutzvorkehrungen zum Datenschutz zu erhalten, indem ein bindendes europäisches Instrumentarium verabschiedet wird.

Mit dem Ziel einer tatsächlichen Verbesserung beim Datenschutz in der dritten Säule unterstreicht die Europäische Datenschutzkonferenz die folgenden Grundsätze, die bei dem wichtigen Gesetzgebungsakt Rahmenbeschluss zu beachten sind:

– Zweckbegrenzung: die Notwendigkeit, die gesetzlichen Zwecke genau zu definieren, zu denen die Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erlaubt ist, ohne irgendwelche Generalklauseln, die die weitere Verarbeitung „für jegliche andere Zwecke“ erlaubt. Das Prinzip der Zweckbegrenzung ist ein Grundsatz in der EU-Richtlinie und in der Konvention 108.

– Datenkategorien: die Verarbeitung besonderer Kategorien von Daten ist verboten, es sei denn besondere Bedingungen werden erfüllt und besondere Garantien werden in der nationalen Gesetzgebung gegeben (Artikel 8 EU-Richtlinie, Artikel 6 Konvention 108). Darüber hinaus sollen angemessene Sicherheitsvorkehrungen für die Verarbeitung biometrischer und genetischer Daten gewährleistet werden.

– Kategorien von Betroffenen: Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, Unterscheidungen zwischen den verschiedenen Kategorien von Personen wieder einzuführen, die von der Verarbeitung für Polizei und Strafverfolgung betroffen sind.

– Regelung der Weitergabe von Daten an Drittstaaten: Es ist ein Erfordernis des Zweckmäßigkeits-Grundsatzes, dass gemeinsame Kriterien definiert und ein Verfahren geschaffen wird, um den Datenschutz-Standard in einem Drittland oder einer internationalen Einrichtung einschätzen zu können, bevor personenbezogene Daten übertragen werden. Dies soll nicht allein dem Ermessen der Mitgliedstaaten überlassen werden. Die Festlegung eines EU-Standards für ein solches Verfahren ist erforderlich, um Harmonisierung in Europa zu erreichen, und das Prinzip der Feststellung eines angemessenen Datenschutzniveaus entspricht der Regelung durch das EuroparatsÜbereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

– Benachrichtigung des Betroffenen: Benachrichtigung des Betroffenen soll umfassend sein, einschließlich der Identität der für die Verarbeitung verantwortlichen Stelle, der möglichen Empfänger und der Rechtsgrundlage für die Verarbeitung. Jede Beschränkung soll präzise gefasst und begrenzt sein.

– Auskunftsrecht: Die Regelung zum Auskunftsrecht muss im Einklang mit den Anforderungen der Europäischen Menschenrechtskonvention und der Rechtsprechung stehen. Durch den Ausschluss eines wirksamen Beschwerderechts in einigen Fällen befindet sich der derzeitige Vorschlag nicht im Einklang mit diesen Anforderungen. Darüber hinaus soll die Kontrollinstanz oder das Beschwerdegericht das Recht haben, dem Betroffenen Informationen zu übermitteln, wenn ihm diese ungerechtfertigterweise vorenthalten wurden. Es sollte weniger Ausnahmen vom Auskunftsrecht geben.

– Anzeige und Vorabkontrolle: Anzeige gegenüber und Vorabkontrolle durch die Kontrollinstanz sollten, soweit angemessen, eine Vorbedingung für die Verarbeitung sein. Die Vorabkontrolle soll von den nationalen Datenschutzkontrollinstanzen vorgenommen werden. Die Möglichkeit von Ausnahmen bei der Veröffentlichung der Anzeige sollte je nach Art der Verarbeitung erwogen werden.

– Kontrollinstanzen: Eine Gemeinsame Kontrollbehörde (JSA) soll als unabhängige Kontrollinstanz konzipiert sein. Der Rahmenbeschluss soll Aussagen über deren Zusammensetzung, Aufgaben und Zuständigkeiten enthalten. Sie soll insbesondere mit der Befugnis zu Beratung, Nachforschung und zum Einschreiten ausgestattet sein.

Die Europäische Datenschutzkonferenz anerkennt auch die Wichtigkeit einer möglichst schnellen Verabschiedung des Rahmenbeschlusses. Jedoch wird der derzeit diskutierte Vorschlag keinen ausreichend harmonisierten und hohen Standard des Datenschutzes gewährleisten. Die grundlegende Bedeutung des Rahmenbeschlusses nicht nur für den Schutz der Rechte der Bürger der Europäischen Union, sondern auch für die Strafverfolgung, rechtfertigt eine Diskussion, die nicht durch einen engen Zeitrahmen gefährdet wird.

Die Europäische Datenschutzkonferenz ruft den Rat daher dazu auf, sich mehr Zeit für die Verhandlungen zur Entwicklung eines Rahmenbeschlusses zu nehmen, der einen hohen Datenschutz-Standard bietet.

Die Europäische Datenschutzkonferenz ist bereit, weiter zum Verfahren der Verabschiedung eines solchen Rahmenbeschlusses beizutragen und schlägt eine Anhörung der Arbeitsgruppe des Rates vor, um ihre Standpunkte darzulegen.

Gemeinsamer Standpunkt zur Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

ERKLÄRUNG

Die Europäische Union hat verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung und des Kampfes gegen den Terrorismus in der Europäischen Union eingeleitet. In diesem Zusammenhang ist der Austausch von Informationen zur Strafverfolgung in Übereinstimmung mit dem Verfügbarkeitsgrundsatz („principle of availability") eine Schlüsselfrage.

Angesichts dieser Entwicklungen rief die Europäische Datenschutzkonferenz die Mitgliedstaaten der Europäischen Union sowie die Kommission, den Rat und das Europäische Parlament dazu auf, tragfähige und harmonisierte Maßnahmen zur Sicherung des Datenschutzes einzuführen.[1]

Die verschiedenen Ausprägungen, in denen dieses Prinzip der „Verfügbarkeit" explizit oder implizit zur Entwicklung von Strategien und Rechtsakten zur Verbesserung der Effizienz bei der Strafverfolgung genutzt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effizienz von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen.

Die Konferenz hat den folgenden Gemeinsamen Standpunkt über die Anwendung des Verfügbarkeitsgrundsatzes bei der Strafverfolgung angenommen. Dieser Gemeinsame Standpunkt enthält eine Checkliste für die Beurteilung eines jeden Vorschlags, dessen Grundlage die Verfügbarkeit von personenbezogenen Daten ist.

Dieses Dokument und die Checkliste sind insbesondere an alle EU-Institutionen und die nationalen Parlamente adressiert, als ein konstruktiver Beitrag zur Achtung und Stärkung der bürgerlichen Freiheiten der in der EU lebenden Bürger bei der Ausweitung der Möglichkeiten zur Nutzung von Informationen durch Strafverfolgungsbehörden.

---

[1] Erklärung von Krakau, 25./26. April 2005,
Erklärung von Budapest, 24./25. April 2006.

Erläuternde Zusammenfassung

Im Zusammenhang mit dem Kampf gegen Terrorismus und zur Verbesserung der inneren Sicherheit hat die Europäische Union verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung in der Europäischen Union eingeleitet und dabei das Verfügbarkeitsprinzip als ein Leitprinzip für den Austausch von Informationen zur Strafverfolgung bei der Zusammenarbeit in der dritten Säule angewandt.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip explizit oder implizit zur Verbesserung der Effizienz der Strafverfolgung angewandt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der datenschutzrechtlichen Aspekte im Zusammenhang mit der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen, wie er in der Charta der Grundrechte der Europäischen Union verankert ist.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Anwendung des Verfügbarkeitsprinzips im folgenden Gemeinsamen Standpunkt und der Checkliste entwickelt. Diese Checkliste kann zur Beurteilung eines jeden Vorschlags genutzt werden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung nutzt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese Checkliste bei der Entwicklung, Beurteilung und Annahme eines jeden Vorschlags zu nutzen, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

Gemeinsamer Standpunkt

1. Einführung

Im Zusammenhang mit der Bekämpfung von Terrorismus und der Verbesserung der internationalen Sicherheit, leitete die Europäische Union verschiedene Initiativen ein, um die Effektivität der Strafverfolgung in der Europäischen Union zu verbessern. Artikel 29 EUV zielt darauf ab, den Bürgern ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts zu verschaf-

fen. Dieser Raum der Freiheit, der Sicherheit und des Rechts entwickelt sich schrittweise und führt zur Abschaffung der Grenzen zwischen den Mitgliedstaaten bezüglich der Informationen zur Strafverfolgung. Jedoch sind die Durchsetzungsbefugnisse der Mitgliedstaaten noch immer an diese nationalen Grenzen gebunden.

In diesem Zusammenhang ist der Austausch von Strafverfolgungs-Informationen unter Anwendung des Verfügbarkeitsprinzips zu einer Schlüsselfrage bei der Zusammenarbeit innerhalb der dritten Säule geworden:

– als wichtiges Instrument bei der Verwirklichung eines freien Flusses von Strafverfolgungs-Informationen, der nicht durch Binnengrenzen behindert wird,

– durch Gewährleistung von Sicherheit für den Bürger im Wege der Vereinfachung des Kampfes gegen grenzüberschreitende Straftaten,

– durch Achtung des Schutzes der Grundrechte und -freiheiten des Bürgers, insbesondere des Rechts auf Privatsphäre und Datenschutz.

Diese drei Ziele müssen in ausgewogener Weise erreicht werden. Dies liegt mit Blick auf den besonderen Charakter der Strafverfolgung und in Anbetracht der Tendenz zur zunehmenden Nutzung personenbezogener Daten für proaktive Nachforschungen der Polizei nicht auf der Hand. Ein Leitsatz bei der Strafverfolgung scheint zu sein: wenn Daten gebraucht werden, sollten sie genutzt werden. Oder noch deutlicher: wenn Daten verfügbar sind, können sie genutzt werden.

Dieses Thema demonstriert deutlich die enge Wechselbeziehung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten, wie es in der Charta der Grundrechte der Europäischen Union verankert ist.

Ein wichtiger Bestandteil in dieser Wechselbeziehung ist gegenseitiges Vertrauen. Gegenseitiges Vertrauen (und gegenseitige Anerkennung) ist eine entscheidende Bedingung für den Austausch von Strafverfolgungs-Informationen. Regierungen und Regierungsbehörden sind zum wirksamen Austausch mit (Behörden in) anderen Mitgliedstaaten nur bereit, wenn sichergestellt ist, dass diese anderen Mitgliedstaaten die Informationen im Einklang mit angemessenen rechtlichen Bestimmungen nutzen, aus Gründen des Datenschutzes und der Sicherheit.

Bereits verabschiedete EU-Rechtsakte und neuere Initiativen beschränken sich nicht darauf, den Austausch solcher personenbezogener Daten zwischen Strafverfolgungsbehörden zu fördern, die bereits von den Behörden verarbeitet werden. Einige konzentrieren sich auch auf die Nutzung solcher personenbezogener

Daten zum Zwecke der Strafverfolgung, die von privaten und öffentlichen Stellen oder in europäischen Datenbanken verarbeitet werden. Wenn es Hinweise darauf gibt, dass diese für die Zwecke der Strafverfolgung benötigt werden, werden sie (so vorgeschlagen) den Strafverfolgungsbehörden zugänglich gemacht.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip bei der Entwicklung von Strategien und Rechtsinstrumenten zur Verbesserung der Effektivität der Strafverfolgung implizit oder explizit angewandt wird, macht die Schaffung eines umfassenden Rahmens für die Beurteilung datenschutzrechtlicher Aspekte in Bezug auf die Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags gegeben, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität der Strafverfolgung nutzt.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Nutzung des Verfügbarkeitsprinzips entwickelt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese bei der Entwicklung, Beurteilung und Annahme jeglichen Vorschlags anzuwenden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

2. Anwendungsbereich des Verfügbarkeitsprinzips

Die Strategie der Europäischen Union, wie sie im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht beschrieben wird[2] zielt darauf, dass mit Wirkung vom 1. Januar 2008 der Austausch von Strafverfolgungs-Informationen durch den Verfügbarkeitsgrundsatz bestimmt wird.

In Verfolgung dieser Strategie legte die Kommission am 12. Oktober 2005 ihren Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit vor.[3] Dieser Vorschlag statuiert eine Verpflichtung der Mitgliedstaaten, Zugang zu bestimmten Daten zu ermöglichen, die für ihre Behörden verfügbar sind oder diese zu beschaffen (vgl. Erwägung 6).

Der Verfügbarkeitsgrundsatz, wie er im Haager Programm und dem vorgeschlagenen Rahmenbeschluss zur Anwendung kommt, bedeutet, dass in der gesamten Europäischen Union in einem Mitgliedstaat ein Polizist, der Informationen zur

2 Amtsblatt Nr. C 53 vom 3.3.2005, S. 1

3 KOM (2005) 490.

Erfüllung seiner Pflichten benötigt, in der Lage sein sollte, diese von einem anderen Mitgliedstaat zu erhalten und dass die Strafverfolgungsbehörde in dem anderen Staat, die über diese Information verfügt, sie zum genannten Zweck zugänglich machen wird. Der vorgeschlagene Rahmenbeschluss begrenzt den Verfügbarkeitsgrundsatz, indem er feststellt, dass er keine Verpflichtung auferlegt, Informationen zum alleinigen Zweck der Zurverfügungstellung zu sammeln oder zu speichern (Artikel 2 [1]).

Die Weitergabe verfügbarer Informationen wie personenbezogener Daten ist bereits in bestehender EU-Gesetzgebung sowie in multilateralen Übereinkommen vorgesehen. Neuere Vorschläge zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden enthalten das Verfügbarkeitsprinzip ebenfalls als Leitsatz. Jedoch wird in all diesen Rechtsinstrumenten und Vorschlägen die Verfügbarkeit personenbezogener Daten in unterschiedlicher Art und Weise ausgelegt, was zu unterschiedlichen Konsequenzen führt. Diese Unterschiede machen die weitere Untersuchung des Anwendungsbereichs dieses Prinzips erforderlich.

Eines der ersten Beispiele für den Austausch personenbezogener Daten als besonderem Bestandteil effektiver Zusammenarbeit zwischen europäischen Strafverfolgungsbehörden ist vielleicht das Übereinkommen vom 19. Juni 1990 zur Durchführung des Schengener Übereinkommens vom 14. Juni 1985.[4] Die Verarbeitung personenbezogener Daten besonderer Personenkategorien und deren Zurverfügungstellung – unter Nutzung eines zentralen Informationssystems – für verschiedene Behörden in den Staaten, die das Schengener Übereinkommen umgesetzt haben, wird als notwendige, ausgleichende Maßnahme zur Schaffung eines hohen Sicherheitsstandards in einem Raum des freien Personenverkehrs angesehen.

Ein weiterer Schritt zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden fand durch das Europol-Übereinkommen[5] und die Eurojust-Entscheidung[6] statt. Zwei Europäische Ämter wurden geschaffen, deren besondere Aufgabe es unter anderem war, den Austausch von Strafverfolgungs-Informationen zu erleichtern.

Diese Formen der Zusammenarbeit können charakterisiert werden als Zusammenarbeit durch Äußerung der Absicht zur Zusammenarbeit ohne besondere Verpflichtung dazu.

Neuere Beispiele der Zurverfügungstellung personenbezogener Daten für Strafverfolgungsbehörden sind der Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbe-

4 Amtsblatt Nr. L 239 vom 22.9.2000, S. 19

5 Amtsblatt Nr. C 316 vom 27.11.1995, S. 1

6 Amtsblatt Nr. L 63 vom 6.3.2002, S. 1

hörden der Mitgliedstaaten der Europäischen Union[7] und der Vertrag von Prüm vom 27. Mai 2005. Diese beiden Rechtsinstrumente führen einen neuen Aspekt in die Zusammenarbeit bei der Strafverfolgung ein: Mitgliedstaaten sind grundsätzlich verpflichtet, personenbezogene Daten zur Verfügung zu stellen. Die Benutzung von Formulierungen wie: „sollen auf Ersuchen" (Rahmenbeschluss) und „gestatten Zugriff … und das Recht zum Abruf" (z. B. Artikel 3 [1] Vertrag von Prüm) zeigen deutlich den verpflichtenden Charakter der Zurverfügungstellung von Daten.

Der Vertrag von Prüm führt darüber hinaus eine Verpflichtung zur Erstellung bestimmter Dateien ein, um die Verhütung und Verfolgung von Straftaten zu erleichtern. Die Vertragsparteien müssen zum Beispiel die Verfügbarkeit von Fundstellendatensätzen von Fingerabdrücken garantieren (Artikel 8).

Der bestehende, mehr oder minder freiwillige Austausch von Informationen wird auf diesen Gebieten nicht nur durch eine Verpflichtung zur Zurverfügungstellung von Informationen ersetzt, sondern auch durch die Verpflichtung, für bestimmte Kategorien personenbezogener Daten eine Infrastruktur zu schaffen, die anderen Strafverfolgungsbehörden den Zugriff darauf ermöglicht.

Eine solche Verpflichtung zur Zurverfügungstellung von Informationen beschränkt sich nicht notwendig auf Strafverfolgungsbehörden. Zum Beispiel wird in Erwägung 19 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze gewonnen oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG ausdrücklich erwähnt, dass *„es notwendig ist, dass vorhandene Daten zugänglich gemacht werden"*. Auf europäischer Ebene wird abgesichert, dass bestimmte Kategorien von Daten, die durch private Stellen verarbeitet werden, für die Strafverfolgung zugänglich gemacht werden sollen.

