Dokumente
zu Datenschutz
und Informationsfreiheit
2009

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: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Stand: Februar 2010

Inhaltsverzeichnis

Vorwort

Beauftragte für Datenschutz und Informationsfreiheit müssen sich Gehör verschaffen. Sie haben dies 2009 auf nationaler wie auf internationaler Ebene zu einer Vielzahl von Problembereichen getan.

Die nationale Konferenz der Datenschutzbeauftragten hat unter Berliner Vorsitz in zwölf Entschließungen zu aktuellen Themen des Datenschutzes Positionen formuliert, die vom Beschäftigtendatenschutz über die polizeiliche Datenverarbeitung und die datenschutzgerechte Gestaltung von Krankenhausinformationssystemen bis hin zu prinzipiellen Defiziten beim Datenschutz und zur Notwendigkeit der Förderung einer Datenschutzkultur reichten. Auch das SWIFT-Abkommen und das Stockholmer Programm veranlassten die Datenschutzbeauftragten zu deutlichen Forderungen nach Beachtung grundrechtlicher Gewährleistungen in der Europäischen Union. Die Aufsichtsbehörden für den Datenschutz in der Wirtschaft haben ebenfalls zu Problemen des grenzüberschreitenden Datenschutzes wie der anlassunabhängigen Übermittlung von Flugpassagierdaten an britische Behörden und dem Mitarbeiter-Screening in international tätigen Unternehmen Stellung genommen. Daneben stand die datenschutzgerechte Gestaltung von Analyseverfahren zur Reichweitenmessung im Internet auf der Tagesordnung der Aufsichtsbehörden.

Auf europäischer und internationaler Ebene stand die Weiterentwicklung und Garantie des Datenschutzes durch verbindliche Standards im Vordergrund, daneben wurden aber auch spezielle Themen wie die Beweiserhebung bei grenzübergreifenden Zivilprozessen behandelt. Die Stellungnahme der Artikel 29-Gruppe zur Nutzung von sozialen Netzwerken geht wesentlich auf frühere Vorarbeiten der sog. Berlin Group zurück, die sich in diesem Jahr mit Problemen der elektronischen Mauterhebung auseinandergesetzt hat.

Die Informationsfreiheitsbeauftragten in Deutschland haben sich mehrfach für eine Vereinheitlichung und Vereinfachung der Regeln zum Informationszugang ausgesprochen, aber auch mit dem notwendigen Schutz von Whistleblowern beschäftigt.

Diese Zusammenstellung von Entschließungen und Arbeitspapieren der Beauftragten für Datenschutz und Informationsfreiheit beleuchtet schlaglichtartig die gemeinsamen Schwerpunkte ihrer Arbeit im zurückliegenden Jahr. Sie ist wie immer auch über unsere Webseite abrufbar.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließung vor der 77. Konferenz (vom 18. Februar 2009)

Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!

Das Bundeskabinett hat am 14. Januar 2009 den **Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes** beschlossen (BR-Drs. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der ITSicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),

2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und

3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor (zu erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der „Netze des Bundes“ als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

2. Entschließungen der 77. Konferenz vom 26./27. März 2009 in Berlin

Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)

- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.

- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

- Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.

- Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch erworbenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.
3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Ländern fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteu-

erungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung der Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch gegenüber der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

3. Entschließung zwischen der 77. und der 78. Konferenz (vom 16. April)

Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3.4.2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst

werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

4. Entschließungen der 78. Konferenz am 8./9. Oktober 2009 in Berlin

Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft,

die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

„Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

„Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu

ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen „Reality"-Reportagen Abstand zu nehmen.

Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem \u201eEuropa der Bürger\u201c. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST – im weiteren Verfahren einzusetzen.

Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;

- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;

- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;

- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;

- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;

- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;

- die Videoüberwachung in Staat und Gesellschaft einzuschränken;

- den Schutz der Meldedaten zu verbessern;

- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

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

1. Beschlüsse der Sitzung am 23./24. April 2009 in Schwerin

Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinaus gehende Listen z. B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind.

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt.

In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

Telemarketing bei NGOs

Auch die so genannten NGOs (non governmental organization), also nichtstaatliche Organisationen, die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt.

Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

2. Beschlüsse zwischen den Sitzungen des Düsseldorfer Kreises

Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern! (vom 13. Juli 2009)

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig (vom 22. Oktober 2009)

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.

2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:

   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;

   - sonstige Daten über negatives Zahlungsverhalten, bei denen

     – die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und

     – eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen – so der damalige Beschluss – seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber so genannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Ein-

schränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer 2. genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

3. Beschlüsse der Sitzung am 26./27. November 2009 in Stralsund

Gesetzesänderung bei der Datenverwendung für Werbezwecke

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden.

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofil genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen

erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.

- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

III. Europäische Konferenz der Datenschutzbeauftragten

Edinburgh, 23./24. April 2009

Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa

Europa hat eine lange und stolze Geschichte von Standards und Gesetzgebung im Bereich des Datenschutzes. Einige davon wurden im Laufe der Zeit geändert und andere werden unter Beobachtung bleiben. Die Gesetzgebung folgt immer dem technischen und sozialen Fortschritt und es ist für die Datenschutzbehörden eine Herausforderung, mit diesen Entwicklungen Schritt zu halten und angesichts dieser sich schnell ändernden Umstände die Gesetze anzuwenden und eine Strategie zu entwickeln.

Datenschutzrechtliche Standards und Gesetzgebung entwickeln sich auch zügig in den restlichen Teilen der Welt und Europa spielte aufgrund seiner beratenden und unterstützenden Tätigkeit eine wichtige Rolle in einigen Ländern. Obwohl die bestehenden Standards und Gesetzgebungen Unterschiede in bestimmten Bereichen aufweisen können, zielen sie letzten Endes doch alle auf den Schutz personenbezogener Daten und die Rechte und Freiheiten der Einzelnen ab.

Die Konferenz verpflichtet sich, einen Beitrag für die Entwicklung des Datenschutzes in Europa zu leisten und dafür zu sorgen, dass aus den Erfahrungen der europäischen Länder Nutzen für die weltweite Diskussion über den Datenschutz gezogen wird. Dazu gehört auch die bessere Umsetzung und Durchsetzung des bestehenden Rechtsrahmens.

Die europäischen Datenschutzbeauftragten stehen zu ihrer Führungsrolle in der Zukunft. Dementsprechend erwartet die Konferenz, dass die Datenschutzbeauftragten einen konstruktiven Beitrag zu den laufenden Arbeiten und Initiativen leisten, die darauf abzielen, die Diskussion über die Zukunft des Datenschutzes in Europa und insbesondere über den zukünftigen Rechtsrahmen voranzubringen.

Die Konferenz wird sich weiterhin für die Notwendigkeit von hohen Datenschutzstandards in allen Lebensbereichen einsetzen, insbesondere in Bezug auf technologische Entwicklungen, die Online-Welt und Strafverfolgungsmaßnahmen.

