Peter Schaar
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Bundesrepublik Deutschland

Rede am 30. Januar 2009 anlässlich des
Europäischen Datenschutztags in Wien

- Es gilt das gesprochene Wort -

Aktuelle Entwicklungen im europäischen und internationalem Datenschutz unter besonderer Berücksichtigung des transatlantischen Dialogs

Sehr geehrter Herr Staatssekretär Dr. Ostermayer,
sehr geehrter Herr Vorsitzender des Datenschutzrats Dr. Wögerbauer,
sehr verehrte Damen, sehr geehrte Herren,

es ist mir eine große Ehre, heute anlässlich des Europäischen Datenschutztages zu Ihnen sprechen zu dürfen.

Das Jahr 2008 hat für die Entwicklung des Datenschutzes auf europäischer wie auf internationaler Ebene einige wichtige Impulse gegeben. Trotz des irischen Neins zum Lissabonvertrag und trotz aller Datenschutzskandale können wir uns gleichwohl über bedeutende Neuerungen und Fortschritte freuen. Ich denke hier etwa an wegweisende Entscheidungen des Europäischen Gerichtshofs (EuGH) und des Europäischen Gerichtshofs für Menscherechte (EGMR) im vergangenen Jahr und an den Rahmenbeschluss zum Datenschutz in der so genannten „Dritten Säule“, also in Bezug auf Daten, die im Rahmen der polizeilichen oder justiziellen Zusammenarbeit verarbeitet werden. Aber auch der Bericht der High Level Contact Group (HLCG), die Diskussionen um die Änderung der EU-Telekommunikationsrichtlinien und die Arbeit der Art. 29 WP zu Binding Corporate Rules (BCRs) haben wichtige Anstöße gegeben, die wir in diesem Jahr hoffentlich aufgreifen und weiterentwickeln werden.

Die vielen Datenschutzskandale überall auf der Welt, so sehr sie auch zu bedauern sind, haben uns erneut die Bedeutung des Datenschutzes für den Einzelnen und für unsere Gesellschaft vor Augen geführt und eine fruchtbare Debatte über die Weiterentwicklung des Datenschutzrechts einschließlich der EU-Datenschutzrichtlinie angeregt.

So begrüße ich die von der britischen Datenschutzbehörde in Auftrag gegebene Studie zum Stand der Umsetzung der Europäischen Datenschutzrichtlinie und zur Frage, in wie weit eine Anpassung dieses Instruments an neue Gegebenheiten notwendig erscheint. Ein Papier mit einer ähnlichen Zielrichtung hat zwischenzeitlich auch die EU-Kommission in Auftrag gegeben.

Es ist unbestreitbar, dass die Welt auch aus datenschutzrechtlicher Sicht anders aussieht als 1995. Die enormen technischen Entwicklungen, der stetig wachsende Hunger des Staates und der Wirtschaft auf Informationen einschließlich personenbezogener Daten, die nach den Anschlägen des 11. September 2001 einsetzende Diskussion über eine Stärkung der Strafverfolgungsbehörden und die damit einhergehende Flut von Sicherheitsgesetzen waren vor 15 Jahren nicht absehbar und haben maßgeblich zu einer Einschränkung des Rechts auf informationelle Selbstbestimmung beigetragen. Die in diesem Jahr anstehenden Erörterungen zu einer Revision der Richtlinie werden daher sicherlich spannend und sollten mutig und offen angegangen werden.

Von der gegenwärtigen Diskussion über die Revision der EU-Telekommunikationsrichtlinien erhoffe ich mir eine Stärkung des Datenschutzes, insbesondere durch die neue Informationspflicht der Unternehmen bei Datenschutzverstößen in der Richtlinie zum Datenschutz in Kommunikationsdiensten, der so genannten ePrivacy-RL. Über das ob einer solchen Informationspflicht scheint es kaum mehr Kontroversen zu geben, offen ist hingegen noch die Frage, wie diese Regelung ausgestaltet wird. Sowohl der Rat als auch die Kommission wollen die Informationspflicht nur bei schweren Fällen des Datenmissbrauchs vorsehen, während wir Datenschützer für eine weitere Verpflichtung eintreten. Wenn die Betroffenen und auch die Öffentlichkeit davon erfahren, dass mit ihren Daten nicht ordentlich umgegangen wurde, wird dies zu einem Bewusstseinswandel bei den Unternehmen beitragen. Mehr Transparenz für die Kunden liegt letztlich auch im Interesse der Unternehmen, die sorgsam mit personenbezogenen Daten umgehen und nicht in Generalhaftung genommen werden, wenn bei einem Unternehmen etwas schief geht.