Das Verfügbarkeitsprinzip ist ebenfalls ein wichtiges Thema der Mitteilung der Kommission an den Rat und das Europäische Parlament vom 24. November 2005 über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen[8]. Die Weitergabe verfügbarer Informationen durch die Verbindung von Datenbanken ist ein Schlüsselelement bei den Zukunftsplanungen in der Europäischen Union.

Andere Initiativen wie die neue Rechtsgrundlage des Schengener Informationssystems der zweiten Generation und die Schaffung des Visa-Informationssystems

7 Amtsblatt Nr. L 386 vom 29.12.2006, S. 89

8 KOM (2005) 597.

beinhalten ebenfalls Aspekte des Verfügbarkeitsprinzips. Personenbezogene Daten, die für einen bestimmten Zweck verarbeitet wurden, werden für andere Zwecke wie etwa Strafverfolgung zugänglich gemacht.

Im Hinblick auf diese Bandbreite der Erscheinungsformen des Verfügbarkeitsprinzips als Schlüsselelement bei der Verbesserung der Strafverfolgung und der Auswirkung auf das Grundrecht auf den Schutz personenbezogener Daten, betont die Europäische Datenschutzkonferenz die Notwendigkeit, die Nutzung des Verfügbarkeitsprinzips in umfassender Weise in den Kontext zu setzen. Jegliche Harmonisierung der Verarbeitung personenbezogener Daten durch die Einführung von Verpflichtungen zur Vorratsspeicherung personenbezogener Daten oder von Verpflichtungen zur Erstellung spezifischer Datenbestände und die Absicht oder die Verpflichtung, diese personenbezogenen Daten für Strafverfolgungsbehörden oder für mit der Strafverfolgung in Zusammenhang stehende europäische oder internationale Einrichtungen verfügbar zu machen, sollte als Umsetzung des Verfügbarkeitsprinzips angesehen werden.

Unter Zugrundelegung dieses Anwendungsbereiches hat die Europäische Datenschutzkonferenz seine Auswirkungen im Hinblick auf anwendbare Datenschutzbestimmungen untersucht.

3. Anwendbares Recht

Zusätzlich zum Recht auf die Achtung des Privat- und Familienlebens, das durch Artikel 8 der EMRK garantiert und durch Artikel 7 der Charta der Grundrechte der Europäischen Union nochmals bestätigt wird, ist das neue Grundrecht auf Datenschutz in Artikel 8 der Charta verankert.

Die EMRK erlaubt den Eingriff in den Schutzbereich des Rechts auf Privatleben, wenn er zur Wahrung der im zweiten Absatz des Artikel 8 bezeichneten Interessen notwendig und durch diese Interessen gerechtfertigt ist; ein solcher Eingriff muss dem Verhältnismäßigkeitsgrundsatz entsprechen. Artikel 8 der Charta der Grundrechte weitet dies aus, indem er festlegt, dass personenbezogene Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen legitimen Grundlage verarbeitet werden müssen. Diese legitime Grundlage muss ebenfalls dem Verhältnismäßigkeitsgrundsatz entsprechen.

Das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 (Konvention 108) enthält spezifischere Grundsätze für den Datenschutz, die auch innerhalb der dritten Säule anwendbar sind. Es gibt auch eine Empfehlung (Nr. R[87] 15) mit spezifischen Datenschutzvorschriften für die Verwendung personenbezogener

Daten bei der Polizei, die 1987 vom Ministerkomitee der Mitgliedstaaten zur Regelung der Verwendung personenbezogener Daten bei der Polizei verabschiedet wurde.[9]

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[10] sieht eine harmonisierte Datenschutzordnung in der Europäischen Union vor. Obwohl Maßnahmen, die in Titel V und VI des Vertrages über die Europäische Union bezeichnet sind, außerhalb des Anwendungsbereichs dieser Richtlinie liegen, wenden Mitgliedstaaten die allgemeinen Datenschutz-Grundsätze auf Maßnahmen der Strafverfolgung an.

Die Verordnung 45/2001 des Europäischen Parlaments und des Rates vom 18. September 2000[11] sieht Regeln für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vor. Die Grundsätze dieser Verordnung werden zur Definition der Datenschutz-Ordnung genutzt, die auf die Verarbeitung personenbezogener Daten in Europäischen Datenbanken wie dem Visa-Informationssystem und dem Schengener Informationssystem der zweiten Generation anwendbar ist.

Das Europol-Übereinkommen und die Eurojust-Entscheidung enthalten für diese Organisationen spezifische Datenschutzregelungen, die auf den allgemeinen Datenschutz-Prinzipien beruhen, wie sie in der Konvention 108 und der Empfehlung Nr. R(87) 15 definiert werden, die oben genannt wurden.

Für Datenverarbeitung durch private und öffentliche Stellen sowie durch die Europäischen Institutionen und in Europäischen Datenbanken enthält das anwendbare EU-Recht einen Grundsatz über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten: Daten sollten für ausdrückliche und legitime Ziele gesammelt werden und nicht in einer Art und Weise weiterverarbeitet werden, die mit diesen Zielen unvereinbar ist. Eine Ausnahme oder Beschränkung ist nur dann erlaubt, wenn diese gesetzlich vorgesehen ist und eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten darstellt. Die in diesen Rechtsinstrumenten genutzte Definition der Datenverarbeitung umfasst die Bekanntgabe durch Weitergabe, Verbreitung oder sonstige Zurverfügungstellung.

In den Situationen, in denen das Verfügbarkeitsprinzip angewendet wird, um ursprünglich zu anderen Zwecken als der Strafverfolgung verarbeitete Daten für die

9 Empfehlung Nr. R (87) 15 vom 17. September 1987.

10 Amtsblatt Nr. L 281 vom 23.11.1995, S. 31

11 Amtsblatt Nr. L 8 vom 12.1.2001, S. 1

Strafverfolgung zu nutzen, muss die Ausnahme vom Grundsatz der Zweckbestimmung alle Bedingungen für das Eingreifen dieser Ausnahme erfüllen.

4. Umsetzung des Verfügbarkeitsprinzips

Die Effektivität der Strafverfolgung wird von der Informationslage der Strafverfolgungsbehörden abhängen, von der Möglichkeit, innerhalb der Grenzen des Rechts Informationen zu sammeln, von der Qualität und dem Nutzen dieser Daten und der Fähigkeit zur Weitergabe dieser Daten an andere Strafverfolgungsbehörden. Die verschiedenen Arten der Zusammenarbeit bei der Strafverfolgung in der Europäischen Union, wie sie in Kapitel 2 beschrieben wurden, umfassen all diese Gesichtspunkte.

Bezüglich aller Initiativen zum Austausch personenbezogener Daten zwischen Strafverfolgungsbehörden in der Europäischen Union und dem Austausch mit Drittstaaten und -stellen, hat die Europäischen Datenschutzkonferenz bereits erklärt, dass *„In Anbetracht der Verpflichtung der Union zur Achtung der Menschenrechte und der Grundfreiheiten, Initiativen zur Verbesserung der Strafverfolgung in der EU, wie der Verfügbarkeitsgrundsatz, nur auf Grundlage eines angemessenen Systems von Vorkehrungen zum Datenschutz eingeführt werden sollten, das einen hohen und gleichwertigen Standard beim Datenschutz gewährleistet.“*[12] Diesbezüglich begrüßt die Europäische Datenschutzkonferenz den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[13] Ein harmonisierter und hoher Standard des Datenschutzes im Bereich der Strafverfolgung, wie er von einem Rahmenbeschluss des Rates gewährleistet werden sollte, wird nun als unabdingbare Voraussetzung für die Strafverfolgung in der Europäischen Union bezeichnet.

Es sollte jedoch betont werden, dass ein solcher harmonisierter Datenschutz-Rahmen an sich noch kein umfassendes Instrument zur Beurteilung der Umsetzung des Verfügbarkeitsprinzips in all seinen in Kapitel 2 beschriebenen Erscheinungsformen darstellt. Dieser Rahmen ist nur dann anwendbar, wenn personenbezogene Daten bereits von Strafverfolgungsbehörden verarbeitet werden. Darüber hinaus wird der Entwurf des Rahmenbeschlusses im Rat weiter diskutiert.

Da die Bandbreite der Nutzung des Verfügbarkeitsprinzips zur Anwendung verschiedener Rechtsinstrumente führt, sollte ein umfassender Rahmen zur Beurteilung der Nutzung dieses Prinzips sämtliche Gesichtspunkte der Nutzung des Verfügbarkeitsprinzips abdecken. Ein solcher Rahmen sollte in einem gesonderten Instrument bestehen, das nachträglich auch auf bestehendes Recht angewendet wird.

---

12 Erklärung von Krakau, 25./26. April 2005.

13 KOM (2005) 475.

5. Ein umfassender Rahmen zur Beurteilung der Nutzung des Verfügbarkeitsprinzips.

Strafverfolgung ist von Informationen abhängig. Grundsätzlich werden zweierlei Informationsquellen genutzt: Informationen, die bereits von Strafverfolgungsbehörden verarbeitet werden und Informationen, die von anderen verarbeitet werden. Diese Unterscheidung ist in gewisser Weise künstlich, weil Daten, die von Strafverfolgungsbehörden verarbeitet werden, von privaten oder öffentlichen Stellen erlangt worden sein können.

Wenn personenbezogene Daten durch private oder öffentliche Stellen verarbeitet werden, sind die in der Richtlinie 95/46/EG definierten Datenschutzgrundsätze maßgeblich. Wenn diese Daten entweder von Europäischen Organen oder in Europäischen Datenbanken verarbeitet werden, sind die Grundsätze der Verordnung 45/2001 und/oder die für diese Dateien einschlägigen spezifischen Regeln anwendbar.

Wie bereits dargelegt, stellt die Nutzung dieser Daten zum Zwecke der Strafverfolgung in der Regel eine Ausnahme vom Grundsatz der Zweckbindung dar, die nur erlaubt ist, wenn dies gesetzlich vorgesehen ist und es um eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten geht.

In dem Falle, dass die Daten bereits von Strafverfolgungsbehörden verarbeitet werden, wird der (Entwurf des) Rahmenbeschluss des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen für den notwendigen rechtlichen Datenschutz-Rahmen bei der Verarbeitung und dem Austausch von Informationen zwischen Strafverfolgungsbehörden sorgen. Es könnten jedoch neue Initiativen für die Verarbeitung dieser Daten vorgelegt werden, die auf dem Verfügbarkeitsprinzip basieren.

Zur Beurteilung, ob eine Ausnahme notwendig ist und den formellen Bedingungen entspricht, oder bei der Beurteilung neuer Initiativen zur Bereitstellung von Daten zur Strafverfolgung, wird es notwendig sein, die verschiedenen Bedingungen in den Blick zu nehmen, die die einschlägigen Datenschutzvorschriften enthalten.

Die erste Bedingung bezieht sich auf die Anforderung, dass jede Maßnahme gesetzlich vorgesehen sein soll. Dieses Gesetz muss strengen Anforderungen entsprechen, so muss es klar, einfach und präzise sein: es soll transparent und für jedermann leicht verständlich sein. Nach der Rechtsprechung des Gerichtshofes erfordert der Grundsatz der Rechtssicherheit, dass Gesetze klar und präzise sein müssen und ihre Anwendung für den Einzelnen vorhersehbar. Darüber hinaus

müssen die Gesetze immer Begründung und Zweck sowie die Bedingungen für die Verarbeitung festlegen und ein angemessenes und effektives Kontrollsystem festsetzen.

Die zweite Bedingung, die erfüllt werden muss, ist, dass jede Maßnahme erforderlich und verhältnismäßig sein muss. Insbesondere die Beurteilung dieses Aspekts erfordert einen umfassenden Ansatz. Ein solcher Ansatz sollte die folgenden Beurteilungs-Schritte enthalten:

A. Evaluation bereits bestehender rechtlicher Maßnahmen, die die Verarbeitung inklusive des Austauschs von Daten erlauben.

Sind diese Maßnahmen nicht ausreichend oder sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv? Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag zur Verbrechensbekämpfung leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird. Wenn jedoch die Evaluation ergibt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme gerechtfertigt ist.

Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt werden:

B. Verhältnismäßigkeit

Effektive Durchsetzung, aber mit minimalen Eingriffen in die Privatsphäre. Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:

- Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.

- Eine weniger eingreifende Maßnahme kann nicht zum gleichen Ergebnis führen.

- Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz gerechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 [2] der Rahmentscheidung zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.

- Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

Die dritte Bedingung bezieht sich auf die Kategorien der zu verarbeitenden Daten und auf weitere besondere Bedingungen.

Verschiedene Arten von Daten sind betroffen: von Daten zur Identifikation (genutzt sowohl zur Identifikation des Betroffenen als auch zu dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z. B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z. B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss zwischen diesen Daten unterscheiden und zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für empfindliche Daten; durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen. Sie sollte Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für besondere Arten von Verbrechen unterscheidet. Zum Beispiel sollten Personen, die von einer Anklage freigesprochen wurden oder gegen die keine Beschuldigungen erhoben werden, klar von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten klar von Daten über Verdächtige unterschieden werden.

Eine solche Unterscheidung könnte mit der Unterscheidung zwischen verschiedenen Kategorien von Personen verbunden sein, wie sie sich in Artikel 4 (3) des Kommissionsvorschlags für den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen findet.

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Auswirkungen der Nutzung von Daten auf die Strafverfolgung sollten ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätz-

lichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung erfordert zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifikation anhand der Nutzung solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung riesiger Mengen von Daten geschieht, wie beim neuen Schengener Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Operationen bei der Verarbeitung, die besondere Gefahren darstellen können (z. B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Stand der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

Die vierte Bedingung bezieht sich auf den Zugang zu diesen Daten.

Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein. Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungsmaßnahme begrenzt sein und die Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein. Empfänger-Behörden müssen klar identifiziert sein. Wenn direkter Zugang zu Daten vorgeschlagen wird, sind die Nutzung eines Index oder von hit-/no hit-Systemen und eine ausreichende Zugangskontrolle erforderlich.

Die fünfte Bedingung bezieht sich auf Kontrolle und Aufsicht.

Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungsvorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Tätigkeiten inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden. Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.

6. Schlussfolgerung

Die Europäische Datenschutzkonferenz erkennt an, dass Informationen und personenbezogene Daten für eine effektive Strafverfolgung entscheidend sind. Sie wiederholt jedoch, dass jegliche Maßnahme unter Nutzung des Verfügbarkeitsprinzips verhältnismäßig sein und die Grundrechte des Einzelnen achten sollte. Dieser Gemeinsame Standpunkt und die Checkliste richten sich insbesondere an die EU-Organe, als ein konstruktiver Beitrag zu gegenwärtigen Initiativen. Sie stellen die Bedingungen dar, die erfüllt werden müssen, um einen hohen Datenschutz-Standard auf dem Gebiet der Strafverfolgung aufrecht zu erhalten. Die Europäische Datenschutzkonferenz ist natürlich bereit, weiter dazu beizutragen, dass der Vorgang der Verbesserung der Strafverfolgung sich im Einklang mit der Achtung von Grundrechten befindet.

Checkliste zur Beurteilung jeglicher Maßnahme zur Umsetzung des Verfügbarkeitsprinzips bei der Strafverfolgung

I. Recht und Evaluation

Jede Maßnahme muss gesetzlich vorgesehen sein. Das Gesetz muss strengen Anforderungen entsprechen. So muss es klar sein und Verlässlichkeit und Vorhersehbarkeit schaffen.

Darüber hinaus muss Gesetzgebung immer:

- Begründung und
- Zweck festlegen, sowie
- die Bedingungen für die Verarbeitung.
- Ein angemessenes und effektives System zur unabhängigen Kontrolle einsetzen.

II. Bedarf und Verhältnismäßigkeit

Die Maßnahme sollte eine notwendige Sicherheitsvorkehrung darstellen.

A. Evaluation bereits bestehender rechtlicher Maßnahmen, die die Verarbeitung inklusive des Austauschs von Daten erlauben.

- Sind diese Maßnahmen nicht ausreichend?

  Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag im Kampf gegen Straftaten leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird.

- Sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv?

  Wenn die Evaluation zeigt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme eine gerechtfertigte Ausnahme vom Grundsatz der Zweckbegrenzung ist.

- Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt sein:

B. Verhältnismäßigkeit

- Die Maßnahme sollte darauf zugeschnitten sein, folgendes zu erreichen:
  - Effektive Durchsetzung,
  - Minimale Eingriffe in die Privatsphäre.
- Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:
  - Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.
  - Sie darf nicht gegen das Erforderlichkeitsgebot verstoßen, was bedeutet, dass eine weniger eingreifende Maßnahme nicht zum gleichen Ergebnis führen kann.

– Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz gerechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 [2] des Rahmenbeschlusses zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.

- Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

III. Besondere Bedingungen

Verschiedene Arten von Daten sind betroffen: von Daten zur Identifizierung (genutzt zur Identifizierung des Betroffenen und dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z. B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z. B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss:

- Zwischen diesen Daten unterscheiden,

- Besondere zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für die Nutzung empfindlicher Daten durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen.

- Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für spezifische Arten von Verbrechen unterscheidet. (Zum Beispiel sollten Personen, die von einem Vorwurf freigesprochen wurden oder gegen die keine Vorwürfe erhoben werden, deutlich von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten deutlich von Daten über Verdächtige unterschieden werden.)

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Aus-

wirkungen der Nutzung von Daten auf die Strafverfolgung sollten ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätzlichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung verlangt zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifizierung anhand der Nutzung solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung umfangreicher Mengen von Daten geschieht, wie beim neuen Schengen-Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Verfahren bei der Verarbeitung, die besondere Gefahren darstellen können (z. B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Standard der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

IV. Zugang der Strafverfolgungsbehörden zu personenbezogenen Daten

- Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein.

- Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungs-Aufgabe begrenzt sein.

- Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein.

- Wenn direkter Zugang zu Daten vorgeschlagen wird, ist die Nutzung eines Index oder von hit-/no hit-Systemen und eine ausreichende Zugangskontrolle erforderlich.

- Die Empfänger-Behörden müssen klar identifiziert sein.

V. Kontrolle und Aufsicht

- Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungs-Vorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Vorgänge inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden.

- Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.

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

Stellungnahme 5/2007 zum Folgeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika vom Juli 2007 über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (WP 138)

Angenommen am 17. August 2007

Zusammenfassung

Die Stellungnahme befasst sich mit den Auswirkungen des neuen dritten Abkommens über die Übermittlung von Fluggastdatensätzen (PNR-Daten) an das US-Heimatschutzministerium (DHS) auf die Grundrechte und Grundfreiheiten und speziell auf das Recht der Fluggäste auf Schutz ihrer Daten.

Mit der Einigung auf ein neues langfristiges Abkommen wurde eine Rechtsgrundlage für die Übermittlung von Fluggastdaten geschaffen. Die Datenschutzgruppe hat die Bekämpfung des internationalen Terrorismus und des weltweiten organisierten Verbrechens stets als notwendiges und legitimes Anliegen betrachtet, das Unterstützung verdient. Für eine Beschneidung der Grundrechte und Grundfreiheiten von Personen einschließlich ihres Rechts auf Achtung ihrer Privatsphäre und Schutz ihrer personenbezogenen Daten muss es jedoch gute Gründe geben, wobei abzuwägen ist zwischen dem notwendigen Schutz der öffentlichen Sicherheit auf der einen und anderen öffentlichen Interessen wie dem Datenschutz auf der anderen Seite. Die Datenschutzgruppe hegt Zweifel, dass gelungen ist, in dem Abkommen ein angemessenes Gleichgewicht zwischen diesen Interessen herzustellen.

Die Ergebnisse der Prüfung des Abkommens aus datenschutzrechtlicher Sicht lassen sich wie folgt zusammenfassen:

1. Insgesamt gesehen wurden die in das frühere Abkommen eingebauten Datenschutzgarantien deutlich gelockert.

* Alle weiteren von der Arbeitsgruppe 2007 beschlossenen Dokumente sind abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_de.htm

2. Das neue Abkommen greift zentrale Fragen und Versäumnisse nicht auf und enthält zu viele Ausnahmen für Notsituationen.

Zu 1):

a) Die Zahl der Datenelemente, die übermittelt werden dürfen, ist gestiegen und schließt Informationen über andere Personen als die jeweils betroffene Person mit ein.

b) Das Herausfiltern sensibler Daten wird selbst bei Einführung eines „Push"-Systems nach wie vor durch das DHS erfolgen.

c) Das DHS darf jetzt in Ausnahmefällen sensible Daten verwenden, was durch das frühere Abkommen ausgeschlossen war.

d) Die anschließende Weitergabe an andere US-amerikanische oder ausländische Behörden ist einfacher geworden und unterliegt nicht mehr denselben Datenschutzgarantien.

e) Die erlaubte Speicherfrist ist auf mindestens 15 Jahre ausgedehnt worden und könnte sogar noch darüber hinausgehen.

f) Das Verfahren der gemeinsamen Überprüfung enthält keinen Hinweis auf eine Beteiligung unabhängiger Datenschutzbehörden.

Zu 2):

a) Die in dem Abkommen und dem Schreiben des DHS enthaltenen Garantien sind nicht präzise formuliert und lassen Raum für zu viele Ausnahmen, die in das ausschließliche Ermessen der Behörden der Vereinigten Staaten gestellt sind.

b) Weder die Zwecke, zu denen die Daten übermittelt werden, noch die vielen Ausnahmen hiervon sind hinlänglich genau beschrieben und gehen über das hinaus, was nach den üblichen Datenschutzgrundsätzen zulässig wäre.

c) Der Übergang vom „Pull"- zum „Push"-System ist für den 1. Januar 2008 vorgesehen, doch ist nicht klar, ob überhaupt und unter welchen Bedingungen dafür gesorgt wird, dass diese neue Art der Übermittlung funktioniert.

d) Unklar bleibt ferner, auf welche Weise das DHS, dem es gestattet ist, in Ausnahmefällen andere als die aufgeführten Daten abzurufen, nach dem Übergang vom „Pull"- zum „Push"-System auf diese Daten zugreifen kann.

e) Aus dem Abkommen wird nicht ersichtlich, wann und unter welchen Umständen eine gemeinsame Überprüfung stattfinden wird.

f) Das Abkommen sieht keinen Streitbeilegungsmechanismus vor, sondern überlässt dies den Vertragsparteien. Speziell im Hinblick auf die gemeinsame Überprüfung wäre dies besonders wichtig.

g) Unklar ist, welcher Regelung die Daten unterliegen, wenn sie durch Drittbehörden oder sonstige Stellen nochmals weitergegeben werden.

h) Es ist schwer einzuschätzen, wie sich das vereinbarte Prinzip der Gegenseitigkeit auf das Datenschutzniveau einer etwaigen PNR-Regelung der EU auswirken wird.

i) Das Abkommen birgt das Risiko, dass etwaige Änderungen in der US-Gesetzgebung einseitig das in dem neuen PNR-Abkommen vorgesehene Datenschutzniveau beeinträchtigen könnten.

Zum Bedauern der Datenschutzgruppe ist die Gelegenheit verpasst worden, sich auf einen ausgewogeneren, an den tatsächlichen Erfordernissen orientierten zu einigen. Das Abkommen ist vielfach kommentiert worden. Die Datenschutzgruppe hätte sich ihrerseits ein anderes Ergebnis der Verhandlungen zwischen der EU und den USA gewünscht. Ihrer Ansicht nach ist das neue Abkommen im Hinblick auf die Wahrung der Grundrechte im Bereich des Datenschutzes nicht ausgewogen.

Da das Abkommen nach wie vor einige Fragen aufwirft, wird die Datenschutzgruppe bei der Kommission schriftlich um Klarstellung folgender Punkte nachsuchen:

- Geltungsbereich des Abkommens: Auf welche Fluggesellschaften ist es anwendbar?

- Unter welchen Voraussetzungen können die Daten für andere als die unter 1., 2. und 3. in Abschnitt I des DHS-Schreibens aufgelisteten Zwecke verwendet werden?

- Wie soll das im Ausnahmefall anzuwendende „Pull"-System funktionieren, d.h. wie sollen diese außerordentlichen Befugnisse im europäischen Rechtsraum kontrolliert werden?

- Wie steht es mit der Zusicherung, dass es beim 1. Januar 2008 als Stichtag bleibt und dieser Termin nicht wieder verschoben wird, weil beispielsweise die Diskussionen über die technischen Spezifikationen noch andauern?

- Welches sind die 13 Fluggesellschaften, die bereits Daten gemäß Abschnitt VIII des DHS-Schreibens hinüberschicken („push“) und welches sind die an sie gestellten Anforderungen?

- Wann und wie wird die Überprüfung des Abkommens vorbereitet und ausgeführt?

- Wie verhält es sich mit Nummer 5 des neuen Abkommens bzw. Abschnitt IX des DHS-Schreibens („Gegenseitigkeit“), die in Bezug auf die Erwartungen der US-amerikanischen Seite keine eindeutigen Aussagen enthalten?

Die Datenschutzgruppe bedauert außerdem, dass sie als offizielles EU-Beratungsgremium in Datenschutzfragen und in Ermangelung eines Pendants für Tätigkeiten der dritten Säule zu den datenschutzrechtlichen Aspekten des Abkommens nicht gehört oder zu Rate gezogen wurde. Sie bedauert dies umso mehr, als die Mitglieder der Datenschutzgruppe die Einhaltung der Datenschutzbestimmungen durch die Fluggesellschaften kontrollieren und die Fluggesellschaften ihrerseits das Abkommen in enger Abstimmung mit den EU-Datenschutzbehörden umsetzen müssen.

Die Datenschutzgruppe möchte ihre konstruktiven Beziehungen zum Rat der Europäischen Union und zur Europäischen Kommission aufrechterhalten. Dies gilt insbesondere im Hinblick auf die Umsetzung des neuen Abkommens. Die Datenschutzgruppe erwartet, dass sie in die Vorbereitung und Durchführung der gemeinsamen Überprüfung eingebunden wird. Sie erwartet ebenfalls, dass sie an den Gesprächen über die Definition sensibler Daten und an sonstigen Folgemaßnahmen beteiligt wird.

STELLUNGNAHME 5/2007 DER GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

I. Vorbemerkungen

Das neue Abkommen

Im Juli 2007[1] schloss die Europäische Union mit den Vereinigten Staaten von Amerika ein Folgeabkommen ab über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS – US-Heimatschutzministerium), das das am 31. Juli 2007 ausgelaufene PNR-Interimsabkommen mit den Vereinigten Staaten vom 19. Oktober 2006 ersetzt.

Es wird vom Tag seiner Unterzeichnung an bis zu seinem Inkrafttreten in den EUMitgliedstaaten vorläufig angewendet und tritt am Tag des Abschlusses eines einvernehmlich ausgehandelten Folgeabkommens, spätestens jedoch sieben Jahre nach dessen Unterzeichnung, außer Kraft.

Ziel des Abkommens ist es, das Interimsabkommen zwischen der Europäischen Union und den USA vom Oktober 2006 abzulösen und auf diese Weise für Fluggesellschaften, die Flüge in die und aus den Vereinigten Staaten von Amerika durchführen, für Reisende und für die Datenschutzbehörden der EU-Mitgliedstaaten Rechtssicherheit zu schaffen. Das Interimsabkommen wurde geschlossen, nachdem der Beschluss 2004/496/EG des Rates vom 17. Mai 2004 (über den Abschluss eines Abkommens durch die Europäische Gemeinschaft über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection (CBP)) und die Kommissionsentscheidung 2004/535/EG vom 14. Mai 2004 (so genannte „Angemessenheitsentscheidung“) wegen unzutreffender Rechtsgrundlage durch das Urteil des Europäischen Gerichtshofs vom 14. Mai 2004 aufgehoben worden waren.

Die neue Vereinbarung hat folgende Bestandteile:

– das von beiden Vertragsparteien unterzeichnete Abkommen

– ein Schreiben des US-Department of Homeland Security (DHS-Schreiben), in dem dieses erläutert, wie es den Schutz der PNR-Daten zu gewährleisten gedenkt und

[1] Das Abkommen wurde am 23. Juli von der EU und am 26. Juli 2007 von den USA unterzeichnet. Es ist abrufbar unter http://www.dhs.gov/xnews/releases/pr_1185470531857.shtm und ist ebenfalls im Amtsblatt der Europäischen Union veröffentlicht (ABl. L 204 vom 4.8.2007, S. 18). http://www.metasearch.dgt.cec.eu.int:17002/showpage.php3?id=25387394&md=8c8d2f2353b5729b95a55abadb609453&source=EN&target=DE

– ein Antwortschreiben der EU, in dem diese den Eingang des Schreibens mit den Garantien bestätigt und erklärt, dass es angesichts dieser Zusicherungen den Schutz der PNR-Daten in den USA für angemessen hält.

Hintergrund

Die Datenschutzgruppe bewertet es positiv, dass ein neues langfristiges Abkommen zustande gekommen ist und so eine Rechtsgrundlage für die Übermittlung von Fluggastdatensätzen geschaffen wurde. Sie würdigt auch die Bemühungen der EU-Verhandlungsführer, denen es trotz des Widerstands der US-Behörden gelungen ist, überhaupt ein Abkommen zustande zu bringen und so ein rechtliches Vakuum zu verhindern.

Die Datenschutzgruppe sieht es als ihre Pflicht an, ihre Meinung zu Fragen der Schutzes der Privatsphäre im Zusammenhang mit der Übermittlung personenbezogener Daten an die US-Behörden zu äußern, da Flugreisende, politische Entscheidungsträger und Datenschutzbehörden über das gegenwärtige Datenschutzniveau in dem neuen Abkommen im Bilde sein müssen. Zudem obliegt die Erhebung und Übermittlung der PNR-Daten den Fluggesellschaften, über die die nationalen Datenschutzbehörden die Aufsicht führen.

Die Datenschutzgruppe hat die Bekämpfung des internationalen Terrorismus und weltweiten organisierten Verbrechens stets als notwendiges und legitimes Anliegen betrachtet, das ihre Unterstützung verdient. Sie räumt ein, dass personenbezogene Daten dabei von großem Wert sein können, vertritt jedoch die Ansicht, dass allein mit der Erhebung und Verarbeitung von Fluggastdatensätzen dieses Phänomen nicht in den Griff zu bekommen sein wird und deshalb auch alle sonstigen verfügbaren Mittel genutzt werden sollten, um mehr Sicherheit zu schaffen und ein sicheres, reibungsloses Reisen mit dem Flugzeug zu ermöglichen.

Jedes Jahr überqueren Millionen von Flugreisenden den Atlantik; nach dem Abschluss des Open-Skies-Abkommens wird mit einem weiteren Anstieg ihrer Zahl gerechnet. Die Fluggesellschaften erheben und nutzen Fluggastdaten für eigene geschäftliche Zwecke. Bei der Bekämpfung von Terrorismus und damit zusammenhängenden Straftaten muss die Achtung der Grundrechte und Grundfreiheiten von Personen gewährleistet sein, wozu auch das Recht auf Schutz der Privatsphäre und von personenbezogenen Daten gehört. Diese Rechte sind nicht verhandelbar.

Wenn diese Grundrechte und Freiheiten beschnitten werden, muss es dafür gute Gründe geben, wobei zwischen dem notwendigen Schutz der öffentlichen Sicherheit und anderen Interessen der Allgemeinheit wie dem Recht auf Schutz der Privatsphäre das richtige Gleichgewicht gefunden werden muss. Eine ungerechtfer-

tigte und unverhältnismäßige generelle Überwachung durch ein Drittland wäre mit der Menschenwürde und dem Recht auf Schutz der Privatsphäre nicht vereinbar.

Um das von dem neuen langfristigen Abkommen garantierte Datenschutzniveau ordentlich bewerten zu können, muss es daher an den Grundsätzen des Datenschutzes wie Verhältnismäßigkeit, Datensparsamkeit, Verantwortlichkeit desjenigen, der die Daten verarbeitet, sowie Auskunfts- und Widerspruchsrecht der betroffenen Person gemessen werden.

Bewertung durch die Artikel-29-Datenschutzgruppe

Zweck der Stellungnahme der Datenschutzgruppe, in der die unabhängigen EU-Datenschutzbeauftragten vereint sind, ist die sorgfältige Analyse des Datenschutzniveaus in dem neuen langfristigen Abkommen. Hierzu wurden die Bestimmungen des neuen Abkommens mit den früheren Vereinbarungen nach Maßgabe anerkannter Datenschutzgrundsätze verglichen. Als Maßstab dienten die Grundsätze der Richtlinie 95/46/EG[2] und des Übereinkommens 108 des Europarates[3] sowie frühere Stellungnahmen der Datenschutzgruppe zu dieser Frage. Zudem sollen die Folgen des Abkommens für den Schutz der Privatsphäre derjenigen, die in die Vereinigten Staaten oder von dort aus nach Europa fliegen, abgeschätzt werden.

Anders als die früheren Vereinbarungen verweist das neue PNR-Abkommen nicht auf die so genannte Verpflichtungserklärung des Bureau of Customs and Border Protection (CBP) vom Mai 2004, die damit hinfällig wird. Obwohl es sich bei dieser Verpflichtungserklärung der USA rechtlich gesehen um einen einseitigen Akt handelte, war sie doch das Ergebnis langwieriger, komplizierter Verhandlungen mit dem Ziel, ein angemessenes Datenschutzniveau bei der Verwendung von PNR-Daten sicherzustellen, worauf die Kommission seinerzeit ihre so genannte Angemessenheitsentscheidung 2004/535/EG stützte. Die Datenschutzgruppe nahm während der Verhandlungen und danach eine Reihe von Stellungnahmen zum Datenschutzniveau an[4].

Das neue Abkommen und vor allem das DHS-Schreiben enthalten jetzt so genannte Zusicherungen, die Datenschutzgarantien für die Verwendung von EU-Fluggastdaten liefern sollen. Diese Zusicherungen treten an die Stelle der Verpflichtungserklärung.

---

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

3 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

4 WP 78 vom 13. Juni 2003, WP 87 vom 29. Januar 2004 und WP 95 vom 22. Juni 2004.

Die Datenschutzgruppe wird daher in ihrer Stellungnahme die Zusicherungen im DHS-Schreiben mit den Verpflichtungen von 2004 genau vergleichen und daraus Rückschlüsse auf das von ihnen garantierte Datenschutzniveau ziehen.