Die Konferenz unterstützt die Entwicklung und Verbesserung einer umfassenden Gesetzgebung zum Datenschutz, die

- die Grundrechte und Freiheiten gewährleistet und fördert;
- auf bestehenden Datenschutzgrundsätzen aufbaut;
- Wert darauf legt, dass die angestrebten Ergebnisse in der Praxis auf effektive Art und Weise erreicht werden;
- Organisationen ermutigt, beste Praktiken zu übernehmen, wie etwa „privacy by design“ (eingebauter Datenschutz);
- die Risiken schädlicher Auswirkungen angeht, denen der Einzelne und die Gesellschaft insgesamt ausgesetzt sind;
- nicht zu rechtfertigende Belastungen vermeidet und
- für eine effektive Durchsetzung sorgt.

Die Konferenz ruft alle auf, die an Diskussionen über Strategien und Gesetze zum Datenschutz beteiligt sind, sich mit den Gemeinsamkeiten statt mit den Unterschieden verschiedener Regelwerke und Rahmenwerke zu befassen und nach Wegen zur Förderung globaler Lösungen zu suchen. Indem sie die Erfahrungen der europäischen Länder in die weltweite Debatte mit einbringt, ermutigt die Konferenz zu einem Geist der Zusammenarbeit, der vollständig mit der Förderung der Grundrechte und Freiheiten im Einklang steht.

Mit dieser Erklärung nimmt die Konferenz zur Kenntnis, dass sich die Datenschutzlandschaft sowohl innerhalb als auch außerhalb Europas weiterentwickelt. Sie sieht auch die Notwendigkeit, unsere Arbeit zur Förderung des Datenschutzes und der Datenschutzstandards fortzusetzen, indem wir uns an die Welt anpassen, in der wir leben.

Entschließung zu bilateralen und multilateralen Abkommen zwischen europäischen Staaten und Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Datenschutzstandards in bilateralen und multilateralen Abkommen, die europäische Staaten mit Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit geschlossen haben, weisen große Unterschiede auf.

Die geltenden Rechtsrahmen, die Konvention 108, ihre Protokolle und der Rahmenbeschluss 2008/977/JHA über den Schutz personenbezogener Daten gewähr-

leisten ein besonderes datenschutzrechtliches Regelwerk für den Austausch personenbezogener Daten.

Angesichts dieser Tatsache weist die Europäische Datenschutzkonferenz darauf hin, dass diese großen Unterschiede das von den europäischen Staaten verfolgte Ziel, nämlich die Schaffung eines möglichst einheitlichen und effektiven Datenschutzes für alle Personen, gefährden.

Die Konferenz fordert daher alle europäischen Staaten auf, sicherzustellen, dass beim Abschluss internationaler Abkommen geltende Datenschutzstandards eingehalten werden. In diesem Zusammenhang setzt sich die Konferenz nachdrücklich für die Entwicklung und die anschließende Aufnahme solcher datenschutzrechtlicher Standardklauseln in diesen Abkommen ein.

IV. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery) (WP 158)

Angenommen am 11. Februar 2009

Zusammenfassung

Dieses Arbeitspapier soll den Personen, die nach EU-Recht für die Datenverarbeitung verantwortlich sind, als Leitfaden bei der Bearbeitung von Ersuchen um Übermittlung personenbezogener Daten ins Ausland zwecks Verwendung in einem Zivilprozess dienen. Anlass für die Ausarbeitung dieses Dokuments war die Feststellung der Arbeitsgruppe, dass die Richtlinie 95/46/EG in den Mitgliedstaaten unterschiedlich angewandt wird, was zum Teil auf die Vielfalt der zivilrechtlichen Verfahren in der EU zurückzuführen ist.

Im ersten Abschnitt dieses Papiers legt die Arbeitsgruppe kurz die unterschiedlichen Positionen zu Rechtsstreitigkeiten und insbesondere zu Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung (pre-trial discovery) in den angloamerikanischen (u. a. USA und Vereinigtes Königreich) und kontinentaleuropäischen Rechtssystemen dar.

Im Anschluss daran werden Leitlinien für die in der EU für die Datenverarbeitung Verantwortlichen aufgestellt, die die prozessualen Anforderungen eines bei einem ausländischen Gericht anhängigen Rechtsstreits mit den Datenschutzverpflichtungen aufgrund der Richtlinie 95/46/EG in Einklang zu bringen suchen.

Einleitung

Die Frage der grenzübergreifenden Offenlegung, insbesondere in Bezug auf in Europa gespeicherte Daten, die beispielsweise für ein Gerichtsverfahren in den Vereinigten Staaten angefordert werden, hat in letzter Zeit an Bedeutung gewonnen. Oft stehen Unternehmen mit einer Niederlassung oder Tochtergesellschaft in den Vereinigten Staaten unter erheblichem Druck, weil sie für Rechtsstreitigkeiten und Ermittlungen der Strafverfolgungsbehörden in den USA Unterlagen und Material (einschließlich elektronisch gespeicherter Daten) vorlegen müssen.

Dabei umfasst das angeforderte Material häufig personenbezogene Daten von Arbeitnehmern oder Dritten, einschließlich Auftraggebern oder Kunden.

Zwischen der Offenlegungspflicht aufgrund des US-amerikanischen Prozess- oder Verwaltungsrechts und der Anwendung datenschutzrechtlicher Bestimmungen der EU besteht ein Spannungsverhältnis. Gleiches gilt für die geografische und territoriale Grundlage des Datenschutzsystems der EU im Verhältnis zum multinationalen Charakter der Wirtschaftstätigkeit, demzufolge ein Unternehmen überall in der Welt Tochtergesellschaften oder Niederlassungen haben kann. Von besonderer Bedeutung ist dies für die europäischen Tochtergesellschaften multinationaler Unternehmen, die dem Dilemma der kollidierenden Anforderungen amerikanischer Gerichtsverfahren und der europäischen Vorschriften für den Datenschutz und den Schutz der Privatsphäre, die für die Übermittlung personenbezogener Informationen gelten, ausgesetzt sind.

Die Arbeitsgruppe räumt ein, dass die an einem Rechtsstreit beteiligten Parteien ein legitimes Interesse am Zugang zu den erforderlichen Informationen haben, um Ansprüche geltend zu machen oder sich zu verteidigen; dies muss aber in einem ausgewogenen Verhältnis zu den Rechten der Person stehen, um deren Daten es geht.

Bei den in diesem Arbeitspapier vorgeschlagenen Leitlinien ist zu bedenken, dass sich die Frage der Offenlegungspflichten im Pre-trial-Discovery-Verfahren nicht mit einer Stellungnahme der Arbeitsgruppe beantworten lässt, sondern nur zwischenstaatlich – etwa durch die Einführung weiterer globaler Vereinbarungen im Sinne des Haager Übereinkommens – geregelt werden kann.

1. Konzept der pre-trial discovery

Verschiedene Aspekte des amerikanischen Prozessrechts und seiner Verfahren können sich auf im Besitz europäischer Unternehmen befindliche Daten auswirken. Besonders verbreitet sind:

- Präventives Vorhalten von Unterlagen in Erwartung eines Gerichtsverfahrens in den USA oder als Reaktion auf ein diesbezügliches Ersuchen, so genanntes „freezing“
- Vorprozessuale Beweisanträge in zivilrechtlichen Verfahren in den USA, die Offenlegungspflichten begründen
- Vorlage von Dokumenten bei straf- oder verwaltungsrechtlichen Ermittlungen in den USA
- Straftaten im Zusammenhang mit der Vernichtung von Daten in den USA.