Bei der ePrivacy-RL ist noch strittig, in wie weit Verkehrsdaten für Datensicherheitszwecke verarbeitet werden dürfen. Die Position des Rates ist sehr weitgehend formuliert, während wir Datenschützer dafür eintreten, die Verarbeitung solcher Daten allenfalls zu bestimmten, eng begrenzten Zwecken zu erlauben, etwa zur Beseitigung von Störungen. Hier wird noch einige Überzeugungsarbeit zu leisten sein, um zu einem Ergebnis zu gelangen, das den Anspruch der Nutzerinnen und Nutzer auf unbeobachtete Kommunikation respektiert und zugleich den Anforderungen an IT-Sicherheit Rechnung trägt. Ich hoffe, dass wir sowohl den Rat als auch das Europäisches Parlament davon überzeugen können, von einer Pauschalermächtigung zur Datenverarbeitung abzusehen.

Der Datenschutz kann sich heute weniger denn je darauf beschränken, nachträglich zu kontrollieren, ob die Datenschutzbestimmungen eingehalten

wurden. Aus diesem Grund sind Ansätze bedeutsam, die es den verantwortlichen Stellen in Staat und Wirtschaft ermöglichen, sich einen guten Datenschutzstandard nach unabhängiger Begutachtung bescheinigen zu lassen. So hat die deutsche Bundesregierung einen Gesetzentwurf zur Einführung eines Datenschutzaudits auf freiwilliger Grundlage auf den Weg gebracht. Auch die Arbeiten zur Einführung eines europäischen Datenschutzgütesiegels „EuroPriSe“ sind nachdrücklich zu begrüßen. Hier soll auf europäischer Ebene eingeführt werden, was sich auf lokaler Ebene schon längst bewährt hat. Ein solches Gütesiegel wird zu einer Standardisierung im Datenschutz führen und IT-Verfahren transparenter machen. Die Verbraucherinnen und Verbraucher sollen in die Lage versetzt werden, Produkte zu vergleichen und sich für das datenschutzfreundlichere entscheiden können.

Eine Stärkung des Datenschutzes ging von zwei wegweisenden Urteilen des EGMR und des EuGH im vergangenen Jahr aus. Zum einen hat der EGMR in dem Urteil S. und Marper/Vereinigtes Königsreich festgestellt, dass eine unbeschränkte und unbefristete Speicherung von Fingerabdrücken und DNA-Material nicht mit Art. 8 der Europäischen Menschrechtscharta vereinbar ist. Er hat damit noch einmal die Datenschutzprinzipien der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung unterstrichen. Zum anderen hat der EuGH in seinem Urteil zum deutschen Ausländerzentralregister entschieden, dass die dort praktizierte generelle Speicherung von personenbezogenen Daten nicht dem Erforderlichkeitsgebot entspricht und gegen das Diskriminierungsverbot verstößt. Ausgangspunkt war dabei übrigens die Klage eines österreichischen Staatsbürgers, der nicht damit einverstanden war, dass seine Daten im Ausländerzentralregister gespeichert wurden.

In diesem Jahr stehen voraussichtlich noch zwei weitere Entscheidungen an, von denen ich mir eine Stärkung des Datenschutzes erwarte. So wird sich der EuGH zur Vereinbarkeit der Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten (2006/24/EG) mit dem Gemeinschaftsrecht äußern sowie ein Urteil zur Unabhängigkeit der Datenschutzaufsichtsbehörden fällen, nachdem die Kommission gegen die Bundesrepublik Deutschland Klage erhoben hat. Diese Entscheidung zur „völligen Unabhängigkeit“ dürfte für eine Klärung des Art. 28 I 2 der Richtlinie 95/46/EG sorgen und auch Auswirkungen auf andere Staaten haben. Interessant wird dabei auch sein, ob und wie der EuGH die Vorgabe der Richtlinie interpretiert, dass den Datenschutzaufsichtsbehörden wirksame Eingriffsbefugnisse zur Verfügung stehen müssen.