II. Das neue PNR-Abkommen

1. Geltungsbereich und Rechtsnatur

Das neue Abkommen gilt für Fluggesellschaften, die Flüge in die oder aus den Vereinigten Staaten durchführen. Dabei ist unklar, ob dies zum Beispiel Fluggesellschaften miteinschließt, die aus einem Drittland mit einem Zwischenstopp in Europa die Vereinigten Staaten anfliegen. Unklar ist auch, bis wohin die Zuständigkeit der EU reicht. Ist es der Verarbeitungsvorgang oder der für die Verarbeitung Verantwortliche, der in der EU beheimatet sein muss? Das Abkommen lässt diese Fragen unbeantwortet, weshalb die Datenschutzgruppe von der Europäischen Kommission eine schriftliche Klärung dieser Punkte erwartet.

Gemäß Nummer 1 sind das Abkommen und das Begleitschreiben des DHS für beide Vertragsparteien bindend. Sowohl das Abkommen als auch das Schreiben werden im EU-Amtsblatt (Reihe L) veröffentlicht. Unklar ist hingegen, ob das DHS-Schreiben im US Federal Register veröffentlicht wird. Bei Verstoß der Vereinigten Staaten gegen das Abkommen kann die EU gemäß Nummer 8 das Abkommen kündigen. Das Abkommen und das Begleitschreiben sind gegenüber nicht-öffentlichen Parteien wie Fluggesellschaften oder Bürgern nicht unmittelbar anwendbar. Die einzelstaatlichen Rechtsvorschriften lässt dieses Abkommen unberührt.

2. Zweckbindung

Das neue langfristige PNR-Abkommen besteht aus der Präambel und 9 Abschnitten (Nummern), die die Übermittlung von PNR-Daten durch Fluggesellschaften an das US Department of Homeland Security regeln. Die Gründe für die Datenübermittlungen sind in der Präambel ausgeführt: Verhütung und Bekämpfung des Terrorismus und sonstiger schwerer Straftaten grenzüberschreitender Art. Im DHS-Schreiben heißt es ausführlicher: Verhütung und Bekämpfung 1. des Terrorismus und damit zusammenhängender Straftaten, 2. sonstiger schwerer Straftaten grenzüberschreitender Art, einschließlich der organisierten Kriminalität sowie 3. der Flucht vor Haftbefehlen oder vor Gewahrsamnahme im Zusammenhang mit den genannten Straftaten.

Die in dem neuen Abkommen genannten Verwendungszwecke sind dieselben wie im vorangegangenen Interimsabkommen. Eine Definition dessen etwa, was unter

mit dem Terrorismus zusammenhängenden Straftaten oder schweren Straftaten grenzüberschreitender Art zu verstehen ist, fehlt, was Raum für Interpretationen lässt.

Die Datenschutzgruppe hält diese Abgrenzung des Verwendungszwecks nach wie vor für zu weit gefasst und hätte sich eine klarere Definition vorstehender Begriffe gewünscht.

In dem DHS-Schreiben heißt es ferner, dass die PNR-Daten auch in anderen Fällen verwendet werden dürfen, so vor allem zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen. Dieser Punkt war auch schon Gegenstand der früheren Verpflichtungserklärung. Die Daten dürfen zudem in Strafprozessen verwendet werden, was den Schluss zulässt, dass auch bei kleineren Vergehen oder Straftaten, die nicht mit einem terroristischen Akt oder einer schweren Straftat grenzüberschreitender Art in Zusammenhang stehen, von ihnen Gebrauch gemacht werden kann. Schließlich dürfen sie auch in anderen Fällen entsprechend den Erfordernissen des US-amerikanischen Rechts verwendet werden. Auch diese Art der Verwendung der PNR-Daten war Gegenstand der Verpflichtungen aus dem Jahr 2004. Allerdings wurde sie lediglich im Zusammenhang mit der Weiterübermittlung von Daten erwähnt. In dem neuen Abkommen erhält dieser Aspekt einen größeren Stellenwert; er ist nicht mehr nur eine Folge der Weiterübermittlung, sondern wird in den Rang eines möglichen Verwendungszwecks erhoben.

Die Datenschutzgruppe ist besorgt über diese Änderung der Zweckbindung, die schon in dem vorangegangenen Abkommen für relativ großzügig befunden worden war. Die Kommission wird daher ersucht, schriftlich zu erläutern, unter welchen Voraussetzungen die Daten für andere Zwecke als die drei oben aufgelisteten verwendet werden dürfen.

3. Empfänger der Fluggastdatensätze

Während in der Präambel des Vorgängerabkommens genau angegeben war, welche Stellen des DHS Zugriff auf die PNR-Daten erhalten sollen (nur einige wenige) und welche nicht (z. B. die US-Einwanderungsbehörde und der US-Geheimdienst), enthält das neue Abkommen keine solche Bestimmung. Es heißt darin lediglich, dass das DHS die PNR-Daten aus der EU als sensibel und vertraulich gemäß dem US-Recht behandelt. Die dem DHS unterstellten Behörden, die zuvor nicht explizit angegeben oder als Empfänger der PNR-Daten sogar ausdrücklich ausgeschlossen waren, werden nicht mehr als „Dritte“ angesehen und unterliegen somit auch nicht mehr den Bedingungen für die Weiterübermittlung von PNR-Daten.

Die Datenschutzgruppe bedauert, dass die Zahl der potenziellen Empfänger stark gestiegen ist; um den Datenfluss kontrollieren zu können, wäre es ihrer Ansicht nach wichtig gewesen, die Zahl der Stellen, die auf die PNR-Daten zugreifen dürfen, zu begrenzen. Sie sieht daher in der gegenwärtigen Situation eine Schwächung der Datenschutzgarantien im Vergleich zum Vorgängerabkommen.

4. Weiterübermittlung

Die Weiterübermittlung an „Drittbehörden" innerhalb des DHS, an andere US-Behörden oder an ausländische staatliche Stellen war zuvor ausschließlich in der Verpflichtungserklärung geregelt, wobei das Interimsabkommen an der Situation, wie sie sich infolge des ersten PNR-Abkommens von 2004 darstellte, nicht gerüttelt hat.

Die Verpflichtungserklärung sah vor, dass die PNR-Daten aus der EU an andere Regierungsbehörden, auch solche in Drittländern, nur auf Einzelfallbasis zum Zwecke der Verhütung und Bekämpfung des Terrorismus und damit verknüpfter Straftaten, anderer schwerer länderübergreifender Straftaten einschließlich internationaler organisierter Kriminalität und der Flucht vor Haftbefehlen bzw. Ingewahrsamnahme im Zusammenhang mit den oben genannten Straftaten weitergegeben werden durften. Die Missachtung der Übermittlungsbedingungen konnte Ermittlungen sowie eine Meldung seitens des Datenschutzbeauftragten des DHS nach sich ziehen und dazu führen, dass die Empfängerbehörde für weitere PNR-Übermittlungen nicht mehr in Frage kam.

Obwohl gemäß Abschnitt II des DHS-Schreibens die Weitergabe von PNR-Daten gewissen Beschränkungen unterliegt, steigt aufgrund der gelockerten Zweckbindung der gemeinsam genutzten PNR-Daten die Wahrscheinlichkeit, dass PNR-Daten auch von staatlichen Stellen entgegengenommen und verarbeitet werden, die nicht unbedingt mit der Bekämpfung von Terrorismus und damit zusammenhängenden Straftaten befasst sind. Dasselbe gilt für die Fälle, in denen die PNR-Daten aufgrund der Erfordernisse des US-amerikanischen Rechts benötigt werden. Die Einschränkung, dass die Daten nur von Fall zu Fall weitergegeben werden dürfen, besteht dann nicht mehr, so dass sich die Frage nach einem möglichen künftigen Transfer *en bloc* stellt.

Im Falle der Weitergabe von PNR-Daten durch „Drittbehörden" an andere staatliche Stellen galt nach dem Vorgängerabkommen die CBP-Behörde als Eigentümerin der Daten; eine Offenlegung war nur mit ausdrücklicher vorheriger Genehmigung des CBP möglich, damit der Datenfluss unter Kontrolle blieb. Der Wegfall dieser nützlichen Schutzklausel gibt Anlass zu Bedenken, was die Qualität und Vorhaltung von personenbezogenen Daten betrifft, nachdem sie von einer „Drittbehörde" an andere Stellen weitergeleitet wurden. Es ist nämlich un-

klar, wer künftig die Verantwortung für die Verarbeitung und weitere Verbreitung dieser Daten trägt.

Die Datenschutzgarantien in dem neuen Abkommen sind nicht so zwingend: zum einen, weil die Liste der als Empfänger in Frage kommenden Stellen erweitert wurde und zum anderen, weil die Weitergabe an andere Stellen erleichtert wurde.

Auch für die Weitergabe von PNR-Daten an Behörden in Drittstaaten gelten die früheren, in der Verpflichtungserklärung enthaltenen Garantien, wonach die Übermittlung nur auf Einzelfallbasis erfolgen durfte, nicht mehr. Drittstaaten kommen für den Austausch personenbezogener Daten dann in Frage, wenn davon ausgegangen wird, dass ihre Datenschutzmaßnahmen mit denen des DHS vergleichbar sind. Dabei stellt sich auch die Frage, wie weitere Transfers von Daten kontrolliert werden, nachdem der Drittstaat über sie verfügt.

5. Datenelemente

Die Liste der in Anhang A der Verpflichtungserklärung der USA vom Mai 2004 enthaltenen Datenelemente wurde für das neue Abkommen überarbeitet und ist jetzt Bestandteil von Abschnitt III des DHS-Schreibens.

Die frühere Vereinbarung enthielt eine Liste von 34 Datenelementen, die zu übermitteln waren, sofern sie vom Buchungssystem der Fluggesellschaften erfasst wurden. In dem neuen Abkommen sind 19 Arten von PNR-Daten aufgeführt, die gebündelt wurden und so den Eindruck vermitteln, als sei die Menge der transferierbaren Daten merklich reduziert worden. In der neuen Liste ist das nach dem Vorgängerabkommen verlangte Datenelement „go show information“ (Fluggäste mit Flugschein, aber ohne Reservierung) nicht mehr aufgeführt, dafür aber alle anderen 33 Datenelemente der früheren Liste, wenn auch in bisweilen leicht veränderter Form.

Außerdem enthält die neue Liste Datenelemente, die in der früheren Liste nicht aufgeführt waren. Der Umfang der vom DHS angeforderten Informationen hat somit zugenommen. Dies gilt für eine Reihe von Datenelementen:

a) Datenelement 5 (Verfügbare Vielflieger- und Bonus-Daten): Während in der Vorgängerregelung die Vielfliegerdaten lediglich zurückgelegte Meilen und Anschrift(en) umfassten, werden nach dem neuen Abkommen zusätzlich Vielfliegernummer, Gratisflugscheine u. a. verlangt. Nach dem Vorgängerabkommen gehörten Bonus-Daten nicht zu den abrufbaren Daten.

b) Datenelement 7 (alle verfügbaren Kontaktinformationen): Hierunter werden zwar die früheren Datenelemente Anschrift (6), Rechnungsanschrift (8), Te-

lefonnummern (9) und E-Mail-Adresse (17) zusammengefasst, doch ist nicht auszuschließen, dass zusätzliche Daten wie beispielsweise die E-Mail-Anschrift des Arbeitgebers ebenfalls weitergegeben werden.

c) Datenelement 15 (sämtliche Informationen zum Gepäck): Musste nach dem Vorgängerabkommen nur die Gepäckscheinnummer angegeben werden, so werden jetzt zusätzliche Einzelheiten zum Gepäck eines Fluggastes verlangt, wie etwa Zahl und Größe der Gepäckstücke. Auch in diesem Punkt wird der Anwendungsbereich des Vorgängerabkommens erweitert.

Obwohl die Datenschutzgruppe aktiv für eine Verringerung der Zahl der Datenelemente eingetreten ist, die zur Bekämpfung von Terrorismus und damit verknüpften Straftaten herangezogen werden dürfen[5], wird die Liste der Datenelemente durch das neue Abkommen noch erweitert, indem noch mehr Informationen zu der betroffenen Person abgefragt werden. Dies ist durch nichts zu rechtfertigen und daher als unverhältnismäßig zu werten.

Personenbezogene Daten Dritter

Nach dem Vorgängerabkommen konnte das DHS Daten verlangen, die nicht mit der betroffenen Person, sondern mit Dritten in Zusammenhang standen, z. B. Rechnungsanschrift, E-Mail-Anschrift, Name des Reisebüros, Angabe des Auftraggebers von Sonderdienstleistungen usw. In dem neuen Abkommen ist nicht nur die Liste der Angaben zu den Fluggästen länger, sondern auch die der Angaben zu Dritten, z. B. im Zusammenhang mit Bonus-Informationen, sofern sie im Buchungssystem der Fluggesellschaft erfasst sind.

Die Datenschutzgruppe ist besorgt über diese Entwicklung, da der betroffene Dritte höchstwahrscheinlich gar nicht weiß, dass Daten im Zusammenhang mit seiner Person an das DHS übermittelt werden, von seinen Rechten in einem solchen Fall ganz zu schweigen. Die betroffene dritte Person kann somit die Rechte, die der betroffenen Person nach dem Abkommen zustehen, gar nicht ausüben.

Zusatzdaten

Gemäß Abschnitt III Absatz 3 des DHS-Schreibens darf das DHS in Ausnahmefällen zusätzlich zu den aufgelisteten Datenelementen noch andere, ebenfalls im Buchungssystem der Fluggesellschaften enthaltene Daten abrufen, wodurch die Menge der Datenelemente noch einmal deutlich erhöht wird. Die Datenschutzgruppe ist nach wie vor der Ansicht, dass es andere, im Rahmen der dritten Säule

[5] WP 78 „Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data" (Gewährleistetes Schutzniveau in den Vereinigten Staaten für die Übermittlung von Fluggastdaten) vom 13. Juni 2003.

entwickelte rechtmäßige Kanäle gibt[6], um in derartigen Ausnahmefällen auf personenbezogene Daten zuzugreifen, ohne in die Privatsphäre von Fluggästen einzugreifen. Sorge bereitet der Datenschutzgruppe auch die Aussage, dass das DHS der Europäischen Kommission „in der Regel" innerhalb von 48 Stunden mitteilen wird, dass auf derartige Daten zugegriffen wurde. Damit wird dem DHS ein Ermessensspielraum eingeräumt, wann es bzw. ob es überhaupt Mitteilung macht.

Offen bleibt, auf welche Weise das DHS nach dem Übergang vom „Pull"- zum „Push"- Übermittlungsmodus diese zusätzlichen Daten abrufen wird. Einzelheiten sind in dem neuen PNR-Abkommen nicht geregelt, und es sieht so aus, dass selbst bei Einführung eines aktiven „Push"-Systems das „Pull"-System für derartige Ausnahmefälle aufrechterhalten wird. Die Datenschutzgruppe erwartet daher, dass die Kommission schriftlich darlegt, wie dieses im Ausnahmefall anzuwendende „Pull"-System funktionieren soll und wie die EU in ihrem Zuständigkeitsbereich diese außerordentlichen Befugnisse kontrollieren will.

6. Analytische Informationen

Laut Abschnitt IX des DHS-Schreibens wird das DHS den zuständigen US-Behörden nahelegen, den Polizei- und Justizbehörden der Mitgliedstaaten sowie gegebenenfalls Europol und Eurojust aus den PNR-Daten abgeleitete analytische Informationen zu übermitteln.

Unklar ist, woraus diese analytischen Informationen bestehen und ob sie auch personenbezogene Daten enthalten werden[7].

In Abschnitt IX wird zudem der Erwartung des DHS Ausdruck gegeben, dass die EU und ihre Mitgliedstaaten im Gegenzug ihren zuständigen Behörden ebenfalls nahelegen, dem DHS und anderen US-Behörden aus PNR-Daten abgeleitete analytische Informationen zur Verfügung zu stellen. Die Übermittlung derartiger Informationen an die Vereinigten Staaten ist jedoch durch das neue Abkommen nicht gedeckt, da es darin ausschließlich um die Übermittlung von in den Buchungssystemen der Fluggesellschaften erfassten Daten geht.

Analytische Informationen sind nicht Bestandteil der Liste in Abschnitt III des DHS-Schreibens, in der alle transferierbaren Datenelemente erschöpfend aufgelistet sind. Je nach Art der analytischen Informationen würde ihr direkter Austausch mit anderen USBehörden die Menge der aufgelisteten Datenelemente er-

[6] Auslieferungsabkommen und Abkommen über gegenseitige Amtshilfe zwischen der EU und den USA, beide am 25. Juni 2003 unterzeichnet.

[7] WP 136 „Stellungnahme 4/2007 zum Begriff der personenbezogenen Daten" vom 20. Juni 2007.

heblich vergrößern und der Liste damit ihren erschöpfenden Charakter nehmen. Jedweder Austausch von Informationen dieser Art sollte über andere Rechtsinstrumente erfolgen, da er von diesem Abkommen nicht gedeckt wird. Für die Datenschutzgruppe steht daher fest, dass diese vom DHS in seinem Schreiben geäußerte Erwartung jeglicher Rechtsgrundlage entbehrt, weshalb sie deren Rechtsverbindlichkeit in Zweifel zieht.