In diesem Dokument werden nur die beiden ersten Aspekte behandelt, da diese Auswirkungen auf den Prozessverlauf und die Frage der Übermittlung personenbezogener Daten an einen Drittstaat haben. Die vorprozessuale Beweisbeschaffung kann nicht nur die Offenlegung von Daten im Rahmen von Gerichtsverfahren umfassen, sondern auch die Vorratsspeicherung von Daten mit Blick auf ein etwaiges künftiges Verfahren.

Mit dem vorprozessualen Beweisbeschaffungsverfahren soll sichergestellt werden, dass die Parteien in einem Rechtsstreit Zugang zu den Informationen haben, die für ihren Fall aufgrund der Vorschriften und Verfahren des Gerichts, bei dem der Prozess anhängig ist, erforderlich und relevant sind. In den Common-Law-Staaten sind die Offenlegungsanforderungen nicht beschränkt auf beispielsweise personenbezogene Daten oder elektronische Dokumente. Die angeforderten Informationen können sensible personenbezogene Daten wie Gesundheitsdaten oder private E-Mails (deren Bereitstellung den Verpflichtungen aus dem Fernmeldegeheimnis oder anderen Geheimhaltungsvorschriften zuwiderlaufen kann) und Daten Dritter, z. B. von Angestellten oder Kunden, einschließen.

Im Zivilprozessrecht des Vereinigten Königreichs wird der Begriff „document" verwendet; er schließt neben aus Computersystemen und anderen elektronischen Geräten leicht zugänglichen Dokumenten elektronische Dokumente, darunter E-Mail und andere elektronische Kommunikation, textverarbeitete Dokumente und Datenbanken, ein. Er umfasst auch auf Servern gespeicherte Dokumente und Datensicherungssysteme sowie „gelöschte" elektronische Dokumente. Er erstreckt sich ferner auf Metadaten, d. h. alle gespeicherten und zugehörigen zusätzlichen Informationen zu elektronischen Dokumenten.

Der verstärkte Einsatz elektronischer Aufzeichnungen, wo früher nur mit Druckexemplaren gearbeitet worden wäre, hat dazu geführt, dass mehr Informationen als je zuvor verfügbar sind. Aufgrund der einfachen Abrufung, Übermittlung oder sonstigen Handhabung elektronischer Aufzeichnungen produziert das vorprozessuale Beweisbeschaffungsverfahren oft eine Fülle an Informationen, von denen die Parteien bestimmen müssen, welche Teile für den entsprechenden Einzelfall relevant sind. Die elektronisch gespeicherten Informationen haben ein weitaus größeres Volumen als Aufzeichnungen auf Papierträger, so dass heute aufgrund der Speicherkapazität der verschiedenen Memory-Produkte mehr Informationen zur Verfügung gestellt und offen gelegt werden können[1].

[1] Gemäß den Zahlen des Advisory Committee on Civil Rules in den USA existieren 92 % aller neuen Informationen heute in digitaler Form, von denen ca. 70 % nie ausgedruckt werden. Infolgedessen hat sich das Verfahren der Pre-trial-Discovery fast vollständig zur E-Discovery entwickelt. Die USA haben jetzt Schritte zur Regelung dieses neuen Bereichs unternommen.

Unterschiede zwischen dem angloamerikanischen und dem kontinentaleuropäischen Recht

Als Erstes fällt auf, dass nicht nur beim Prozessrecht allgemein, sondern insbesondere bei der Beweiserhebung Unterschiede zwischen dem angloamerikanischen und dem kontinentaleuropäischen Recht bestehen. Die Beweisbeschaffung ist in den beiden Rechtssystemen höchst unterschiedlich geregelt. Die Möglichkeit, im Laufe des Rechtsstreits Informationen zu erhalten, ja die Pflicht, diese schon vor dem Prozess bereitzustellen, ist in den angloamerikanischen Rechtsordnungen Bestandteil des Verfahrens. Der extensive Informationsaustausch vor der eigentlichen Gerichtsverhandlung gilt als die effizienteste Methode zur Klärung strittiger Fragen. Insbesondere gilt dies für die Vereinigten Staaten, in denen die vorprozessuale Beweiserhebung sehr viel weiter geht als in den anderen Common-Law-Staaten.

Common Law – Vereinigte Staaten

Sobald ein Rechtsstreit begonnen hat, müssen Unternehmen in den USA den Verpflichtungen nachkommen, die ihnen das amerikanische Prozessrecht nicht nur nach dem Bundesrecht, sondern auch nach den Zivilprozessordnungen der einzelnen Bundesstaaten auferlegt, nach denen die Parteien dazu angehalten werden, vor dem Prozess Informationen auszutauschen[2]. Dies betrifft nicht nur die Offenlegung relevanter Informationen, sondern auch die Offenlegung von Informationen, die an sich vielleicht nicht unmittelbar relevant sind, aber zur Offenlegung relevanter Informationen führen könnten (die so genannten „smoking-gun"). Dies steht im Widerspruch zu vielen europäischen Rechtsordnungen, in denen solche „Fischzüge" („fishing expeditions") untersagt sind.

Nach Rule 26f der Zivilprozessordnung der USA müssen sich die Parteien treffen und beraten („meet and confer"), um den Parteien in einem frühen Stadium des Prozesses die Diskussion und Einigung über die mit der Offenlegung zusammenhängenden Fragen zu ermöglichen. Ein Ziel dieses Treffens ist die Sicherung der Beweismittel, einschließlich der für den Rechtsstreit erforderlichen Daten und Unterlagen.

US-Gerichte können auch von sich aus oder auf Antrag einer Partei mittels einer Schutzverfügung (Protective Order) den Umfang zu weit reichender vorprozes-

[2] So sehen die Federal Rules of Civil Procedure (Zivilprozessordnung) beispielsweise unter Rule 34 (b) vor, dass jede Partei jede andere Partei auffordern kann, alle bezeichneten Dokumente oder elektronisch gespeicherten Informationen vorzulegen – einschließlich Schriften, Zeichnungen, Grafiken, Karten, Fotographien, Tonaufnahmen, Bilder und andere in einem Medium gespeicherte Daten oder Datensammlungen, von dem die Informationen abgerufen werden können … die sich im Besitz, im Gewahrsam oder unter der Kontrolle der Partei befinden, an die die Aufforderung gerichtet ist, und der Antrag stellenden Partei oder einer in ihrem Namen handelnden Person zu erlauben, Einsicht in diese Dokumente und Informationen zu nehmen, sie zu kopieren, zu testen oder von ihnen Stichproben zu nehmen.

sualer Beweisanträge einschränken, da sie aufgrund der Vorschriften befugt sind, die Häufigkeit oder das Ausmaß der Verwendung solcher Anträge aus verschiedenen Gründen zu begrenzen; unter anderem wegen der Möglichkeit, die Information aus einer geeigneteren Quelle zu erhalten, oder wenn die Belastung oder die Ausgaben in Bezug auf die vorgeschlagene Offenlegung den zu erwartenden Nutzen übertreffen. Mittels dieser Schutzverfügung können die Gerichte ferner eine Person oder Partei vor Belästigungen, Unannehmlichkeiten, Schikane, unzumutbaren Belastungen oder Ausgaben schützen, indem sie z. B. anordnen, dass eine Offenlegung oder Aufdeckung nur unter bestimmten Voraussetzungen erfolgen kann, wobei auch die Methode oder der Sachverhalt zu berücksichtigen ist.