Einen gewissen Fortschritt hat es auch bei der Diskussion um eine Beschleunigung der Genehmigungsverfahren von Binding Corporate Rules (BCRs) gegeben. Dabei geht es in erster Linie darum, dass Entscheidungen der Datenschutzaufsichtsbehörden über die Angemessenheit von unternehmens- und

konzernweiten Datenschutzregeln in der Gemeinschaft nicht nur auf nationaler Ebene, also im Extremfall in jedem der 27 Mitgliedstaaten, getroffen werden. Hier hat die Art. 29 WP gezeigt, dass sie sich der zum Teil berechtigten Kritik aus Wirtschaftskreisen an den langwierigen und komplizierten Antragsverfahren stellt. Sicherlich bleibt noch viel zu tun und insbesondere kann der Dialog mit den Unternehmen noch intensiviert werden. Hervorzuheben ist aber ganz besonders, dass schon jetzt eine Reihe von Mitgliedstaaten bereit sind, sich an dem gegenseitigen Anerkennungsverfahren zu beteiligen. Die rasch wachsende Zahl der Länder, die an der gegenseitigen Anerkennung teilnehmen, zeigt, dass eine Zusammenarbeit auch ohne rechtliche Verpflichtungen möglich und von gegenseitigem Nutzen ist. Allerdings habe ich den Eindruck, dass wir bei dieser Frage letztlich nicht um eine Anpassung des europäischen Rechtsrahmens herumkommen.

Den von der EU-Kommission im November 2007 vorgelegte Vorschlag für ein europäisches PNR-System im Rahmen eines europäischen Grenzkontrollmanagements sehe ich sehr kritisch. Er ist übrigens nicht nur bei den Datenschutzbeauftragten, sondern auch beim Europäischen Parlament und bei den Fluggesellschaften auf erheblichen Widerstand gestoßen. Die Diskussionen im Rat haben hier bis jetzt - man könnte fast sagen: zum Glück - zu keinem greifbaren Ergebnis geführt. Dieser Vorschlag würde im Falle seiner Umsetzung zu einer gigantischen Datensammlung führen und sämtliche, die EU-Grenzen mit dem Flugzeug überquerenden Personen in einer Sicherheitsdatei speichern, ohne dass hierfür ein konkreter Anlass bestünde. Europa sollte hier nicht dem schlechten Beispiel folgen, dass auf diesem Gebiet andere Staaten gegeben haben - ich verweise hier insbesondere auf das mit den USA geschlossene Abkommen zur Übermittlung von Passagierdaten. Diese neue Art der Vorratsdatenspeicherung würde auch in das in der EU-Grundrechte-Charta garantierte Grundrecht auf Datenschutz eingreifen. Ich halte die Initiative der Kommission, ein solches System in Europa einzuführen, auch deshalb für verfehlt, weil bisher nicht einmal die bestehenden Rechtsinstrumente wie die API-Richtlinie (2004/82/EG) vollständig umgesetzt wurden. Auch dabei geht es um Flugpassagierdaten, die allerdings mit einer klaren Zweckbestimmung erhoben werden und die nicht längerfristig aufbewahrt werden sollen. Die Datenschutzbehörden der europäischen Mitgliedstaaten sehen deshalb keinen Bedarf an weiteren Passagierdaten, die über die API-Daten hinausgehen. Ein solches EU-PNR System soll nach Plänen der Kommission zudem noch ergänzt werden durch eine Reihe anderer Instrumente, wie etwa ein Entry-exit System oder EU-ESTA. Bei allen diesen Initiativen geht es darum, Reisende immer lückenloser und umfassender zu registrieren, die dabei anfallenden Daten längere Zeit aufzubewahren und zu verknüpfen, ohne dass der einzelne hierfür irgend einen Anlass geboten hätte. Besorgnis erregend ist in diesem Zusammenhang vor allem, dass manchen Verantwortlichen offensichtlich jedes rechte Maß abhanden gekommen zu sein

scheint. Niemand, auch nicht wir Datenschützer - hat etwas dagegen, dass im Einzelfall, bei Tatverdacht oder Hinweisen auf konkrete Gefahren gezielt personenbezogene Daten erhoben und verarbeitet werden. Nicht hinzunehmen ist es hingegen, wenn pauschal ganze Personengruppen umfassend registriert und letztlich unter Generalverdacht gestellt werden.