7. Art der Übermittlung der PNR-Daten

Wie in dem vorangegangenen Abkommen ist vorgesehen, für die Datenübermittlung später zu einem „Push"-System überzugehen; dies gilt jedoch nur für diejenigen Fluggesellschaften, die über ein den technischen Anforderungen des DHS entsprechendes System verfügen. In allen anderen Fällen werden die PNR-Daten weiterhin von den US-Behörden extrahiert („Pull"-System").

Die europäischen Fluggesellschaften haben in der Vergangenheit in großem Maßstab in ein „Push"-System investiert und bestätigt, dass ein solches System inzwischen technisch machbar sei. Eigentlich sollten die Bemühungen bis Ende Dezember 2006 – der in der Verpflichtungserklärung von 2004 gesetzten Frist – zu einem konkreten Ergebnis geführt haben. Es sei zum jetzigen Zeitpunkt nochmals darauf verwiesen, dass aus datenschutzrechtlicher Sicht ein „Push"-System der einzig annehmbare Weg der Übermittlung personenbezogener Daten ist und dass weitere Verzögerungen zu der Frage verleiten, ob das DHS tatsächlich an einer Änderung der bisherigen Praxis interessiert ist. Die Datenschutzgruppe verfolgt mit großer Sorge die Verzögerungen bei der Einführung eines „Push"-Systems seit Unterzeichnung des PNR-Abkommens im Mai 2004 und verweist diesbezüglich auf ihre früheren Stellungnahmen. Die Datenschutzgruppe erwartet von der Europäischen Kommission die feste Zusage, dass der jetzige Stichtag 1. Januar 2008 nicht noch einmal verschoben wird, beispielsweise weil die Diskussionen über die technischen Anforderungen weiter andauern. Ferner wird erwartet, dass die Kommission angibt, welches die 13 Fluggesellschaften sind, die gemäß Abschnitt VIII des US-Schreibens bereits Daten hinüberschicken („Push"-System) und welches die an sie gestellten Anforderungen sind.

Mit Sorge erfüllt sie nach wie vor der Umstand, dass der Übergang zu einem funktionierenden „Push"-System einseitig vom Ermessen des DHS abhängt und dass das neue Abkommen weder ein gemeinsam vereinbartes Verfahren vorsieht, das zu einer raschen Einführung des „Push"-Systems führt, noch einen Problemlösungsmechanismus.

Die technischen Einzelheiten der Übermittlung der PNR-Daten betreffen in erster Linie die Fluggesellschaften, die deshalb auch gehört werden sollten und deren Anliegen von beiden Vertragsparteien ernst genommen werden müssen. Der Um-

stand, dass es einzig und allein einer Seite überlassen bleibt, darüber zu entscheiden, welche technischen Anforderungen für einen Wechsel vom „Pull"- zum „Push"-System erforderlich sind, gefährdet den Übergang zu einem „Push"-System.

Im Zusammenhang mit der Häufigkeit der einzelnen Datenübermittlungen („Pushes") ist in dem Begleitschreiben lediglich die Rede von Aktualisierungen, die erforderlich werden können, ohne dass angegeben wird, wie oft die Fluggesellschaften nach der erstmaligen Übermittlung 72 Stunden vor Abflug noch weitere Datenübermittlungen vornehmen müssen. Die Datenschutzgruppe ist der Auffassung, dass diese Entscheidung nicht in das alleinige Ermessen des DHS gestellt werden sollte, da die Aktualisierungen in einem angemessenen Verhältnis zum Eingriff in die Privatsphäre der Reisenden und zu den finanziellen Belastungen für die Fluggesellschaften stehen müssen. Deshalb sollte eine für beide Seiten annehmbare Lösung gefunden werden, die einer einseitig getroffenen Entscheidung vorzuziehen ist.

Weder das Abkommen noch das Begleitschreiben des DHS enthalten außerdem irgendwelche Angaben zu einer Begrenzung der Datenanforderungen in der Zeit vor der 72-Stunden-Frist.

8. Herausfiltern sensibler Daten

Eng mit der Frage der Übermittlungsmethode für PNR-Daten verknüpft ist das Filtern der Fluggastdaten (Abschnitt III des DHS-Schreibens).

Einer der wesentlichen Grundsätze des Datenschutzes ist der, dass derjenige, der die personenbezogenen Daten verarbeitet, hierfür die Verantwortung trägt. Dies ergibt sich aus Artikel 2 Buchstabe d in Verbindung mit Artikel 6 Absatz 2 der Richtlinie 95/46/EG. Danach gilt als für die Verarbeitung Verantwortlicher („data controller") jede natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung bestimmt. Ähnliche Bestimmungen finden sich in Artikel 2 Buchstabe d sowie Artikel 5 des Übereinkommens 108. Bei den Fluggastdaten sind es die Fluggesellschaften, die die Daten für ihre eigenen Zwecke erheben und verarbeiten. Ihnen sollte es daher obliegen, dafür zu sorgen, dass nur die in dem Abkommen und dem DHS-Schreiben aufgelisteten Daten an das DHS übermittelt werden. Die Liste der PNR-Daten, die gemäß Abschnitt III des DHS-Schreibens übermittelt werden müssen, enthält keine sensiblen Daten. Allerdings könnten die Datenfelder Nr. 17 „Allgemeine Bemerkungen einschließlich OSI, SSI und SSR" und Nr. 19 „Historie aller Änderungen der PNR-Daten" sensible Daten beinhalten. Da sensible Daten nicht Bestandteil der Liste der transferierbaren Datenelemente sind, verpflichtet sich das DHS, sie herauszufiltern. Es sollte jedoch Aufgabe des für die Verarbeitung Verantwortlichen sein, sämtliche Daten zu filtern, bevor sie im Wege des „Push"-Systems übermittelt werden, damit

keine nicht unter das Abkommen fallenden Daten, zum Beispiel eben sensible Daten, übermittelt werden.

Nach Ansicht der Datenschutzgruppe widerspricht es den Datenschutzgrundsätzen, dass das neue Abkommen diejenigen, die die Daten erheben, von ihrer Verantwortung entbindet und es dem DHS überlässt, bestimmte Daten herauszufiltern. Dies gilt umso mehr für sensible Daten, die nicht verarbeitet werden dürfen. Nach dem neuen Abkommen darf das DHS in Ausnahmefällen bei Bedarf sogar auf in seinem Besitz befindliche sensible Daten zurückgreifen.

Auch wenn sich das DHS verpflichtet hat, ein Protokoll über den Zugang zu sensiblen Daten zu führen und die Daten innerhalb von 30 Tagen zu löschen, nachdem sie nicht mehr benötigt werden, bleibt die Frage unbeantwortet, mit welchen Mitteln die Verwendung und der weitere Verbleib der Daten kontrolliert werden soll, wenn das DHS sensible Daten an andere US- oder ausländische Behörden weitergibt und damit nicht mehr „Eigentümer“ dieser Daten ist.

Angemerkt sei ferner, dass sensible Daten im Sinne des Übereinkommens 108 oder der Datenschutz-Richtlinie vom DHS im Benehmen mit der Europäischen Kommission ermittelt werden. Da sich Verständnis und Bedeutung sensibler Daten im Laufe der Zeit wandeln können, ist es nötig, ständig neue relevante Daten herauszufiltern und gemeinsam mit den Datenschutzbehörden und der Luftverkehrsbranche einer regelmäßigen Überprüfung zu unterziehen, um die Liste auf dem neuesten Stand zu halten. Dieser Aspekt ist in dem neuen Abkommen nicht geregelt. Die Datenschutzgruppe erwartet, in die Gespräche über die Definition sensibler Daten mit eingebunden zu werden.

9. Datenvorhaltung

In dem Abkommen selbst ist die Frage, wie lange die PNR-Daten vom DHS vorgehalten werden dürfen, nicht geklärt. Jedoch enthält Abschnitt VII des DHS-Schreibens eine diesbezügliche Regelung; dabei wird unterschieden zwischen einer aktiven analytischen Datenbank, in der die Daten sieben Jahre lang gespeichert werden, was einer Verdoppelung der früheren Speicherfrist gleichkommt, und einem „ruhenden“ bzw. inaktiven Status, in dem die Daten für weitere acht Jahre verbleiben. In der Verpflichtungserklärung von 2004 war festgelegt, dass die Daten in eine Datei für gelöschte Datensätze überführt werden, wo sie acht Jahre verbleiben, aber dies galt nur für die begrenzte Zahl von Daten, auf die während der anfänglichen Speicherfrist von dreieinhalb Jahren manuell zugegriffen wurde.

Aus datenschutzrechtlicher Sicht besteht kein Unterschied zwischen aktiven und so genannten ruhenden Zugriffsfristen. Solange die personenbezogenen Daten

zugänglich sind, selbst wenn sich der Zugang auf einige wenige Fälle während der „Ruhefrist“ bezieht, bleiben sie in einer Datenbank für das DHS abrufbar, das sie dann verarbeiten kann. Somit wurde die Speicherfrist de facto von dreieinhalb auf fünfzehn Jahre verlängert.

Aber selbst diese Frist muss nicht unumstößlich sein, denn in dem DHS-Schreiben heißt es weiter, dass das DHS davon ausgeht, dass die PNR-Daten am Ende dieses Zeitraums gelöscht werden, wobei die Frage, ob und wann die Daten vernichtet werden, im Rahmen weiterer Gespräche zwischen dem DHS und der EU noch zu erörtern sein wird. Dies legt den Schluss nahe, dass die Speicherfrist sogar noch länger ausfallen könnte, was höchst bedenklich und mit anerkannten Datenschutzgrundsätzen, wie sie in Artikel 5 lit. e des Übereinkommens 108 und Artikel 6 Buchstabe e der Datenschutzrichtlinie verankert sind, nicht vereinbar ist.

Die Datenschutzgruppe hielt bereits die dreieinhalbjährige Vorhaltungsfrist gemessen am Zweck der Fluggastdatenspeicherung für unverhältnismäßig. Der Nachweis, dass die bestehende Frist notwendig ist (wie in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte verlangt) oder nicht ausreicht, wurde nicht erbracht.

Des Weiteren wird in dem DHS-Schreiben ausgeführt, dass die aufgrund des früheren Abkommens erhobenen Daten nun ebenfalls den längeren Speicherfristen des neuen Abkommens unterliegen. Dies widerspricht der Verpflichtungserklärung der USA vom Mai 2004, die eine allgemeine, in gegenseitigem Einvernehmen festgelegte Speicherfrist von dreieinhalb Jahren vorsah. Das DHS hat die Speicherfrist für diese auf der Grundlage des ersten PNR-Abkommens erhobenen Daten (zwischen dem 28. Mai 2004 und Oktober 2006) einseitig verlängert. Alle in diesem Zeitraum an das DHS weitergeleiteten Daten wurden in der festen Überzeugung übermittelt, dass sie nach dreieinhalb Jahren vernichtet würden, sofern in dieser Zeit nicht manuell auf sie zugegriffen wird. Dieses Prinzip wird jetzt durch das DHS-Schreiben ausgehebelt. Die durch das DHS einseitig und ohne ersichtlichen Grund vorgenommene Verlängerung der Speicherfrist ist daher nicht akzeptabel.

10. Gemeinsame Überprüfung

Gemäß Nummer 4 des neuen Abkommens und Abschnitt X des DHS-Schreibens werden die Vertragsparteien die Durchführung des Abkommens, des Begleitschreibens und der PNR-Regelungen und -Verfahren der USA und der EU in regelmäßigen Abständen überprüfen, um sich wechselseitig zu vergewissern, dass ihr System ordnungsgemäß und unter Gewährleistung des Schutzes der Privatsphäre funktioniert. In dem Schreiben heißt es ferner, dass dabei alle Fälle, in

denen auf sensible Daten zugegriffen wurde, ebenfalls überprüft werden. Vorgenommen werden soll die Überprüfung durch den US-Heimatschutzminister und das für den Bereich Justiz, Freiheit und Sicherheit zuständige Kommissionsmitglied oder durch einen für beide Seiten akzeptablen Beamten, den die Vertragsparteien einvernehmlich benennen. Die Modalitäten der gemeinsamen Überprüfung werden von der EU und dem DHS gemeinsam festgelegt.

Im Vergleich zur Verpflichtungserklärung wurden in Bezug auf die unabhängige Überwachung des Systems aus datenschutzrechtlicher Sicht deutliche Abstriche gemacht.

Die Verpflichtungserklärung sah eine Überprüfung mindestens einmal jährlich oder auf beiderseitigen Wunsch der Parteien auch öfter vor. Aus dem neuen Abkommen geht hingegen nicht genau hervor, wie oft die geplante Überprüfung stattfinden soll bzw. ob sie überhaupt stattfindet. Das DHS-Schreiben nennt weder einen genauen Termin für die Überprüfung noch liefert es irgendwelche Anhaltspunkte, wann mit den Vorbereitungen hierfür begonnen werden soll.

Des Weiteren ist in dem DHS-Schreiben auch nicht mehr die Rede davon, dass die Vertragsparteien bei der Überprüfung von unabhängigen Vertretern europäischer Strafverfolgungsbehörden und/oder Behörden der EU-Mitgliedstaaten unterstützt werden müssen. Unabhängige Sachkompetenz und Kontrolle gehören zu den Eckpfeilern eines wirksamen Datenschutzes; sie gewährleisten, dass Mängel ordentlich behoben und den Anliegen der betroffenen Personen Gehör geschenkt wird.

Im Rahmen des ersten PNR-Abkommens fand eine Überprüfung statt, die gemeinsam von den Vertragsparteien unter Einbeziehung der unabhängigen Datenschutzbehörden organisiert wurde und als Erfolg betrachtet werden kann. Die Datenschutzgruppe verweist daher nochmals auf die Notwendigkeit, die Datenschutzbehörden zu allen künftigen Überprüfungen hinzuzuziehen. Fehlende Unabhängigkeit auf Seiten der Prüfer kann den Datenschutz für Fluggäste lockern. Die Datenschutzgruppe erwartet daher, dass sie in die Vorbereitung und Durchführung der gemeinsamen Überprüfung eingebunden wird. Sie erwartet, dass die Kommission so bald wie möglich schriftlich ausführt, wann und wie die Überprüfung des Abkommens vorbereitet und ausgeführt wird.

Ein weiteres Problem ergibt sich aus dem Umstand, dass eine Überprüfung nur stattfindet, wenn beide Seiten sich auf deren Modalitäten verständigen. Können sich die Vertragsparteien nicht einigen oder stellt sich eine Partei einseitig quer, erfolgt überhaupt keine Überprüfung, was de facto bedeutet, dass bestehende Probleme nicht in der gebührenden Weise angegangen werden. Das neue Abkommen sieht keinen Mechanismus vor, um derartige Konflikte zu lösen: vielmehr verfügen die Vertragsparteien über einen weitreichenden Ermessensspielraum,

der es ihnen ermöglicht, die Modalitäten einer Überprüfung zu beeinflussen und den eigenen Vorstellungen anzupassen. Die Datenschutzgruppe erwartet, dass sich die Kommission auch dieser Frage widmet, auch vor dem Hintergrund, dass es während des PNR-Interimsabkommens zu keiner gemeinsamen Überprüfung kam, da sich die Vertragsparteien nicht auf die Einzelheiten des Verfahrens einigen konnten.

11. Rechte der betroffenen Personen (z. B. Widerspruchsrecht)

Die Datenschutzgarantien, die die US-Behörden den Reisenden im Zusammenhang mit der Übermittlung und Verarbeitung von PNR-Daten geben wollen, sind nicht Bestandteil des eigentlichen Abkommens, sondern Gegenstand des DHS-Begleitschreibens.

Zwar sind sowohl das Abkommen als auch das DHS-Begleitschreiben rechtsverbindlich, doch bleibt das Schreiben, wie in dieser Stellungnahme erläutert wird, in vielen Punkten vage. Bei der Umsetzung der Zusicherungen bleibt viel dem Ermessen des DHS überlassen, z. B. der Übergang von „Pull"- zum „Push"-System und die 15-Jahres-Speicherfrist. Bei so vielen ungeklärten Details stellt sich die Frage, wie die Zusicherungen des DHS in seinem Schreiben rechtlich durchgesetzt werden können. Nach Ansicht der Datenschutzgruppe sind die Garantien des DHS-Schreibens rechtlich gesehen weniger robust als in dem Vorgängerabkommen.

Zwar wird in Abschnitt V des DHS-Schreibens auf gesetzliche Regelungen hingewiesen, auf die sich die Reisenden zur Durchsetzung ihrer Rechte berufen können, doch ist nicht klar, ob das DHS-Schreiben überhaupt im amerikanischen Gesetzblatt veröffentlicht wird und als Rechtsgrundlage für die Durchsetzung von datenschutzrechtlichen Ansprüchen herangezogen werden kann. Die Datenschutzgruppe fordert daher die Europäische Kommission auf, auf die Veröffentlichung des Schreibens im Federal Register hinzuwirken.

Trotz dieser Einschränkung würdigt die Datenschutzgruppe den Umstand, dass sich das DHS entschlossen hat, US-amerikanische datenschutzrechtliche Verwaltungsvorschriften auch auf Reisende anzuwenden, die weder US-amerikanische Staatsbürger sind noch ihren rechtmäßigen Aufenthalt in den USA haben.