Ein US-Richter wird somit einem Beweisantrag stattgeben, solange dieser in vertretbarer Art und Weise auf die Erlangung zulässiger Beweismittel abzielt und keine unmöglichen Forderungen enthält.

Vereinigtes Königreich

Ähnlich, aber weniger umfassend ist die Regelung in Rule 31 der Zivilprozessordnung des Vereinigten Königreichs, wonach eine Partei Unterlagen offen legen muss, auf die sie sich zu stützen gedenkt, sowie alle weiteren Unterlagen, die für sie nachteilig sind, eine andere Partei belasten oder unterstützen oder die durch einschlägige Anweisungen des Gerichts offen zu legen sind. Im Gegensatz zu den USA bestehen im Vereinigten Königreich (wie auch in Kanada) Datenschutzverpflichtungen.

Länder mit kontinentaleuropäischem Rechtssystem

Im Gegensatz zu dem auf völlige Transparenz abstellenden Discovery-Verfahren in den USA und anderen Common-Law-Staaten verfahren die meisten kontinentaleuropäischen Systeme restriktiver und kennen oft kein formelles Offenlegungsverfahren im Rahmen der Beweiserhebung. Viele kontinentaleuropäische Rechtsordnungen beschränken die Offenlegung von Beweismitteln auf für den Prozess erforderliche Beweise und untersagen eine weitergehende Offenlegung. Es ist Sache der Streitpartei, zur Unterstützung ihrer Sache Beweismittel vorzulegen. Benötigt die gegnerische Partei diese Informationen, so ist es an ihr, sich Kenntnis darüber zu verschaffen und die Informationen genau zu benennen. In Frankreich und Spanien ist die Offenlegung einzig und allein auf die Dokumente beschränkt, die vor Gericht zulässig sind. Die Offenlegung der Dokumente wird von dem Richter überwacht, der über die Relevanz und die Zulässigkeit des von den Parteien vorgeschlagenen Beweismittels entscheidet.

In Deutschland sind die Streitparteien nicht verpflichtet, der anderen Partei Dokumente offen zu legen. Sie müssen nur die Dokumente vorlegen, die ihr Vor-

bringen unterstützen. Dabei muss es sich um authentische und beglaubigte Originale handeln. Die Partei, die die Vorlage eines Dokuments begehrt, muss bei Gericht eine entsprechende Anordnung erwirken. Dazu ist eine genaue Beschreibung des Dokuments erforderlich, die den Sachverhalt, für den das Dokument als Beweismittel dienen soll, und die Rechtfertigung für die Vorlage des Dokuments umfasst. Befindet sich das Dokument im Besitz eines Dritten, so benötigt die Partei, die sich um das Dokument bemüht, die Genehmigung dieser Person. Wird die Genehmigung verweigert, so muss der Antragsteller gegen den Besitzer der Dokumente ein Verfahren anstrengen.

Die Unterschiede zwischen der Herangehensweise des angloamerikanischen und des kontinentaleuropäischen Rechts bei der Offenlegung von Informationen, einschließlich personenbezogener Daten, werden – vom Datenschutz abgesehen – an der Dichotomie zwischen der „Überzeugung von der Wahrheit" und dem Postulat „die Wahrheit und nichts als die Wahrheit" deutlich.

Präventive Rechtsvorschriften

Einige Länder, im Wesentlichen Länder mit kontinentaleuropäischem Recht, aber auch einige Common-Law-Staaten, haben Gesetze (*blocking statutes*) erlassen, um die grenzüberschreitende Offenlegung von Informationen zwecks Vorlage bei ausländischen Gerichten zu beschränken. Wenig Einheitlichkeit lässt sich bezüglich ihrer Einführung, ihres Anwendungsbereichs und ihrer Wirkung feststellen. Einige, wie zum Beispiel Frankreich, verbieten die Offenlegung bestimmter Kategorien von Dokumenten oder Informationen als Beweismittel für gerichtliche oder administrative Verfahren im Ausland. Eine Partei, die Informationen offen legt, kann sich des Verstoßes gegen die Gesetze des Landes schuldig machen, in dem sich die Informationen befinden, und das kann zu zivil- oder sogar strafrechtlichen Sanktionen führen[3].

Die amerikanischen Gerichte haben bisher solche Bestimmungen nicht als Grund akzeptiert, die Offenlegung von Daten für Rechtsstreitigkeiten in den USA zu verweigern. Gemäß der dritten Anpassung (Third restatement) des Gesetzes Nr. 442 über die Außenbeziehungen der Vereinigten Staaten (Foreign Relations Law) kann ein Gericht eine unter seine Gerichtsbarkeit fallende Person anweisen,

[3] Ein Beispiel dafür ist das französische Strafgesetz Nr. 80-538, das Folgendes vorsieht: Vorbehaltlich geltender internationaler Verträge oder Abkommen, Rechts- und Verwaltungsvorschriften ist es jeder Person untersagt, schriftlich, mündlich oder in anderer Form als Beweismittel im Hinblick auf gerichtliche oder administrative Verfahren im Ausland oder im Rahmen derartiger Verfahren Dokumente oder Informationen wirtschaftlicher, kommerzieller, industrieller oder finanzieller Art anzufordern, zu beantragen oder zu übermitteln. 2008 bestätigte der französische Oberste Gerichtshof wegen Verletzung dieser Vorschriften die strafrechtliche Verurteilung eines französischen Anwalts, der einem Ersuchen amerikanischer Gerichte in der Rechtssache Strauss gegen Crédit Lyonnais, S.A., 2000 U.S. Dist. Lexis 38378 (E.D.N.Y. 25. Mai 2007) nachgekommen war. Dem Anwalt wurde eine Geldstrafe von 10 000 EUR (ca. 15 000 USD) auferlegt.

Beweismittel vorzulegen, auch wenn sich die Informationen nicht in den Vereinigten Staaten befinden[4] Wie von einem Teil der Rechtsprechung befürwortet[5], sollte eine Abwägung erfolgen mit dem Ziel, dass das Gericht über den Antrag einer Partei auf Vorlage von im Ausland befindlichen Informationen nur nach Berücksichtigung folgender Aspekte entscheiden sollte:

(1) Bedeutung der angeforderten Informationen für den Rechtsstreit;

(2) Detailliertheit der angeforderten Informationen;

(3) ob die Informationen aus den Vereinigten Staaten stammen;

(4) Verfügbarkeit alternativer Mittel zur Informationssicherung;

(5) inwieweit ein Zurückweisen den Interessen der Vereinigten Staaten bzw. ein Stattgeben den Interessen eines souveränen ausländischen Staates schaden würde.