Wenn man bedenkt, dass diese Daten mit anderen Datenbanken - bereits existierenden oder im Aufbau befindlichen Systemen (VIS, SIS II) verknüpft werden könnten, bestärkt dies unsere Kritik. Es ist ein grundlegender Irrtum, dass ein Mehr an Daten automatisch ein Mehr an Sicherheit bedeutet. Bisweilen ist sogar das Gegenteil wahr. Zusätzliche Datenmengen führen zu zusätzlichen Begehrlichkeiten und bringen zusätzliche Risiken für den Missbrauch mit sich. Statt immer mehr personenbezogene Daten anzuhäufen, sollten die Verantwortlichen mehr Mühe darauf verwenden, die Qualität der bestehenden Datensammlungen zu verbessern und intelligente - und das heißt auch datenschutzfreundliche - Wege zu ihrer sinnvollen Auswertung zu suchen.

Ein allerdings nur bescheidener Meilenstein bei der Entwicklung des Datenschutzes war die Verabschiedung des Rahmenbeschlusses für den Datenschutz in der so genannten „Dritten Säule“ der EU am 27. November 2008.
Nach langjährigen Debatten ist damit endlich ein Ergebnis erzielt worden, das allerdings nicht viel mehr ist als ein erster Schritt in die richtige Richtung. Der Rahmenbeschluss stellt nicht - anders als von uns Datenschützern erhofft - den erforderlichen hohen und gleichwertigen Datenschutz bei der Verarbeitung von Daten durch die Polizei- und Justizbehörden sicher. Insbesondere lässt er die Datenverarbeitung dieser Behörden auf nationaler Ebene unberührt. Insofern unterscheidet er sich fundamental von der EG-Datenschutzrichtlinie von 1995, die ausdrücklich die inländische Datenverarbeitung einbezieht. Unterschiedliche Datenschutzstandards in der EU - wie passt das mit dem Grundrecht auf informationelle Freiheit zusammen? Zudem unterscheidet das Instrument nicht zwischen verschiedenen Datenkategorien etwa bei Daten von Zeugen, Verdächtigen oder Opfern.
Als weiterer gravierender Mangel ist anzusehen, dass der Rahmenbeschluss keine Regelungen für ein unabhängiges Gremium der Datenschutzbeauftragten aus den Mitgliedstaaten vergleichbar mit der Art. 29 WP enthält, welches die Kommission, den Rat und das Europäische Parlament in datenschutzrechtlichen Fragen berät. Ein entsprechender Vorschlag der Kommission und des Europäischen Parlaments wurde vom Rat leider nicht übernommen. Es ist bedauerlich, dass EU-Rechtsakte zur polizeilichen und justiziellen Zusammenarbeit in Strafsachen damit auch künftig ohne Beteiligung von Datenschutzgremien auf EU-Ebene verabschiedet werden können. Das Inkrafttreten des Vertrags von Lissabon könnte allerdings den Weg dazu ebnen, auch beim Schutz personenbezogener Daten, die von Sicherheitsbehörden

verarbeitet werden, weiter voran zu kommen. Eine Überarbeitung des Rechtsrahmens in diesem Bereich ist auch deshalb notwendig, da die Polizei- und Strafverfolgungsbehörden in Zukunft noch enger miteinander kooperieren werden, wie dies die Future Group in ihrem Bericht vom Juni 2008[1] skizziert hat. Ein intensivierter Informationsaustausch zwischen den Mitgliedstaaten und ggfs. mit Drittstaaten darf nur einhergehen mit umfassenden Garantien für den Schutz der Daten und der Rechte der Betroffenen.