Nicht-US-Amerikaner sind somit gegenüber US-amerikanischen Staatsbürgern nicht mehr benachteiligt. Damit wird dem universellen Recht auf Datenschutz Geltung verschafft. Dies ist sicherlich ein positives Signal, doch bleibt noch Einiges zu tun, um sicherzustellen, dass die Rechte auch in der Praxis geltend gemacht werden können. Hierbei fällt den Datenschutzbehörden eine gewichtige Rolle zu.

Die Gruppe begrüßt ferner, dass die USA zusammen mit der EU im Interesse der Reisenden für eine bessere Publizität der Hinweise über die PNR-Systeme sorgen und die Fluggesellschaften dazu anhalten wollen, diese Hinweise in den offiziellen Beförderungsvertrag aufzunehmen. Diese Vereinbarung im Rahmen des neuen Abkommens, durch die die Transatlantikreisenden besser über ihre Rechte und Rechtsbehelfe informiert werden, wird sicherlich zu mehr Transparenz führen.

Die Datenschutzgruppe, die die einzelstaatlichen Datenschutzbehörden repräsentiert, war bei der Abfassung und Verbreitung der bisherigen Hinweisblätter der Fluggesellschaften behilflich und geht davon aus, auch in Zukunft an dieser wichtigen Arbeit beteiligt zu werden.

12. Auswirkungen des Abkommens auf eine etwaige EU-Regelung für PNR-Daten

Nummer 5 des neuen Abkommens und Abschnitt IX des DHS-Schreibens („Gegenseitigkeit“) sind hinsichtlich der Erwartungen der US-amerikanischen Seite an das Maß an Datenschutz, das für die US- und eine etwaige künftige EU-Regelung im Bereich der PNR-Daten gelten soll, nicht eindeutig. Zwar wird diese Aussage allgemein so verstanden, dass die USA bei einer künftigen EU-Regelung im Bereich der PNR-Daten kein Schutzniveau erwartet, das unter dem des neuen Abkommens liegt, aber sie könnte ebenso gut auch bedeuten, dass das DHS von der EU verlangt, bei einer PNR-Regelung der EU kein höheres Datenschutzniveau anzusetzen; anderenfalls würde es das Abkommen aussetzen. Dies wäre eine äußerst Besorgnis erregende Entwicklung und könnte die Bemühungen der EU um ein hohes Maß an Datenschutz in einer möglichen künftigen EU-Regelung erschweren. Es ist von außerordentlicher Bedeutung, dass die Europäische Kommission die genaue Bedeutung dieser Klausel schriftlich klarstellt.

Außerdem sei angemerkt, dass der Abschnitt zur Gegenseitigkeit unausgewogen ist, da die Vereinigten Staaten lediglich verpflichtet werden, die Einhaltung dieses Grundsatzes durch die US-Fluggesellschaften aktiv zu fördern, während die Europäische Union dessen Einhaltung garantieren soll.

III. Schlussfolgerungen

Die Datenschutzgruppe wertet es als positiv, dass ein neues langfristiges PNR-Abkommen mit den Vereinigten Staaten über die Übermittlung von PNR-Daten an das DHS zustande gekommen ist. Das Vorhandensein eines solchen Abkommens ist von größter Bedeutung, damit für Mitgliedstaaten, Flugreisende und Fluggesellschaften gleichermaßen kein rechtliches Vakuum entsteht.

Die Datenschutzgruppe würdigt die Tatsache, dass das DHS die Transparenz der Verarbeitung der PNR-Daten mittels entsprechender Hinweise an die Flugreisenden verbessern will. Sie verweist nochmals darauf, dass sie sich in der Vergangenheit mit dem Datenschutzbeauftragten des DHS ins Benehmen gesetzt hat und daraufhin zwei Stellungnahmen abgegeben hat[8], die den Fluggesellschaften als Orientierung dienen und die Reisenden besser mit diesem Sachverhalt vertraut machen sollten. Die Datenschutzgruppe begrüßt ferner, dass durch eine politische Entscheidung des DHS der Datenschutz entgegen dem früheren Abkommen auch für Nicht-US-Bürger gilt.

Sie bedauert hingegen, dass diese geringfügigen Verbesserungen angesichts der generellen Senkung des Datenschutzniveaus kaum ins Gewicht fallen. Die Zusicherungen in dem DHS-Begleitschreiben sind nicht so weit reichend wie diejenigen in der Verpflichtungserklärung. Sie bedauert ebenfalls, dass die EU die Datenschutzgarantien des Abkommens für angemessen befunden hat, ohne die Meinung einer anerkannten Datenschutzinstanz eingeholt zu haben, und dies, obwohl das Abkommen von den Mitgliedstaaten künftig in enger Zusammenarbeit mit den einzelstaatlichen Datenschutzbehörden umgesetzt werden muss.

Die Datenschutzgruppe hält die Zweckbindung der Fluggastdatenübermittlung für zu weit gefasst und bedauert, dass die Zweckbestimmungen über das hinausgehen, was nach den üblichen Datenschutzgrundsätzen zulässig wäre; dies gilt ebenfalls für die vielen Ausnahmen, die nicht hinlänglich genau spezifiziert sind. Die Datenschutzgruppe nimmt besorgt zur Kenntnis, dass die Zahl der möglichen Empfänger innerhalb des DHS stark gestiegen ist und es keine verlässliche Liste aller DHS-Abteilungen und Behörden gibt, denen der Zugriff auf die PNR-Daten gestattet ist.

Was die Art der Übermittlung der PNR-Daten betrifft, stellt die Datenschutzgruppe besorgt fest, dass sich die Einführung eines „Push"-Systems seit Unterzeichnung des PNR-Abkommens im Mai 2004 immer wieder verzögert hat. Sie erwartet deshalb, dass es zu keiner weiteren Verschiebung kommt. Die Datenschutzgruppe wendet sich gegen die Bestimmung in dem neuen Abkommen, wonach der Übergang vom „Pull"- zum „Push"-System in das alleinige Ermessen des DHS gestellt wird, ohne dabei die legitimen Rechte der betroffenen Fluggesellschaften zu berücksichtigen. Dies gilt auch für die Häufigkeit der Übermittlungen, die ebenfalls dem Gutdünken des DHS überlassen bleibt. Die Verbesse-

[8] WP 97 „Stellungnahme 8/2004 zur Unterrichtung von Fluggästen anlässlich der Übermittlung persönlicher Daten bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika" vom 30. September 2004 und
WP 132 „Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden" vom 15. Februar 2007 sowie ein „Kurzes Informationsblatt für Reisen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika".

rung des Datenschutzes muss in gegenseitigem Einvernehmen und auf wirtschaftlich tragfähige Weise ohne Benachteiligung irgendwelcher Beteiligten – insbesondere der Fluggesellschaften der EU – erreicht werden.

Die deutliche Verlängerung der Speicherfrist und die Erweiterung der Liste der zu übermittelnden einzelnen Datenelemente bedeuten weitere Abstriche beim Datenschutz im Vergleich zum Vorgängerabkommen. Der Umstand, dass sensible Daten nach wie vor vom DHS herausgefiltert werden und dem DHS in Ausnahmefällen sogar der Zugriff auf diese Daten gestattet ist, widerspricht anerkannten Datenschutzgrundsätzen, wie sie beispielsweise das Übereinkommen 108 und die Datenschutzrichtlinie enthalten.

Die Datenschutzgruppe hält eine Beteiligung der Datenschutzbehörden an einer unabhängigen Überprüfung des Abkommen sowohl in der Vorbereitungs- als auch in der praktischen Durchführungsphase für unerlässlich. Die Kommission muss klarstellen, wann und wie die Überprüfung des Abkommens vorbereitet und ausgeführt wird.

Es gibt keine rechtliche Grundlage für den Austausch analytischer Informationen; es ist daher fraglich, inwieweit die diesbezüglichen Erwartungen des DHS rechtsverbindlich sind.

Die Datenschutzgruppe verkennt nicht, dass das neue PNR-Abkommen im Vergleich zu dem früheren Abkommen einige kleinere Verbesserungen enthält, macht aber auch aus ihrer Enttäuschung über das unzureichende Datenschutzniveau des neuen PNR-Abkommens keinen Hehl. Das neue Abkommen weist noch nicht einmal das Datenschutzniveau des früheren PNR-Abkommen auf, das von der Datenschutzgruppe in ihren vorangegangenen Stellungnahmen bereits als niedrig eingestuft wurde.

Das neue PNR-Abkommen schneidet gemessen an anerkannten Datenschutzgrundsätzen wie denen des Übereinkommens 108 oder der Datenschutzrichtlinie nicht gut ab. Es wird bei Transatlantikreisenden, die sich um ihre Rechte im Bereich des Datenschutzes sorgen, verständliche Bedenken hervorrufen. It will cause understandable concern for all transatlantic travellers who are worried about their privacy rights.

Brüssel, den 17. August 2007

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR

V. Internationale Konferenz der Datenschutzbeauftragten

Resolutionen der 29. Konferenz vom 26. – 28. September 2007 in Montreal

Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Strafverfolgungs- und Grenzschutzzwecken herangezogen werden*

Die Konferenz beruft sich auf

- das 2002 auf der 24. Internationalen Konferenz in Cardiff angenommene Kommuniqué;
- die 2003 auf der 25. Internationalen Konferenz in Sydney angenommene Resolution über die Übertragung von Passagierdaten;
- die 2005 auf der 27. Internationalen Konferenz in Montreux verabschiedete Deklaration zum Datenschutz und zum Schutz der Privatsphäre in einer globalisierten Welt;

in denen zum Ausdruck kommt, dass es gilt, zwischen dem legitimen Kampf gegen den Terrorismus und gegen die internationale Kriminalität einerseits und dem Datenschutz und dem Schutz der Privatsphäre andererseits ein Gleichgewicht herzustellen.

Die Konferenz vermerkt, dass

- Regierungsstellen zunehmend den Zugriff zu Passagierdaten suchen, die im Kampf gegen den Terrorismus, gegen illegale Einwanderung und andere Verbrechen verwendet werden sollen, ohne dass genügend Rücksicht auf Persönlichkeitsschutz und die Menschenrechte der Passagiere genommen wird;

* Antragsteller: Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (Deutschland)
Unterstützt von: Österreichische Datenschutzkommission (Österreich), Office of the Privacy Commissioner of Canada (Kanada), Office of the Information and Privacy Commissioner of British Columbia, Office of the Information and Privacy Commissioner of Ontario, European Data Protection Supervisor (Europäische Gemeinschaft), La Commission Nationale de l'Informatique et des Libertés (Frankreich), Landesbeauftragte für Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (Deutschland – Regional), Garante per la protezione dei dati personali (Italien), College Bescherming Persoonsgegevens (Niederlande), Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Rumänien), Agencia de Protección de Datos (Spanien), Information Commissioner (Vereinigtes Königreich)

- manche Passagierdaten dazu benutzt werden können, Folgerungen über Religionszugehörigkeit, Ethnie und andere äußerst heikle Zusammenhänge zu ziehen,

- weltweit viele Regierungen ständig mehr Daten von Verkehrsträgern verlangen,

- Verkehrsträger die Passagierdaten aus kommerziellen Gründen erfassen und dann aufgefordert werden, sie für Justizvollzugszwecke zur Verfügung zu stellen,

- Verkehrsträger zunehmend viele verschiedene Forderungen zur Übergabe von Daten erfüllen müssen und sich an viele verschiedene Datenübertragungssysteme halten müssen, wodurch unter den Verkehrsträgern wie auch unter den Passagieren Ungewissheit über ihre Rechte und Pflichten entsteht, wodurch die Passagiere nur schwer verstehen, wie ihre Daten genutzt werden, und wodurch auch das Risiko entsteht, dass die Verkehrsträger die Daten unsachgemäß übertragen,

- diese vielen verschiedenen Forderungen und Systeme sowohl für die Verkehrsträger als auch für die Passagiere mit Kosten verbunden sind,

- juristische und technische Übereinstimmung erforderlich ist, damit die Verkehrsträger diese Forderungen erfüllen können,

- manche Verkehrsträger immer noch nicht ihrer Pflicht nachkommen, Passagiere über die Verwendung und Offenlegung ihrer Daten zu unterrichten,

- andere globale Abmachungen zur Erleichterung des internationalen Flugverkehrs getroffen worden sind, und dass dringender Bedarf besteht, globale Lösungen zu treffen, die den internationalen Reiseverkehr erleichtern und dabei das Recht der Passagiere auf Persönlichkeitsschutz respektieren.

Die Konferenz bestätigt erneut, dass

- Datenschutz und Schutz der Privatsphäre – wie in Art. 12 der Allgemeinen Deklaration der Menschenrechte und in anderen Rechtsinstrumenten verankert – Privatpersonen und ihre persönlichen Daten schützen und zusammen mit anderen Rechten in allen Ersuchen zur Übertragung und Nutzung von Passagierdaten für Justizvollzugszwecke berücksichtigt werden müssen,

- die Verarbeitung von Passagierdaten in einem Rahmen stattfinden sollte, der die anerkannten Datenschutzgrundsätze und -standards berücksichtigt,

- in allen Ersuchen staatlicher Behörden für die Nutzung von Passagierdaten Folgendes nachgewiesen werden sollte:

  – sie sind nachweisbar notwendig, um ein spezifisches Problem anzusprechen,

  – sie sind nachweisbar mit Wahrscheinlichkeit geeignet, das Problem anzusprechen,

  – sie entsprechen proportional ihrem Sicherheitswert, und

  – sie greifen nachweisbar weniger in die Privatsphäre ein als alternative Optionen, sowie dass all solche Ersuche regelmäßig zu überprüfen sind, um festzustellen, ob die Maßnahmen noch erforderlich sind,

  – die Notwendigkeit, unter allen Umständen die Privatsphäre zu schützen, nicht nur für globale Datenschutzkreise, sondern auch für alle eine grundsätzliche Aufgabe bleibt, die um die Wahrung der fundamentalen Rechte und Freiheiten besorgt sind, und

  – wenn Regierungsstellen sich nicht bemühen, die Datenschutzbelange richtig zu wägen, die echte Gefahr besteht, dass diese Stellen beginnen könnten, die fundamentalen Rechte und Freiheiten selbst, die sie schließlich schützen wollen, zu unterminieren.

Im Bestreben nach globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden, ruft die Konferenz dazu auf,

- dass internationale Organisationen (wie z. B. IATA und ICAO), Regierungsstellen und Verkehrsträger mit den Beauftragten für den Datenschutz und für die Privatsphäre zusammenarbeiten, um verbindliche globale Lösungen mit angemessenen Datenschutzsicherheiten einzuführen,

- dass Regierungsstellen gewährleisten, dass alle Ersuche für die Nutzung von Passagierdaten

  – nachweisbar notwendig sind, um ein spezifisches Problem anzusprechen,

  – nachweisbar mit Wahrscheinlichkeit geeignet sind, das Problem anzusprechen;

  – ihrem Sicherheitswert proportional entsprechen, und

  – nachweisbar weniger in die Privatsphäre eingreifen als alternative Optionen,

  – sowie dass all solche Ersuche regelmäßig überprüft werden sollten, um festzustellen, ob die Maßnahmen noch erforderlich sind,

- dass alle Passagierdaten nutzenden staatlichen Programme für Datenminimalisierung sowie für die ausdrückliche Beschränkung der Nutzung, Offenlegung und Einbehaltung der Daten auf die entsprechenden Programmzwecke sowie für die Richtigkeit der Daten, für das Recht auf Zugriff zu den Daten, für die Korrigierung der Daten und für eine unabhängige Überprüfung sorgen sollten,

- dass alle Lösungen die juristischen, technischen, finanziellen und wirtschaftlichen Belange der Verkehrsträger und der Behörden berücksichtigen müssen,

- dass Regierungsstellen offen und transparent die Zwecke, zu denen die Daten gesammelt und genutzt werden, angeben, und sicher stellen, dass alle Passagiere – ungeachtet ihrer Nationalität oder ihres Herkunftslandes – Zugang zu ihren persönlichen Informationen sowie zu einem angemessenen Rechtshilfemechanismus haben,

- dass Verkehrsträger ihre Passagiere über die Nutzung und Offenlegung ihrer Daten durch Regierungsstellen und Justizvollzugsbehörden, über Flugverbotslisten und ähnliche Überwachungslisten sowie über die Verfügbarkeit von Rechtshilfemaßnahmen im Zusammenhang mit Passagierdaten und damit zusammenhängenden persönlichen Informationen ausreichend unterrichten, und

- dass die Beauftragten für den Datenschutz und den Schutz der Privatsphäre weiterhin zusammenarbeiten, um sachgemäße Datenschutzmaßnahmen zu gewährleisten und auf verbindliche globale Lösungen zu dringen.

Erläuternder Hinweis

Die Regierungen verschiedener Länder haben zunehmend versucht, Passagierdaten als Waffe im Kampf gegen Terrorismus, transnationale Kriminalität und andere Verbrechen zu nutzen. Dadurch sind in Bezug auf die geforderten Datenelemente, die Verwendung der Daten und die Stufe der Sicherheitsmaßnahmen Differenzen aufgetreten.

Das Wesen des internationalen Reiseverkehrs fordert einen globalen Ansatz, und es ist eine globale Lösung dringend erforderlich, um eine angemessene Sicherheitsstufe zu erlangen und das Vertrauen der Passagiere zu gewinnen, während proportionale Maßnahmen unternommen werden, die den notwendigen Datenschutz und den Schutz der Privatsphäre beinhalten.