Die jüngste Veröffentlichung der Sedona-Konferenz über Konflikte bei der grenzüberschreitenden Beweisbeschaffung enthält eine detaillierte Analyse der Rechtsprechung in den USA sowie eine Betrachtung der Faktoren, die für den Umfang grenzübergreifender Offenlegungspflichten maßgebend sind[6]. Danach sind Notwendigkeit, Kosten und Belastung der Offenlegung mit den Interessen der betreffenden ausländischen Rechtsordnung am Schutz der Privatsphäre und des Gemeinwohls ihrer Bürger abzuwägen. Im Sedona Conference Framework wird auch festgestellt, dass die französische Entscheidung im Crédit-Lyonnais-Fall bei den US-Gerichten dazu geführt hat, ausländische Präventivgesetze mit anderen Augen zu sehen[7].

---

4 Dazu ist anzumerken, dass vom Standpunkt des amerikanischen Richters aus – unabhängig vom „materiellen" Aufbewahrungsort der Daten – das amerikanische Recht anwendbar ist und keine Notwendigkeit besteht, internationale Übereinkommen wie das Haager Übereinkommen anzuwenden, wenn das Unternehmen amerikanischem Recht unterliegt und sich die Informationen in seinem Besitz, unter seiner Kontrolle oder in seinem Gewahrsam befinden oder wenn es vom Hoheitsgebiet der USA aus (über einen Computer) auf diese Informationen zugreifen darf.

5 Société Nationale Industrielle Aérospatiale gegen United States District Court, 482 U.S. 522, 544 n.28 (1987), Volkswagen AG gegen Valdez [Nr.95-0514, 16. November 1995, Texas Supreme Court] und In re: Baycol Litigation MDL nr. 1431 (Mfd/JGL), 21. März 2003. Für eine weitergehende Analyse der amerikanischen Rechtsprechung siehe Sedona Conference Framework for Analysis of Cross Border Discovery Conflicts (Fußnote 6).

6 The Sedona Conference Framework for analysis of cross border discovery conflicts – A practical guide to navigating the competing currents of international data privacy and discovery – 23. April 2008 (Public Comment Version), A Project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery and Disclosure.

7 Sedona Framework, S. 31.

Das Haager Beweisübereinkommen

Informationsverlangen können auch über das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen erfolgen. Es bietet ein Standardverfahren für Rechtshilfeersuchen, d. h. für Anträge eines Gerichts an die benannte Zentrale Behörde eines anderen Staates auf Unterstützung bei der Erlangung relevanter Informationen, die sich in ihrem Staat befinden. Allerdings sind nicht alle EU-Mitgliedstaaten Vertragsstaaten des Haager Übereinkommens.

Eine weitere Komplikation besteht aufgrund von Artikel 23 des Übereinkommens, demzufolge „[j]eder Vertragsstaat bei der Unterzeichnung, bei der Ratifikation oder beim Beitritt erklären [kann], dass er Rechtshilfeersuchen nicht erledigt, die ein Verfahren zum Gegenstand haben, das in den Ländern des „Common Law" unter der Bezeichnung „pre-trial discovery of documents" bekannt ist". Viele Vertragsstaaten, darunter Frankreich, Deutschland, Spanien und die Niederlande, haben einen entsprechenden Vorbehalt nach Artikel 23 eingelegt und erklärt, dass eine Offenlegung von Informationen, ungeachtet ihrer Relevanz, nicht genehmigt würde, wenn die Informationen für ein Gerichtsverfahren im Ausland bestimmt sind. In Frankreich kann der zuständige Richter solche Rechtshilfeersuchen erledigen, wenn die angeforderten Dokumente/Informationen in den Rechtshilfeersuchen genau bezeichnet sind und mit dem betreffenden Rechtsstreit unmittelbar und konkret zusammenhängen.

Gemäß dem Haager Übereinkommen fallen unter das Verfahren der „pre-trial discovery" Beweisanträge, die nach der Klageerhebung, aber vor der Hauptverhandlung gestellt werden. Im Vereinigten Königreich wird diese Regel weiter ausgelegt. Danach kann ein Antrag gestellt werden, wenn die Beweismittel für Zivilverfahren erlangt werden sollen, die vor dem ersuchenden Gericht anhängig sind oder deren Einleitung vor diesem Gericht geplant ist[8]. Dies würde somit im Vereinigten Königreich eine großzügigere Bereitstellung von Informationen ermöglichen als in anderen Mitgliedstaaten.

Laut einer Entscheidung des Obersten Gerichtshofs der Vereinigten Staaten stellt das durch das Haager Beweisübereinkommen vorgesehene Verfahren ein fakultatives, aber kein bindendes Mittel zur Erlangung von Beweismitteln im Ausland für Streitparteien vor US-Gerichten dar[9].

Seitdem sind die amerikanischen Gerichte weitgehend diesem Ansatz gefolgt, gelegentlich haben sie aber auch Streitparteien aufgefordert, auf das Haager Beweisübereinkommen zurückzugreifen[10].

8 Evidence (Proceedings in Other Jurisdictions) Act 1975.

9 Société Nationale Industrielle Aérospatiale gegen United States District Court, 482 U.S. 522, 544 Nr. 28 (1987).

10 Siehe die Sammlung von post-Aérospatiale-Fällen, die sich auf das Haager Beweisübereinkommen berufen, zusammengestellt für die amerikanische Anwaltskammer von McNamara/Hendrix/Charepoo (Juni 1987 bis Juli 2003).

Sonstige Probleme

Eine der Hauptschwierigkeiten bei grenzübergreifenden Rechtsstreitigkeiten liegt in der Kontrolle der Verwendung von personenbezogenen Daten, die bereits aus anderen Gründen – z. B. aufgrund von BCR- oder Safe-Harbour-Regeln – ordnungsgemäß in die USA übermittelt worden sind. Diese Frage wird hier nicht behandelt, aber die Arbeitsgruppe räumt ein, dass dies der Offenlegung von Daten Vorschub leisten kann.

2. Stellungnahme

Die Arbeitsgruppe hält es für notwendig, die Erfordernisse des US-amerikanischen Prozessrechts mit den Datenschutzbestimmungen der EU in Einklang zu bringen. Sie räumtein, dass die Richtlinie Übermittlungen für Verfahrenszwecke nicht ausschließt und weltweit tätige Unternehmen im Ausland oft kollidierenden Anforderungen ausgesetzt sind, so dass diese sich genötigt fühlen, die für den Rechtsstreit im Ausland angeforderten Informationen zu übermitteln. Bestimmte Datenschutzerfordernisse müssen jedoch erfüllt sein, wenn für die Datenverarbeitung Verantwortliche personenbezogene Daten im Hinblick auf einen Rechtsstreit übermitteln wollen. Um die Datenschutzauflagen mit den Erfordernissen des ausländischen Rechtsstreits in Einklang zu bringen, schlägt die Arbeitsgruppe für die in der EU für die Datenverarbeitung Verantwortlichen die nachstehenden Leitlinien vor.