Auch hinsichtlich des transatlantischen Dialogs zum Datenschutz hat es einige Fortschritte gegeben. Allerdings gibt es hier neben viel Licht auch viel Schatten. Uneingeschränkt positiv bewerte ich, dass die Kontakte zwischen den verschiedenen Ansprechpartnern intensiver geworden sind. Sie haben dazu beigetragen, die unterschiedlichen Auffassungen der anderen Seite besser zu verstehen. Das gilt sowohl für die Politiker als auch die Datenschützer.

Weniger positiv ist hingegen, dass es unter der letzten US-Administration noch keine personellen Entscheidungen bei der Besetzung des Civil Liberties and Privacy Oversight Board (CLPOB) gegeben hat. Auch in anderen Fragen war die Stärkung des Datenschutzes nicht gerade ein Schwerpunkt der amerikanischen Politik. Zwar konnte auf verschiedenen Feldern - meist nachträglich - die eine oder andere datenschutzrechtliche Sicherung eingebaut werden, gleichwohl haben in der Summe die Eingriffe in das Recht auf informationelle Selbstbestimmung im transatlantischen Verhältnis überwogen. Dies gilt nicht nur für die Übermittlung der Daten von Flugpassagieren, sondern auch bei anderen sicherheitsempfindlichen Vorhaben. Ich hoffe, dass die Obama-Administration hier einen Richtungswechsel vollzieht. So könnte das Civil Liberties and Privacy Oversight Board vielleicht der Nukleus einer unabhängigen US-Datenschutzaufsichtsbehörde werden und Ansprechpartner für alle datenschutzrechtlichen Fragen sein.

Die Arbeit der EU-US High Level Contact Group zu gemeinsamen Datenschutzgrundsätzen ist allgemein zu würdigen. Kritisch sehe ich allerdings, dass die unabhängigen Datenschutzinstitutionen nicht in diese transatlantischen Diskussionen einbezogen worden sind, also weder die Art. 29 WP noch der EDPS. Gleichwohl enthalten die Diskussionsergebnisse, zusammen gefasst im Abschlußbericht[2] der Gruppe, wichtige Grundlagen für weitere Gesprächsrunden. Auch soll in Zukunft das Europäische Parlament eingebunden werden. Sowohl der amerikanischen als auch der europäischen Seite geht es dabei um die Schaffung eines Rechtsrahmens für den Austausch von Daten für Strafverfolgungszwecke. Ich möchte bei dieser Gelegenheit betonen, dass es keine pauschale Ermächtigung zur Datenübermittlung geben darf, wenn nicht

[1] Freedom, Security, Privacy – European Home Affairs in an open world. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group") vom Juni 2008
[2] Abschlußbericht der EU-US High Level Contact Group vom Juni 2008

auf der anderen Seite ein angemessener Schutz der personenbezogenen Informationen sichergestellt ist.

Im privaten Sektor kommt dem Safe Harbor Abkommen wachsende Bedeutung zu. Im Grunde geht es darum, den europäischen Datenschutzstandard, wie er in der EG-Datenschutzrichtlinie festgeschrieben ist, auch im transatlantischen Datenverkehr zu gewährleisten. Dabei ist es von entscheidender Bedeutung, die Abmachungen mit Leben zu erfüllen und eine beiderseits des Atlantik harmonisierte Interpretation der Regelungen zu gewährleisten. Einen wichtigen Beitrag für dieses gemeinsame Verständnis haben regelmäßige Seminare geleistet, die auf Anregung der Art. 29-Gruppe seit einigen Jahren stattfinden. Das vierte derartige Seminar, das im vergangenen Oktober in Brüssel stattfand, hat erneut gezeigt, wie wichtig eine regelmäßige Evaluierung der Vereinbarung ist. Sowohl die von der EU-Kommission in Auftrag gegebene zweite Studie[3] zur Umsetzung des Safe Harbors als auch die Studie von Chris Connolly, Galexia[4] belegen eindrucksvoll, dass ein Abkommen kein Selbstläufer ist, sondern von beiden Seiten mit Leben erfüllt und tatkräftig umgesetzt werden muss. Nur wenn die jetzt aufgezeigten Schwächen, wie etwa mangelnde Unterrichtung der Verbraucher oder ein fehlerhaftes Datenschutzkonzept bei den Unternehmen, von beiden Vertragsparteien angegangen werden, kann das Abkommen seinen Zweck erfüllen, ein angemessenes Datenschutzniveau für in die USA übermittelte Daten sicher zu stellen. Dabei richtet sich die Kritik nicht alleine an die US-Stellen, sondern auch an die europäischen Aufsichtsbehörden, die ihren Aufgaben nur gerecht werden können, wenn sie die Firmen und Betroffenen besser über das Abkommen unterrichten, über vorhandene Rechtsmittel aufklären und Verstöße aktiv ahnden.