Während Bedenken über den Datenschutz und den Schutz der Privatsphäre die vorrangigen Themen darstellen, die bei jeder globalen Lösung zu berücksichtigen sind, bietet sich auch Gelegenheit, andere juristische, technische, finanzielle und wirtschaftliche Fragen von Fluggesellschaften und Passagieren in Betracht zu ziehen.

Globale Standards können die Fairness, Übereinstimmung, juristische Gewissheit und Sicherheit für Passagiere und Verkehrsträger gewährleisten. Es ist klar, dass Verkehrsträger, Justizvollzugsbehörden, internationale Organisationen, zivilgesellschaftliche Gruppen und Datenschutzexperten an der globalen Lösung beteiligt sein müssen. Das Engagement der Datenschutzbeauftragten ist unentbehrlich, wenn Fortschritte erzielt werden sollen. Sie müssen die Führung übernehmen und auf einer solchen Lösung bestehen.

Resolution über die Entwicklung internationaler Standards[1]

Die Entwicklung von Standards im Datenschutz für die Anwendung und den Einsatz neuer und bestehender Technologien ist in den letzten Jahren Gegenstand erheblicher Debatten und Diskussionen sowohl innerhalb der internationalen Normungsorganisationen als auch in internationalen Datenschutzkreisen. Solche Standards sind u. a. bereits auf den 25., 26. und 28. internationalen Konferenzen in Sydney/Australien, Breslau/Polen und London/Großbritannien erörtert worden.

Diese Diskussionen spiegeln die zunehmende Erkenntnis in Kreisen des Datenschutzes und des Schutzes der Privatsphäre wider, dass Datenschutzgesetze und Gesetze zum Schutz der Privatsphäre zwar zum Schutz privater Informationen unerlässlich sind, dass sie allein jedoch nicht genügen. Vielmehr sind auch internationale Standards erforderlich, um die Beteiligten bei der Aufstellung und Befolgung gesetzlicher Regelungen zum Datenschutz und zum Schutz der Privatsphäre zu unterstützen.

Die Entwicklung von Datenschutzstandards für die Nutzung und den Einsatz neuer und bestehender Technologien sollte nicht so verstanden werden, dass sie von der zentralen Rolle der einzelnen nationalen Datenschutzbehörden und Kommissionen zum Schutz der Privatsphäre ablenken. Standards sind eine Methode

[1] Antragsteller: Datenschutzbeauftragter von Kanada
Unterstützt durch: Bundesbeauftragter für den Datenschutz, Deutschland, Datenschutzkommission, Belgien, Berliner Beauftragter für Datenschutz und Informationsfreiheit, Ontario Beauftragter für Datenschutz und Informationsfreiheit, Datenschutzbeauftragter, Spanien, Eidgenössische Datenschutzbeauftragte, Schweiz

zur Anwendung technischer und organisatorischer Spezifikationen, die gesetzliche Regelungen für die Praxis interpretieren können. Was technische Standards anbelangt, so ist dies bisher ohne aktive Beteiligung der Datenschutzkreise geschehen. Diese Situation muss sich ändern, damit die konsequente Interpretation und Befolgung gewährleistet ist.

Mit der Aufstellung der Arbeitsgruppe 5 (Identitätsmanagement und Datenschutztechnologien) im Unterausschuss 27 (Sicherheit der Informationstechnik) hat die Internationale Organisation für Normung (ISO) ihre Absicht bekundet, die Entwicklung von Datenschutzstandards voranzutreiben. Die Arbeitsgruppe hat dazu aufgerufen, mit der Internationalen Konferenz der Datenschutzbeauftragten (im Folgenden die „Konferenz") zusammenzuarbeiten. Besonders hervorgehoben werden dabei die gemeinsamen Datenschutzinteressen beider Organisationen sowie das Ziel der Arbeitsgruppe, „Aspekte des Identitätsmanagements, der Biometrik und des Datenschutzes im Zusammenhang mit der Informationstechnologie mit einem internationalen Standardpaket zu harmonisieren".

Wenn auch die Entwicklung datenschutzrelevanter Standards[2] unter der Federführung einer sicherheitsorientierten Gruppe keine Ideallösung für die am Datenschutz und dem Schutz der Privatsphäre Beteiligten darstellt, ist dies nun einmal – zumindest vorläufig – die von der ISO gewählte Struktur. Will man gewährleisten, dass Datenschutzstandards entwickelt werden, ist es unerlässlich, auf diesen Ansatz von Seiten der Normungskreise mit aktiverer Einbindung in den Standardentwicklungsprozess zu reagieren. Es ist auch eine natürliche Erweiterung der Arbeit, die von der Konferenz bereits im Einvernehmen mit dem Datenschutz in anderen Kompetenzbereichen auf internationaler Ebene geleistet wird – zum Beispiel mit der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung und der Asiatisch-Pazifischen Wirtschaftsgemeinschaft –, dass man sich mit Datenschutzfragen befasst, die durch grenzüberschreitende Datenströme entstehen. Vereinfacht ausgedrückt, liegt es im besten Interesse der Konferenz sowie der Normungsexperten, dass die Konferenzmitglieder einen kooperativeren, gemeinschaftlicheren Weg zur Entwicklung von Standards antreten.

Die Konferenz fasst darum folgende Entschlüsse:

1. Die Konferenz unterstützt die Entwicklung effektiver, universal akzeptierter internationaler Datenschutzstandards und wird der ISO dafür ihre Erfahrungen bei der Entwicklung solcher Standards zur Verfügung stellen.

---

[2] Zu den Standards, an denen die neue ISO-Arbeitsgruppe gegenwärtig arbeitet, gehören ISO 29101 – Eine Datenschutz-Referenzarchitektur (beste Praktiken für konsequente technische Implementierung von Datenschutzprinzipien); ISO 29100 – Ein Datenschutzrahmen (Definition von Datenschutzanforderungen bei der Verarbeitung persönlicher Daten in den Informationssystemen aller Länder); und ISO 24760 – Ein Rahmen für Identitätsmanagement (Rahmen für das sichere, zuverlässige Datenschutzkonformitäts-Management der Identitätsinformationen).

2. Die Konferenz ruft ihre Mitglieder auf, sich über ihre nationalen Normungsorganisationen stärker am Entwicklungsprozess der ISO-Standards zu beteiligen.

3. Angesichts der Tatsache, dass vielen Mitgliedern nur beschränkte Mittel zur Verfügung stehen, ruft die Konferenz ihre Mitglieder auf, in Betracht zu ziehen, wie sie ihre Erfahrungen und Fachkenntnisse am Besten teilen können, um diese Erfahrungen und Fachkenntnisse der ISO zur Verfügung zu stellen.

4. Die Konferenz ruft ihre Mitglieder auf, in Betracht zu ziehen, wie sie ihre Beiträge zum Standardentwicklungsprozess am Besten koordinieren können, damit gewährleistet ist, dass diese Beiträge allen Konferenzmitgliedern zugute kommen.

5. Die Konferenz ruft ihre Mitglieder auf, potentielle Mechanismen zu untersuchen, die zur Zusammenarbeit zwischen ISO und der Konferenz zustande bringen.

6. Die Konferenz ruft ihre Mitglieder auf, die Beteiligung an der Entwicklung von ISO-Standards durch andere Interessierte (wie Akademiker, NGOs, Forschungszentren usw.) aktiv zu fördern und sie aufzufordern, sich über ihre nationalen Normungsorganisationen zu beteiligen.

Resolution über internationale Zusammenarbeit *

Unter Bezugnahme auf die Deklaration von Montreux, in der die Bereitschaft der Datenschutzbeauftragten, die Zusammenarbeit untereinander und mit anderen mit dem Datenschutz befassten Organisationen zu fördern, und in der Regierungen aufgerufen wurden, die Einführung von Rechtsmitteln für den Datenschutz und den Schutz der Privatsphäre einzuführen,

in der Erkenntnis, dass mehrere internationale Organisationen aktiv die Zusammenarbeit im Datenschutz fördern, einschließlich dieser Konferenz, dem Europarat, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der Asiatisch-Pazifischen Wirtschaftsgemeinschaft (APEC), den Asiatisch-Pazifischen Datenschutzbehörden (APPA), dem Iberoamerikanischen Datenschutznetz, dem Verband französischsprachiger Datenschutzbehörden, und der Arbeitsgruppe „Artikel 29 der Europäischen Union“,

* Antragsteller: Privacy Commissioner of Canada
Unterstützt von: Information Commissioner, UK, Privacy Commissioner, New Zealand, Information and Privacy Commisssioner, Alberta, Information and Privacy Commissioner, Saskatchewan

in Anerkennung der seit der 28. Konferenz in Paris und Brüssel unternommenen Schritte als Teil der Londoner Initiative, praktische Informationen mit dem Ziel auszutauschen, den Datenschutz durch bessere Kommunikation und Durchsetzung effektiver zu gestalten,

im Bewusstsein, dass die sowohl an Volumen als auch an Komplexität zunehmenden globalen Datenströme mit personenbezogenen Informationen in Hinsicht auf den Schutz persönlicher Informationen zu neuen Herausforderungen führen, und

im Bewusstsein, dass eine zunehmende Anzahl an Nationen heute die wichtige Bedeutung des Datenschutzes erkannt hat und schnell dazu übergeht, sich mit dem Schutz personenbezogener Informationen auf eine Weise zu befassen, die ihren jeweiligen juristischen, politischen und kulturellen Realitäten entspricht,

haben die an der 29. Internationalen Konferenz teilnehmenden Beauftragten für den Datenschutz und für die Privatsphäre daher wie folgt beschlossen:

1. Sie erkennen an, dass die Nationen jeweils verschiedene Ansätze entwickelt haben, um personenbezogene Informationen zu schützen und private Rechte zu stärken,

2. Sie unterstützen Datenschutzbeauftragte dabei, ihre gegenwärtigen Bemühungen zur Förderung internationaler Zusammenarbeit fortzusetzen und mit internationalen Organisationen daran zu arbeiten, den Datenschutz weltweit zu stärken,

3. Sie begrüßen, dass der OECD-Rat die Empfehlungen über grenzüberschreitende Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen angenommen hat, und sie rufen die Regierungen der OECD-Mitgliedstaaten auf, die Empfehlungen zu implementieren,

4. Sie fördern die Beauftragten in ihrem Bestreben, ihre wertvolle Arbeit gemäß der Londoner Initiative fortzusetzen und dabei Instrumente, Rahmenbedingungen und Erfahrungen auszutauschen, um die Wirksamkeit und Effizienz unserer Aktivitäten und Eingriffe auf nationaler und internationaler Ebene auswerten zu können, und

5. Sie unterstützen die Beauftragten in ihren fortlaufenden Bemühungen um die Steigerung des Datenschutzbewusstseins und des Bewusstseins für den Schutz der Privatsphäre durch Initiativen wie z. B. die „Woche des Datenschutzbewusstseins“ (APPA) und den „Tag des Datenschutzes“ (Europarat).

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 41. Sitzung am 12./13. April 2007 in St. Peter Port (Guernsey)

Arbeitspapier zum grenzüberschreitenden Telemarketing

– Übersetzung –

Hintergrund

Gestützt auf frühere Arbeiten dieser Arbeitsgruppe haben zahlreiche Länder nunmehr legislative Maßnahmen ergriffen, die das Recht des Einzelnen respektieren, den Empfang unverlangter Telemarketing-Anrufe zu verhindern. Zu diesen Maßnahmen zählen die Telekommunikations-Richtlinien der Europäischen Union von 1997 und 2002, die in der Schaffung von Sperr-Registern in einigen Mitgliedstaaten der Europäischen Union mündeten, und in der Einrichtung der US-amerikanischen Sperrliste durch die Federal Trade Commission, während in anderen Rechtsordnungen auf der Einwilligung basierende Regelungen oder Mischungen aus Einwilligungs- und Widerspruchslösungen geschaffen wurden.

Diese Register und die damit verbundenen Durchsetzungsbefugnisse nationaler Behörden haben sich im Großen und Ganzen als recht effektiv zur Verhinderung des Empfangs unverlangter Telemarketing Nachrichten erwiesen, die aus dem selben Land oder Territorium herrühren, in dem sich der Angerufene befindet, waren jedoch weitgehend unwirksam hinsichtlich der Verhinderung von Anrufen aus dem Ausland.

Durch die fallenden Kosten internationaler Telefonanrufe und besonderes die Nutzung des Voice over Internet Protocol ist zu erwarten, dass die Häufigkeit grenzüberschreitender Telemarketing-Anrufe zunehmen wird.

Diese Situation wird verschärft durch die Tatsache, dass viele Werbeanrufe, insbesondere solche aus dem Ausland, häufig keinerlei Informationen über die Rufnummer des Anrufenden enthalten, die ihre Identifikation durch den Anrufer erlauben würden. Darüber hinaus scheint es, dass die Information zur Rufnummernanzeige nicht immer zwischen nationalen und internationalen Netzwerken übertragen wird.

Es scheint gegenwärtig keine Mechanismen zur Zusammenarbeit der Betreiber von nationalen Sperr-Registern zu geben, die eine datenschutzfreundliche Nut-

zung ihrer Datenbanken durch international operierende Telemarketing-Unternehmen ermöglichen würden.

Jedenfalls wird es sich ohne die Schaffung bindender internationaler Instrumente als sehr schwierig erweisen, das Recht durchzusetzen, keine unverlangten Werbeanrufe aus dem Ausland zu erhalten. Daher müssen alternative technische und organisatorische Maßnahmen erwogen werden.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

- Telemarketing-Unternehmen sollten sich über die anwendbaren Regelungen (Einwilligung und/oder Widerspruch) in den Ländern, in denen sie tätig sind, informieren und diese Regelungen respektieren.

- Telemarketing-Unternehmen sollten verpflichtet werden, ihre Rufnummern bei allen Werbeanrufen zu übertragen, so dass der Angerufene den Anrufer identifizieren und die Löschung von der Anrufliste des Werbetreibenden fordern kann, soweit dies vorgesehen ist, oder sich – zum Beispiel in Rechtsordnungen, die eine Einwilligung vorsehen – bei den zuständigen Behörden beschweren kann.

- Anbieter von Telekommunikationsdienstleistungen sollten zusammenarbeiten, um die Übermittlung der Rufnummer des Anrufenden im Bezug auf Werbeanrufe zwischen nationalen, internationalen und Voice over IP-Netzwerken zu gewährleisten.

- Anbieter von Telekommunikationsdienstleistungen sollten ihren Nutzern ein Verfahren anbieten, in dem diese sich über unverlangte Werbeanrufe beschweren können, und sicher stellen, dass solche Beschwerden an die zuständigen Behörden in dem Land weitergeleitet werden, aus dem der Anruf herrührt.

- Anbieter von Telekommunikationsdienstleistungen sollten den Nutzern eine einfache technische Möglichkeit eröffnen, die Zurückweisung eines ankommenden Werbeanrufs zu signalisieren und, soweit der Angerufene dies wünscht, sollte dieses Signal an den Anrufer übertragen und als Hinweis genutzt werden, dass weitere Anrufe bei diesem Nutzer zu unterbleiben haben.

Die Internationale Arbeitsgruppe ruft die Datenschutzbehörden weltweit auf, ihre Anstrengungen zur Zusammenarbeit untereinander und mit Aufsichtsbehörden im Bereich der Telekommunikation zu intensivieren, um die Aktivitäten von Organisationen, die über Landesgrenzen hinweg unverlangte Werbeanrufe durchführen, zu begrenzen.

2. 42. Sitzung am 4./5. September 2007 in Berlin

Arbeitspapier E-Ticketing in öffentlichen Verkehrsmitteln

– Übersetzung –

1. Die technologische Entwicklung im Bereich der Chipkarten und das Streben nach erhöhter Effizienz und Kosteneffektivität beim Management von Dienstleistungen im öffentlichen Verkehr – dies betrifft integrierte Eisenbahnen, U-Bahn und Flächentransportdienstleistungen – haben zu einer wachsenden Nutzung innovativer E-Ticketing Systeme geführt.

   Solche Systeme arbeiten mit elektronischen Karten, die gewöhnlich personalisiert sind und die vornehmlich für Transportdienstleistungen, aber zunehmend auch zur Bezahlung damit zusammenhängender anderer Leistungen genutzt werden können (z. B. für elektronische Bezahlung von Parkgebühren bei Pendlern)*.

2. Die Chipkarten enthalten einen Mikroprozessor, der Informationen einschließlich personenbezogener Daten speichert (dazu können z. B. die Chipidentifizierungsnummer, die Nummer des Abonnnements des Benutzers sowie die Zeit, das Datum und die Nummer des Gerätes zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gehören); in manchen Fällen arbeiten sie mit RFID/Near Field Communication (NFC)Technologie.

   Die Nutzung solcher Chipkarten beinhaltet daher die Verarbeitung von verschiedenen unmittelbar und/oder mittelbar zuordenbaren personenbezogenen Informationen:

   - Zu dem Zeitpunkt, zu dem die Karten an die Benutzer ausgegeben werden;

   - Jedes Mal, wenn die Karten benutzt werden, dank der Identifikationsnummern, die jedem Abonnenten zugeordnet sind und die durch Geräte zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gesammelt und dann möglicherweise in Echtzeit in den Datenbanken der Transportunternehmen gespeichert werden.

   In diesem Kontext müssen besonders die so genannten Validierungsdaten (Daten über die Entwertung oder Überprüfung der Gültigkeit) beachtet werden, deren Verarbeitung – insbesondere die Speicherung von Zeit und Ort der

* Andere Zahlungsformen sind z. B. Barzahlung, Zahlung über Mobiltelefon, etc.