Leitlinien

Ein Rechtsstreit umfasst verschiedene Phasen. Die Verwendung personenbezogener Daten gilt in jeder dieser Phasen als Verarbeitung. Für die Legitimierung der Verarbeitung personenbezogener Daten in jeder einzelnen Phase ist eine entsprechende Voraussetzung zu erfüllen. Diese verschiedenen Phasen umfassen:

- Aufbewahrung
- Offenlegung
- Weiterleitung
- Sekundäre Nutzung.

Verschiedene Aspekte sind im Zusammenhang mit der Aufbewahrung zu betrachten, da gemäß der Richtlinie personenbezogene Daten während der für die

Zwecke erforderlichen Dauer aufzubewahren sind, für die die Daten gesammelt wurden oder für die sie weiter verarbeitet werden. Es ist nicht wahrscheinlich, dass die betroffenen Personen darüber unterrichtet wurden, dass ihre personenbezogenen Daten in ihrem eigenen Land oder im Ausland Gegenstand eines Rechtsstreits sein könnten. Auch wegen der unterschiedlichen Fristen, die in den einzelnen Ländern gelten, um Ansprüche geltend zu machen, lässt sich eine bestimmte Aufbewahrungsdauer für Daten nicht vorsehen.

Verantwortliche in der Europäischen Union besitzen keine Rechtsgrundlage dafür, personenbezogene Daten aufs Geratewohl unbefristet aufzubewahren, weil es möglicherweise in den Vereinigten Staaten zu einem Rechtsstreit kommen könnte. Nach den US-Zivilprozessregeln müssen lediglich *vorhandene* Informationen offen gelegt werden. Verfolgt der Verantwortliche eine klare Dokumentenverwaltungspolitik, die auf der Grundlage gesetzlicher Anforderungen kurze Aufbewahrungszeiten vorsieht, so verstößt er nicht gegen US-Recht. Anzumerken ist, dass in jüngster Zeit auch in den Vereinigten Staaten dahin tendiert wird, eine restriktive Aufbewahrung zu verfolgen, um die Wahrscheinlichkeit von Offenlegungsanträgen zu reduzieren.

Wenn jedoch die personenbezogenen Daten rechtserheblich sind und in einem konkreten oder unmittelbar bevorstehenden Verfahren verwendet werden sollen, sollten sie bis zum Verfahrensabschluss und bis zum Ende der Berufungsfrist aufbewahrt werden. Die Vernichtung von Beweismitteln kann einschneidende verfahrensrechtliche und andere Sanktionen nach sich ziehen.

Es kann sich als notwendig erweisen, Informationen, einschließlich personenbezogener Daten, präventiv oder für ein Gerichtsverfahren („litigation hold“) aufzubewahren. De facto bedeutet dies, dass das Unternehmen Dokumente, die für bereits anhängige oder noch zu erwartende Klagen relevant sein können, vorübergehend aus seinem Dokumentenverwaltungssystem, das die Aufbewahrung oder Vernichtung von Dokumenten regelt, herausnimmt.

Ein weiteres Problem kann sich ergeben, wenn die Informationen für einen zusätzlichen anhängigen Rechtsstreit erforderlich sind oder wenn ein künftiger Rechtsstreit vorhersehbar ist. Die Möglichkeit, dass eine Sache vor ein US-Gericht gebracht werden könnte, reicht allein ohne eine fundierte Begründung für die Offenlegung nicht aus.

In den Vereinigten Staaten wird zwar die Speicherung personenbezogener Daten für einen Rechtsstreit nicht als Verarbeitung angesehen, nach der Richtlinie 95/46/EG stellt aber jede Aufbewahrung, Konservierung oder Archivierung von Daten für derartige Zwecke eine Verarbeitung dar. Die Aufbewahrung von Daten für einen künftigen Rechtsstreit ist lediglich gemäß Artikel 7 Buchstaben c oder f der Richtlinie 95/46/EG möglich.

Rechtmäßigkeit der Verarbeitung für gerichtliche Verfahren

Ein rechtmäßiges Pre-trial-Discovery-Verfahren setzt eine zulässige Verarbeitung personenbezogener Daten im Einklang mit Artikel 7 der Datenschutzrichtlinie voraus. Außerdem müssen für Übermittlungen an ein ausländisches Gericht die Erfordernisse gemäß Artikel 26 erfüllt sein.

Die Verarbeitung kann aus drei Gründen rechtmäßig sein: die betroffene Person hat ihre Einwilligung erteilt, die Erfüllung der vorprozessualen Offenlegungspflichten ist für die Erfüllung einer rechtlichen Verpflichtung gemäß Artikel 7 Buchstabe c oder gemäß Artikel 7 Buchstabe f zur Verwirklichung eines berechtigten Interesses erforderlich, das von dem für die Verarbeitung Verantwortlichen oder Dritten wahrgenommen wird, denen die Daten übermittelt werden. Aus den nachstehend dargelegten Gründen ist die Arbeitsgruppe der Ansicht, dass in den meisten Fällen nicht damit zu rechnen ist, dass die Einwilligung einen triftigen Grund für eine solche Verarbeitung darstellt.

Einwilligung

Nach Artikel 7 ist zwar die Einwilligung eine Voraussetzung für die Verarbeitung, die Arbeitsgruppe vertritt aber die Auffassung, dass es in den meisten Fällen nicht wahrscheinlich ist, dass sie eine gute Grundlage für eine Verarbeitung darstellt. In Artikel 2 Buchstabe h ist die Einwilligung der betroffenen Person definiert als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden." Seit dem Aérospatiale-Fall ist das Hauptargument der US-Rechtsprechung, dass ein Unternehmen, wenn es sich für eine Geschäftstätigkeit in den Vereinigten Staaten oder mit Einbeziehung amerikanischer Partner entschieden hat, die US-Zivilprozessregeln zu beachten hat. Sehr oft haben allerdings betroffene Personen wie Kunden und Mitarbeiter dieses Unternehmens diese Wahl nicht oder waren nicht an der Entscheidung beteiligt, in den oder in Verbindung mit den Vereinigten Staaten Geschäfte zu tätigen.

Deshalb sollten für die Übermittlung ins Ausland Verantwortliche in der Europäischen Union in der Lage sein, die Einwilligung der betroffenen Person in jedem einzelnen Fall eindeutig nachweisen zu können. Außerdem kann von ihnen der Nachweis verlangt werden, dass die betroffene Person ordnungsgemäß informiert war. Handelt es sich bei den angeforderten personenbezogenen Daten um Daten eines Dritten, beispielsweise eines Kunden, so ist derzeit unwahrscheinlich, dass der für die Verarbeitung Verantwortliche den Beweis erbringen könnte, dass die betroffene Person gebührend informiert war und von der Verarbeitung in Kenntnis gesetzt wurde.

Gleichzeitig beinhaltet eine gültige Einwilligung, dass die betroffene Person ihre Einwilligung tatsächlich verweigern konnte, ohne Sanktionen zu erleiden, oder sie später zurückziehen konnte, falls sie ihre Meinung geändert hat. Dies kann vor allem im Fall der Einwilligung von Arbeitnehmern von Belang sein. Die Artikel-29-Datenschutzarbeitsgruppe führt dazu in ihrem Papier zur Auslegung von Artikel 26 Absatz 1 aus: „Das Erfordernis der Einwilligung kann also als vermeintlich gute Lösung erscheinen, die auf den ersten Blick einfach, in der Praxis jedoch komplex und schwerfällig ist“[11].