Eine Evaluierung hätte ich mir auch für das im Juli 2007 geschlossene EU-US PNR Abkommen gewünscht, dessen Überprüfung im Rahmen eines Joint Reviews - einer gemeinsamen Überprüfung durch Vertreter von US- und europäischen Behörden - noch aussteht. Zweck der Vereinbarung war vornehmlich die Übermittlung von Passagierdaten zur Terrorismusbekämpfung, aber die USA sind uns nach wie vor den Beweis schuldig geblieben, dass die Daten auch tatsächlich im Kampf gegen den Terrorismus erforderlich sind. Auch ist nicht zu erkennen, welchen zusätzlichen Nutzen das jetzt von Washington eingeführte elektronische Reisegenehmigungsverfahren ESTA[5] hat, da viele Daten bereits im Rahmen des PNR-Abkommens übermittelt werden und andere Angaben nur sehr schwer überprüft werden können. Die Anfangsschwierigkeiten in den USA bei der Einführung von ESTA sind enorm. Die EU wäre deshalb gut beraten, erst einmal die Erfahrungen der US-Seite

[3]“ Second Safe Harbour Agreement Implementation Study prepared by Charlotte Born, Prof. Cécile de Terwangne and Prof. Yves Poullet”, Universität Namur, Belgien vom 30. Juni 2008
[4] “The US Safe Harbor – Fact or Fiction?” von Chris Connolly, Galexia vom 2. Dezember 2008
[5] ESTA: Electronic System for Travel Authorization

abzuwarten, bevor sie sich, wie bereits erwähnt, an die Einführung eines europäischen ESTA-Systems macht. Problematisch ist aus meiner Sicht insbesondere, dass das Prinzip des freien - auch visafreien - Reiseverkehrs durch derartige Systeme faktisch unterlaufen wird. Die dabei erhobenen Datenmengen sind immens und sollen für viele Jahre gespeichert werden. Teilweise geht es dabei um sensibelste Informationen, etwa zum Gesundheitszustand. Wenn die Tatsache, dass ein Reisender HIV-positiv ist, einmal in einer solchen Datenbank landet, kann dies erhebliche Folgen für sein weiteres Leben haben. Ich betone: dies ist keine theoretische Annahme, sondern logische Folge des von den USA kürzlich eingeführten ESTA-Systems, denn eine HIV-Infektion gehört zu den elektronisch abgefragten Informationen.

Sehr kritisch sind auch die Memoranden zu sehen, die die USA mit einer Reihe von osteuropäischen Ländern zum Austausch von u. a. biometrischen und daktyloskopischen Daten geschlossen haben und die zum Teil unter Ausschluss parlamentarischer Kontrolle und ohne Mitwirkung der unabhängigen Datenschutzbeauftragten zu Stande kamen. Diese Vorhaben, von der Öffentlichkeit nur unzureichend wahrgenommen, führen zu unterschiedlichen Datenschutzregimen in der EU und schwächen die Haltung Europas. Zwar ist der Wunsch dieser Staaten, wie ihre westeuropäischen Partner am Visa Waiver Programm teilnehmen zu wollen, nur zu verständlich, es stellt sich aber die Frage, ob der Preis, den sie zu zahlen bereit sind, angemessen ist.