Entwertung oder Überprüfung – es ermöglicht, die Bewegungen und Aufenthaltsorte einzelner Benutzer zu verfolgen.

3. Die Informationen, die öffentliche Transportunternehmen im Rahmen der Erbringung ihrer Dienstleistungen verarbeiteten, einschließlich der Informationen, die zum Zeitpunkt der Entwertung oder Überprüfung der Karte gespeichert werden, können für verschiede Zwecke genutzt werden, wie z. B.:

   - die Bereitstellung von Transportdienstleistungen,
   - die Bekämpfung von Betrug beim E-Ticketing (wenn Chipkarten verloren, gestohlen oder ohne Autorisierung kopiert werden),
   - Werbung,
   - die Aufteilung der Einnahmen unter verschiedenen Beteiligten, wenn öffentliche Transportdienstleistungen gemeinsam durch mehrere Transportunternehmen erbracht werden,
   - die Analyse aggregierter Daten über Verkehrsflüsse, um die Effizienz der erbrachten Dienstleistungen zu steigern.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

Vorabkontrolle (Privacy Impact Assessment)

Das Recht der Kunden auf den Schutz ihrer personenbezogener Daten muss bereits beim Entwurf und im Rahmen der Entwicklung von Informationssystemen der Transportunternehmen berücksichtigt werden; grundsätzlich sollten das Recht auf persönliche Freizügigkeit und die Anforderungen effizienten öffentlichen Verkehrs miteinander in Einklang gebracht werden.

Anonymität

Verkehrsbetriebe und Transportunternehmen sollten ihren Kunden alternativ Möglichkeiten zur anonymen Nutzung (ohne unbillige Hindernisse) anbieten, z. B. Barzahlung oder anonyme E-Tickets.

Wo Anonymität aus technischen Gründen nicht angeboten werden kann, müssen die folgenden Empfehlungen beachtet werden:

Datenschutzinformation und Transparenz

Verkehrs- oder Transportunternehmen, die E-Ticketing-Systeme nutzen, sollten die Betroffenen unmissverständlich über die Verarbeitung ihrer personenbezogenen Daten informieren. Die Betroffenen sollten in der Lage sein, die spezifischen Zwecke leicht zu verstehen, die von den Unternehmen verfolgt werden, welche Arten von personenbezogenen Daten über sie gesammelt und gespeichert werden, und wie diese Informationen genutzt werden.

Datensparsamkeit und Speicherungsdauer

Insbesondere in Bezug auf die Verarbeitung der Reisedaten der Nutzer sollten die Informationssysteme von Transportunternehmen so geplant und entwickelt werden, dass sie die Nutzung anonymer Daten priorisieren. Wenn (direkt oder indirekt) personenbezogene Daten genutzt werden, sollten diese Informationen für die kürzestmögliche Zeitdauer gespeichert (und danach gelöscht) und die gesetzliche Zweckbestimmung der Verarbeitung beachtet werden – grundsätzlich sollten die betreffenden Informationen nicht länger als ein paar Tage nach ihrer Erhebung gespeichert bleiben.

Sicherheit

Die Sicherheitsmaßnahmen beim Zugriff auf personenbezogene Daten sollten ein Überwachungssystem zur Verhinderung des Missbrauchs von Informationen umfassen. Verkehrsunternehmen sollten sicherstellen, dass der Schutz der Privatsphäre registrierter Nutzer garantiert wird, wenn sie ihren Partnern und ihren eigenen Mitarbeitern den Zugriff auf ihre Datenbanken eröffnen.

Werbung

Ein Verkehrs- oder Transportunternehmen sollte die freiwillige und informierte, vorherige Einwilligung seiner Kunden für die Nutzung personenbezogener Daten für eigene Werbezwecke oder die Nutzung durch verbundene Partnerunternehmen für unverlangte Werbung gegenüber dem Reisenden einholen. Diese Einwilligung sollte sich von der Zustimmung zu allgemeinen Geschäftsbedingungen unterscheiden.

Zahlungsnachweis

Soweit z. B. zur Kostenerstattung oder aus steuerlichen Gründen ein Zahlungsnachweis über einzelne Reisen erforderlich ist, sollten dafür datenschutzfreundliche Lösungen angeboten werden.

Verhaltensregeln

Die Entwicklung von Verhaltensregeln zum Datenschutz sollte gefördert werden. Insbesondere im Hinblick auf die Verarbeitung von Bewegungsdaten der Nutzer sollten Informationssysteme von Transportunternehmen unter Priorisierung der Nutzung von anonymen Daten geplant und entwickelt werden.

Systemdesign

Die Systementwicklung sollte so erfolgen, dass personenbezogene Daten von Reisedaten getrennt werden (2-Komponenten-Modell). Eine zentrale Speicherung sollte auf aggregierte und/oder anonyme Transaktionen beschränkt werden. Karteninhaber sollten Daten über die Nutzung ihrer Karten kontrollieren können.

Arbeitspapier

Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen

– Übersetzung –

Entwicklungszusammenhang

Das Fernsehen hat im letzten Jahrzehnt fundamentale Veränderungen erfahren.

Die erste Entwicklung – der Übergang vom **analogen** zum **digitalen Fernsehen** – war überwiegend eine Umrüstung von analoger zu digitaler Erfassung, Aufnahme, Übertragung und Wiedergabe. Sie bewirkte besseren Ton, bessere Bilder, mehr Kanäle und mehr Auswahl, veränderte aber nicht fundamental Form und Funktion der klassischen Ausstrahlung von Fernsehen.

Die zweite Entwicklung – die Auslieferung von Fernsehen und anderen Audio- und Videodiensten als digitale Signale **über Breitbanddatennetzwerke** – verändert die Bedingungen der Medienproduktion, -verteilung und -inanspruchnahme in signifikanter Weise. Sie beinhaltet die Konvergenz der Kommunikations-, Computer- und Massenmediensektoren in einem einzigen, interaktiven Netzwerk – **Konvergenz der Netzwerke** – und die Einführung einer zunehmenden Anzahl von statischen oder mobilen Endgeräten, die in der Lage sind, gleichmäßig mit diesen drei Sektoren zu interagieren – **Divergenz der Endgeräte**. Sie beinhaltet

auch die Einführung neuer Navigationsparadigmen, die durch neue Werkzeuge und Dienste, wie Video-Suchmaschinen, peer-to-peer-Verteilung usw. den Zugriff auf eine explosiv wachsende Anzahl von Bildmedien gestattet – **Divergenz der Inhalte**. Schließlich ermöglicht sie potenziell die Erhebung und Verarbeitung personenbezogener Daten aus verschiedenen Quellen, z. B. bei Multiple-Play-Diensten.

Zu den wichtigen Folgen dieser zweiten Evolution zählen die Einführung neuer Wege zur Verteilung digitaler Medieninhalte, wie digitales interaktives Fernsehen, IPTV, web-basiertes Fernsehen etc. und die Ersetzung traditioneller set-top-Boxen im Kabelfernsehen durch interaktive, intelligente Geräte. In diesen Systemen können Nutzer einen bestimmten Strom von Videosignalen oder einen Fernsehkanal „on demand" herunterladen, und sie können nicht nur mit dem Inhalt des TV-Programms direkt interagieren, sondern auch mit jeglichem anderen TV-bezogenen Inhalten.

Während das digitale interaktive Fernsehen einen neuen, personalisierten Ansatz beim Fernsehen darstellt – jedermann zu beliebigen Zeitpunkten an beliebigen Orten und auf beliebigen Endgeräten alle möglichen Inhalte zur Verfügung zu stellen – und neue Dienste wie „T-Commerce[1]", Video-on-demand, Home-Banking und Fernstudium ermöglicht, führt es auch zu neuen Gefährdungen, insbesondere im Hinblick auf den Schutz der Privatsphäre der Nutzer.

Die neuen interaktiven, digitalen Fernsehsysteme nutzen in den meisten Fällen eine versiegelte „Black-Box", die von den Anbietern kontrolliert werden und dem Nutzer wenig oder überhaupt keine Kontrolle ermöglichen. Es handelt sich um geschlossene Systeme und es ist selbst für fortgeschrittene Nutzer schwierig, wenn nicht unmöglich, herauszufinden, was diese Systeme tun.

Eine der wichtigsten Gefahren, die durch diese neuen Arten der Verteilung digitaler Medieninhalte entstehen, ist die Möglichkeit, die emotionale Kraft des Fernsehens (Menschen, die sich zuhause entspannen, neigen eher zu offenen unbefangenen Reaktionen mit der Transaktions-orientierten Macht des Internet (Data Mining, Nutzer-Modellierung, intelligente Agenten etc.) zu kombinieren, um hinreichend individualisierte, personalisierte Informationen über jeden Nutzer zu sammeln, um seine Seherfahrungen umgehend daran anzupassen und sogar sein Verhalten zu verändern.

Wenn der Fernsehdienst von einem Internetserviceprovider im Rahmen eines Triple- oder Quadruple-Play-Dienstes angeboten wird, wird das Fernsehprogramm entweder auf einem Fernsehgerät oder einem Personalcomputer ange-

[1] Fernseh-basierter Geschäftsverkehr

zeigt. In beiden Fällen kann der Kanal „on demand“ abgerufen werden (wenn der Nutzer einen Kanal wählt) und der Anbieter kann daher präzise bestimmen, welcher Nutzer ein Programm zu einem bestimmten Zeitpunkt ansieht. Im Falle des Web-TV, bei dem die Inhalte über eine Website angeboten werden, wird der Videodatenstrom ebenfalls „on demand“ heruntergeladen; personenbezogene Daten können teilweise wohl durch den Betreiber der Website als auch durch den Internetserviceprovider erhoben und gespeichert werden, der dem Nutzer den Internet-Zugang anbietet[2]. Schließlich erlauben einige Systeme einzelnen Nutzern sogar das Heraufladen eigener Inhalte auf eine Video-on-demand-Plattform (wo andere Nutzer auf sie zugreifen können), oder Nutzer können auch ihre eigenen Bilddaten live in einem speziellen Video-on-demand-Fernsehkanal senden.

Empfehlungen und Bekräftigung fundamentaler Prinzipien

Die Arbeitsgruppe ist insbesondere unter Berücksichtigung der Bedeutung der neuen Möglichkeiten digitalen Medienkonsums in jedermanns täglichen Leben und dessen führender Bedeutung für die Gesellschaft, die Demokratie, die Bildung und Kultur als ein kultureller Dienst, der den freien Zugang zu Informationen garantiert sowie Meinungsvielfalt und Medienpluralismus, und in Erwägung, dass andererseits riesige Mengen sehr sensibler Informationen durch die Registrierung von Nutzungsgewohnheiten gesammelt werden können, der Auffassung, dass:

1. Die Möglichkeit zur anonymen Nutzung des digitalen Fernsehens erhalten bleiben muss. Anonyme Zahlungsmethoden (z. B. durch vorausbezahlte Karten) sollten wenigstens als eine Möglichkeit und ohne zusätzliche Kosten angeboten werden. Informationssysteme (Geräte, Programme und deren Organisation), die für die Verbreitung digitalen Fernsehens genutzt werden, müssen so entworfen, entwickelt und konfiguriert werden, dass sie Anonymität oder Minimierung der Nutzung personenbezogener Daten befördern und sicherstellen. Zu diesem Zweck sollte eine Vorabkontrolle durchgeführt werden.

2. Wenn personenbezogene Daten gespeichert werden, so darf dies nur für legitime Zwecke geschehen und der Umfang der Daten und die Mechanismen, die zu ihrer Verarbeitung implementiert werden, müssen relevant und nicht unverhältnismäßig im Hinblick auf die zu erreichenden Zwecke sein. Die Eröffnung

[2] Darüber hinaus können personenbezogene Daten von der Inhalte-Industrie mittels eines „broadcast flag“ erhoben und gespeichert werden, wie man es in den Vereinigten Staaten von Amerika einzuführen versucht hat, und das möglicherweise auch in anderen Ländern erwogen wird. In diesem System sind maschinenlesbare Daten in das Fernsehsignal eingebettet, um die Weiterverbreitung von Inhalten zu verhindern, die urheberrechtlichen Beschränkungen unterliegen. Datenschutzbedenken können entstehen, wenn Technologien zum digitalen Rechte-Management die Nutzung von Inhalten überwachten und mögliche Urheberrechtsverstöße eines Einzelnen an den Inhalteanbieter zurückmelden (vgl. auch den Gemeinsamen Standpunkt der Arbeitsgruppe zu Datenschutz- und Urheberrechts-Management, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000 in Rethymnon/Kreta; http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_en.htm).

von Wahlmöglichkeiten für den Einzelnen im Hinblick auf Inhalte sollte nicht unvermeidbar mit ihrer Identifizierung einhergehen.

3. Anbieter digitalen Fernsehens sollten die Zuschauer im Vorhinein über die genauen Zwecke der Speicherung und Verarbeitung personenbezogener Daten informieren, sowie über die Arten der gespeicherten Daten, den Ort und die Dauer der Speicherung.

4. Die Verarbeitung von Nutzerprofilen sollte die vorherige, informierte Einwilligung der Betroffenen voraussetzen („opt in“). Insbesondere sollte die Übermittlung von Zuschauerdaten oder -profilen durch Anbieter digitalen Fernsehens an Dritte (z. B. zu Werbezwecken) nur mit der freiwilligen und informierten Einwilligung der Betroffenen erfolgen. Diese Einwilligung sollte sich von der Zustimmung zu allgemeinen Geschäftsbedingungen des digitalen Fernsehdienstes unterscheiden. Die Zuschauer sollten das Recht haben, ihre Einwilligung jederzeit mit Wirkung für die Zukunft zurückzuziehen.

5. Zuschauer sollten – vorzugsweise kostenfrei – das Recht auf Auskunft, Überprüfung und – wo notwendig – Berichtigung aller ihrer personenbezogenen Daten haben, einschließlich ihrer bei Anbietern von digitalem Fernsehen gespeicherten Profile.

6. Gespeicherte personenbezogene Daten müssen durch angemessene Sicherheitsmaßnahmen geschützt werden.

7. Die Überprüfung der Einhaltung von Datenschutzbestimmungen durch unabhängige Einrichtungen ist unerlässlich.

B. Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Entschließung der 14. Konferenz am 11. Juni 2007 in Kiel

Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken!

Die Wahrung von Betriebs- und Geschäftsgeheimnissen hat für Unternehmen eine besondere Bedeutung. Betriebs- und Geschäftsgeheimnisse können den Wert eines Unternehmens und seine Stellung am Markt erheblich beeinflussen. Bei ihrer Aufgabenerfüllung erhalten öffentliche Stellen bisweilen Kenntnis von Betriebs- und Geschäftsgeheimnissen. Als Bestandteil amtlicher Aufzeichnungen unterliegen die Betriebs- und Geschäftsgeheimnisse den Informationsfreiheitsgesetzen, sie werden hier aber durch einen Ausnahmetatbestand geschützt.

Die Konferenz der Informationsfreiheitsbeauftragten stellt fest, dass die Auslegung und Anwendung des Ausnahmetatbestandes das Informationsfreiheitsrecht der Bürgerinnen und Bürger übermäßig einschränkt. So führt oft die beträchtliche Rechtsunsicherheit der Behörden bei der Anwendung dieser Bestimmung zu einer besonders restriktiven Auskunftspraxis. Aber nicht jedes Unternehmensdatum ist ein Betriebs- oder Geschäftsgeheimnis. Nach der Rechtsprechung des Bundesgerichtshofes zum Wettbewerbsrecht müssen hierfür folgende Voraussetzungen kumulativ vorliegen:

Es muss sich um Tatsachen handeln, die

- im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehen,
- nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig sind,
- (subjektiv) nach dem erkennbaren Willen des Unternehmens und
- (objektiv) nach dessen berechtigten und schutzwürdigen wirtschaftlichen Interessen geheim gehalten werden sollen (insbesondere, wenn bei Offenbarung ein Schaden eintritt).

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb den Bundes- und die Landesgesetzgeber auf, die gesetzlichen Regeln zu ergänzen und zu präzisieren.

1. Es gibt Betriebs- oder Geschäftsgeheimnisse, bei denen das öffentliche Interesse an der Offenbarung den Schutzbedarf überwiegt. Soweit daher eine Abwägungsklausel in den gesetzlichen Grundlagen noch nicht vorhanden ist, soll sie aufgenommen werden. Dabei muss auch verdeutlicht werden, dass Verträge, die mit der öffentlichen Hand geschlossen werden, nicht grundsätzlich geheimhaltungsbedürftig sind: Wer mit dem Staat Geschäftsbeziehungen eingeht, muss sich darüber im Klaren sein, dass staatliches Handeln besonderen Kontrollrechten unterliegt und damit nicht alle Vertragsinhalte geheim bleiben können.

2. Nach dem Beispiel des Gentechnik- und Chemikalienrechts sollte in Form eines Kataloges klargestellt werden, welche Unternehmensinformationen keine Betriebs- oder Geschäftsgeheimnisse darstellen (z. B. rechtswidriges Verhalten).

3. Kennzeichnungs- und Darlegungspflichten des Unternehmens können die Prüfung des Geheimhaltungsinteresses erleichtern. Vergleichbare Regelungen existieren bereits in anderen Bereichen.