Die Arbeitsgruppe räumt ein, dass es Situationen geben kann, in denen der Betroffene Kenntnis von dem Rechtsstreit hat oder sogar daran beteiligt ist und somit seine Einwilligung als korrekte Grundlage für die Verarbeitung anzusehen ist.

Erforderlich für die Erfüllung einer rechtlichen Verpflichtung

Eine durch ein ausländisches Rechtssystem oder ausländische Vorschriften auferlegte Verpflichtung kann nicht als rechtliche Verpflichtung eingestuft werden, die eine Datenverarbeitung in der EU legitimieren würde. In einzelnen Mitgliedstaaten kann es jedoch eine rechtliche Vorschrift geben, einer Anordnung eines ausländischen Gerichts Folge zu leisten, mit der um Offenlegung ersucht wird.

In den Mitgliedstaaten, in denen keine derartige Verpflichtung besteht (z. B. wegen eines Vorbehalts aufgrund von Artikel 23 des Haager Beweisübereinkommens), kann Artikel 7 Buchstabe f dem für die Datenverarbeitung Verantwortlichen, der um Offenlegung im Rahmen des Discovery-Verfahrens ersucht wird, eine Handlungsgrundlage bieten.

Erforderlich zur Verwirklichung eines berechtigten Interesses

Die Erfüllung der Erfordernisse eines Gerichtsverfahrens kann für die Zwecke eines berechtigten Interesses von dem für die Verarbeitung Verantwortlichen oder Dritten für notwendig gehalten werden, denen die Daten gemäß Artikel 7 Buchstabe f übermittelt werden. Diese Grundlage ist nur akzeptabel, „sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen“.

Es käme zweifellos den Interessen der Justiz entgegen, wenn die Handlungsfähigkeit einer Organisation hinsichtlich der Förderung oder Verteidigung eines rechtmäßigen Anspruchs nicht unnötig eingeschränkt würde. Das Pre-trial-Discovery-Verfahren zielt darauf ab, für den Rechtsstreit potenziell relevante Informationen zu sichern und bereitzustellen. Jede Partei soll den Zugang zu solchen

[11] Siehe Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (WP 114), S. 11.

Informationen erhalten, die zur Unterstützung ihrer Forderung oder Verteidigung benötigt werden. Auf diese Weise soll für Fairness im Verfahren und ein gerechtes Ergebnis gesorgt werden.

Diese Ziele müssen allerdings gegen die Rechte und Freiheiten der betroffenen Person abgewogen werden, die – wie z. B. Mitarbeiter und Kunden – nicht unmittelbar am Rechtsstreit beteiligt ist und die nur deshalb einbezogen wird, weil ihre personenbezogenen Daten im Besitz einer Streitpartei sind und für die behandelten Fragen für erheblich erachtet werden.

Bei dieser Interessenabwägung sollten Aspekte der Verhältnismäßigkeit, die Relevanz der personenbezogenen Daten für den Rechtsstreit und die Konsequenzen für die betroffene Person berücksichtigt werden. Ferner müssen angemessene Garantien festgelegt werden und insbesondere müssen die Widerspruchsrechte der betroffenen Person nach Artikel 14 der Richtlinie anerkannt werden, wenn die Verarbeitung sich auf Artikel 7 Buchstabe f stützt und in Ermangelung anderslautender einzelstaatlicher Rechtsvorschriften zwingende legitime Gründe in Bezug auf die besondere Situation der betroffenen Person vorliegen.

Als ersten Schritt sollten die für die Verarbeitung Verantwortlichen die Offenlegung nach Möglichkeit auf anonymisierte oder zumindest pseudonymisierte Daten beschränken. Nach dem Herausfiltern irrelevanter Daten – möglicherweise durch eine vertrauenswürdige dritte Partei in der Europäischen Union – würden in einem zweiten Schritt personenbezogene Daten in einem sehr viel begrenzteren Umfang offen gelegt werden.

Sensible personenbezogene Daten und andere besondere Kategorien

Wenn es sich bei den betreffenden Informationen um sensible personenbezogene Daten handelt, muss gemäß Artikel 8 der Richtlinie eine Grundlage für die Verarbeitung gefunden werden. Ein angemessener Grund wäre die ausdrückliche Einwilligung der betroffenen Person nach Artikel 8 Buchstabe a oder die Notwendigkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche nach Artikel 8 Buchstabe e. In den einzelnen Mitgliedstaaten kann es spezifische Erfordernisse hinsichtlich der Verarbeitung und Übermittlung personenbezogener Daten nach Übersee geben, die der für die Verarbeitung Verantwortliche erfüllen muss.

Datenschutz ist nicht die einzige Frage, die sich im Zusammenhang mit der Verwendung personenbezogener Daten eines Individuums stellt. Geht es beispielsweise bei den angeforderten personenbezogenen Daten um Gesundheitsdaten, so können sie der ärztlichen Schweigepflicht unterliegen. Weitere Geheimhaltungserfordernisse oder Verpflichtungen zur Vertraulichkeit können aufgrund des Beichtgeheimnisses oder der anwaltlichen Schweigepflicht bestehen. Darüber

hinaus kann ein Rechtsschutz für bestimmte Informationsarten gelten, z. B. in Gestalt der Datenschutzrichtlinie für die elektronische Kommunikation. In einem solchen Fall ist es möglicherweise nicht fair oder rechtmäßig, diese personenbezogenen Daten in einer Weise zu verarbeiten, die mit den übrigen Verpflichtungen nicht vereinbar ist. Nicht zuletzt können Verstöße gegen das Fernmeldegeheimnis in einer Reihe von Mitgliedstaaten zu strafrechtlichen Sanktionen führen.

Verhältnismäßigkeit

Nach Artikel 6 der Richtlinie müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet sowie für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise verwendet werden. Personenbezogene Daten müssen dem Zweck entsprechen, für den sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen.

Bei der Offenlegung in Verbindung mit der vorprozessualen Beweiserhebung besteht ein Dilemma zwischen dem Bedürfnis der Parteien, alle Informationen zu erhalten, bevor ihre Rechtserheblichkeit in der Streitsache feststeht, und den Rechten der Betroffenen, deren personenbezogene Daten Teil der für das Verfahren angeforderten Informationen sind.

Aus den amerikanischen Zivilprozessregeln und den Grundsätzen der Sedona-Konferenz ergibt sich eindeutig, dass sowohl das US-Recht als auch die Rechtssysteme in der EU dem Verhältnismäßigkeitsprinzip und dem Ausgleich der verschiedenen Interessen Bedeutung beimessen.