Gegen das Abkommen[6], das die Bundesrepublik Deutschland mit den USA zur polizeilichen Zusammenarbeit am 1. Oktober 2008 unterzeichnet hat, das allerdings noch nicht in Kraft getreten ist, habe ich mich wiederholt ausgesprochen. Die USA und die Bundesrepublik Deutschland räumen sich in diesem Abkommen einen gegenseitigen Zugriff auf daktyloskopische Daten und DNA-Profile ein. Im Abkommen sind keine subjektiven Rechte der Betroffenen geregelt, so dass diese keinen Rechtsschutz von unabhängigen Stellen erlangen können. Auch gibt es in den USA keine unabhängige Datenschutzkontrolle und es ist nicht klar, für wie lange die Daten dort gespeichert werden. Ich kann mir nur wünschen, dass das Abkommen in seiner jetzigen Form nicht vom Bundestag verabschiedet wird und in Europa keine Schule macht.

Auf internationaler Ebene möchte ich einige positive Entwicklungen hervorheben.
Zu nennen ist hier der Datenschutztag, zu dem Sie mich freundlicherweise eingeladen haben und der auf eine Initiative des Europarats im Jahre 2006 zurückgeht. Wir begehen ihn in diesem Jahr bereits zum dritten Mal. Die Internationalen Datenschutzkonferenz 2008 in Straßburg hat eine Arbeitsgruppe eingerichtet, die das Konzept des Datenschutztages weiterentwickeln soll. Die

[6] Deutsch-Amerikanisches Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität

internationale Datenschutzgemeinde ist sich einig, dass die anstehenden Probleme und Herausforderungen für den Datenschutz globale Antworten erfordern und nur gemeinsam angegangen werden können und dass deshalb das Bewusstsein für den Datenschutz auf internationaler Ebene gefördert werden muss. Ich bin zuversichtlich, dass der Datenschutztag weitere Verbreitung finden und zu nachhaltigen Diskussionen über aktuelle Fragen anregen wird.

Eine weitere Initiative des Europarats verdient gleichfalls unsere Wertschätzung, nämlich die Öffnung der Konvention 108 für Nicht-Mitglieder. Wir erhoffen uns von dieser Maßnahme eine intensivere Diskussion zum Stand des Datenschutzes in Nicht-Mitgliedstaaten. Eine solche Debatte wird den Datenschutz langfristig stärken. Dem Europarat ist zu wünschen, dass seine Initiative Erfolg hat und viele weitere Länder dieser Konvention beitreten.

Immer noch fehlt ein weltweit verbindliches Rechtsinstrument für den Datenschutz. Eine globale Karte des Datenschutzes ist schon deshalb notwendig, weil auch die Datenverarbeitung zunehmend auf globaler Ebene stattfindet. Nationale und auch regional begrenzte Regelungen - wie etwa die EG-Datenschutzrichtlinie - können den mit der Globalisierung der Datenströme einhergehenden Risiken nur unzureichend Rechnung tragen. Immerhin hat auch hier die internationale Datenschutzgemeinschaft eine Initiative gestartet und ich erhoffe mir konkrete Ergebnisse von der Internationalen Konferenz, die im November 2009 in Madrid stattfindet.

Globale Standards sind auch auf anderen Gebieten erforderlich. So hat die internationale Datenschutzkonferenz 2007 in Montreal globale Standards für die Verwendung von Flugpassagier-Daten gefordert. Wer die derzeit bestehenden EU-Abkommen mit den USA, Kanada und Australien vergleicht, wird rasch feststellen, welche Unterschiede es hier beim Datenschutz gibt und welch unterschiedliche Rechte Fluggäste genießen oder ihnen verweigert werden. Es ist höchste Zeit, endlich sicherzustellen, dass alle Passagiere, wohin sie auch fliegen, die gleichen Rechte wahrnehmen können und ihre Privatsphäre geschützt bleibt. Auch hier liegt noch viel Arbeit vor uns.

Sehr geehrte Damen und Herren, wenn ich mir die hier skizzierten Entwicklungen zum Datenschutz anschaue, sei es auf europäischer, sei es auf internationaler Ebene, gibt es keinen Grund zu Pessimismus. Die vor uns liegenden Herausforderungen sind enorm, aber die stetig wachsende Datenschutzgemeinde ist gut vernetzt, sie ist aktiv und wird sich diesen Herausforderungen stellen. Wir hoffen bei diesen wichtigen Vorhaben auf eine möglichst breite Unterstützung in der Politik und in der Öffentlichkeit.

Ich danke Ihnen für Ihre Aufmerksamkeit.