Die für die Verarbeitung Verantwortlichen, die an einem Rechtsstreit beteiligt sind, sind verpflichtet, geeignete Vorkehrungen zu treffen (im Hinblick auf die Sensibilität der betreffenden Daten sowie auf alternative Informationsquellen), um die Offenlegung personenbezogener Daten auf die Daten zu beschränken, die für die zur Verhandlung anstehenden Fragen objektiv erheblich sind. Dieses „Filtern“ erfolgt in mehreren Phasen: zunächst wird festgestellt, welche Informationen für den Rechtsstreit relevant sind, dann wird geprüft, inwieweit diese Informationen personenbezogene Daten enthalten. Sind personenbezogene Daten betroffen, muss der für die Verarbeitung Verantwortliche abwägen, ob es erforderlich ist, dass die personenbezogenen Daten vollständig verarbeitet werden, oder ob sie beispielsweise in einer stärker anonymisierten oder überarbeiteten Form vorgelegt werden können. Wenn die Identität der betroffenen Person für den Streitgegenstand nicht relevant ist, besteht keine Notwendigkeit, eine solche Information in erster Instanz bereitzustellen. Diese kann allerdings in einer späteren Phase vom Gericht angefordert werden, was zu einer weiteren „Filterung“

führen kann. In den meisten Fällen wird es ausreichen, die personenbezogenen Daten pseudonymisiert, d. h. mit anderen Identifikatoren als dem Namen der betroffenen Person, zu übermitteln.

Wenn personenbezogene Daten benötigt werden, sollte die „Filterung" in dem Land vorgenommen werden, in dem sich die personenbezogenen Daten befinden, und zwar bevor die für den Rechtsstreit relevanten Daten in einen Drittstaat übermittelt werden.

Die Arbeitsgruppe räumt ein, dass es wegen der strengen Fristen, die aufgrund der amerikanischen Zivilprozessregeln für die Offenlegung der angeforderten Informationen gelten, schwierig werden kann, eine geeignete Person zu bestimmen, die beurteilen kann, welche Informationen für den Rechtsstreit relevant sind. Es liegt auf der Hand, dass es sich um eine Person handeln muss, die mit dem ausländischen Streitverfahren hinreichend vertraut ist.

Hierzu muss möglicherweise auf die Dienste eines vertrauenswürdigen Dritten in einem Mitgliedstaat zurückgegriffen werden, der in dem Rechtsstreit keine Rolle spielt, aber über ein ausreichendes Maß an Unabhängigkeit und Vertrauenswürdigkeit verfügt, um korrekt bestimmen zu können, welche personenbezogenen Daten relevant sind.

Die Arbeitsgruppe fordert die Streitparteien auf, die Datenschutzbeauftragten so früh wie möglich in das Pre-trial-Discovery-Verfahren (einschließlich der Datensicherung für Prozesszwecke) einzubeziehen. Sie möchte ferner die für die Verarbeitung Verantwortlichen in der EU ermutigen, an die amerikanischen Gerichte heranzutreten, um die ihnen obliegenden Datenschutzverpflichtungen zu erläutern, und die US-Gerichte um Schutzmaßnahmen zu ersuchen, um die Datenschutzauflagen in der EU und den Mitgliedstaaten zu erfüllen. Wie der Oberste Gerichtshof im Aérospatiale-Fall hervorhob, sollten amerikanische Gerichte bei vorprozessualen Verfahren besondere Sorgfalt darauf verwenden, ausländische Streitparteien vor der Gefahr zu schützen, dass sie durch eine unnötige oder unverhältnismäßig aufwändige Offenlegung benachteiligt werden[12].

Transparenz

In den Artikeln 10 und 11 der Richtlinie geht es um die Informationen, die die betroffene Person erhalten sollte.

Im Kontext des Discovery-Verfahrens bedeutet dies, dass die betroffene Person vorab davon in Kenntnis gesetzt wird, dass generell die Möglichkeit besteht, dass ihre personenbezogenen Daten für einen Rechtstreit verarbeitet werden könnten.

[12] 482 U.S. 522, 546 (Nr. 15, 16a).

Werden die personenbezogenen Daten dann tatsächlich für einen Rechtsstreit verarbeitet, sind die Identität aller Empfänger, die Zweckbestimmung der Verarbeitung, die Kategorien der betreffenden Daten und die diesbezüglichen Rechte mitzuteilen.

Nach Artikel 11 sind betroffene Personen darüber zu unterrichten, wenn personenbezogene Daten nicht unmittelbar bei ihnen, sondern bei Dritten erhoben werden. Dies kommt wahrscheinlich häufig vor, wenn personenbezogene Daten sich im Besitz einer der Streitparteien oder einer Tochtergesellschaft oder eines Mitglieds einer solchen Streitpartei befinden.

In diesen Fällen sollten die betroffenen Personen vom für die Verarbeitung Verantwortlichen informiert werden, sobald dies vernünftigerweise nach Verarbeitung der Daten möglich ist. Gemäß Artikel 14 besitzt die betroffene Person ferner ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten, wenn sich die Legitimität der Verarbeitung auf Artikel 7 Buchstabe f stützt und der Widerspruch aus überwiegenden, schutzwürdigen, aus der besonderen Situation der Person ergebenden Gründen erfolgt.

In der Stellungnahme der Artikel-29-Datenschutzgruppe zu internen Verfahren zur Meldung mutmaßlicher Missstände[13] ist allerdings eine Ausnahme von dieser Regel vorgesehen, wenn das erhebliche Risiko besteht, dass eine solche Mitteilung die Fähigkeit der Streitpartei zur wirksamen Untersuchung der Sache oder zur Sammlung der erforderlichen Beweismittel gefährden würde. In einem solchen Fall kann die Unterrichtung der betroffenen Person so lange aufgeschoben werden, wie dieses Risiko besteht; das soll dazu dienen, die Vernichtung oder Veränderung von Beweismitteln durch diese Person zu verhindern und somit Beweismittel zu sichern. Diese Ausnahme muss restriktiv und fallbezogen angewandt werden.

Rechte auf Auskunft, Berichtigung und Löschung von Daten

Nach Artikel 12 der Richtlinie hat jede betroffene Person das Recht auf Zugang zu den sie betreffenden Daten, um ihre Richtigkeit zu überprüfen und sie zu berichtigen, falls sie unrichtig, unvollständig oder überholt sind. Der in der EU für die Verarbeitung Verantwortliche hat sicherzustellen, dass die Rechte des Einzelnen auf Auskunft sowie auf Berichtigung unrichtiger, unvollständiger oder überholter personenbezogenen Daten vor der Übermittlung gewahrt werden.

Die Arbeitsgruppe schlägt vor, dass diese Verpflichtungen der Partei auferlegt werden, die die Informationen erhält. Dies könnte über eine gerichtliche Verfü-

[13] Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (WP 117 00195/06/DE).

gung (Protective Order) erreicht werden. Das hätte den Vorteil, dass einer betroffenen Person die Überprüfung der personenbezogenen Daten ermöglicht würde und sie sich selbst davon überzeugen könnte, dass die Datenübermittlung nicht unverhältnismäßig ist.

Einschränkungen dieser Rechte sind nur aufgrund von Artikel 13 und nur im Einzelfall möglich, wenn beispielsweise die Rechte und Freiheiten anderer Personen geschützt werden müssen. Die Arbeitsgruppe stellt klar, dass die Rechte der betroffenen Person während des Gerichtsverfahrens weiter gelten und es keinen allgemeinen Verzicht auf Auskunfts- oder Änderungsrechte gibt.

Es ist allerdings darauf hinzuweisen, dass sich aus diesen Rechten ein Konflikt mit den prozessualen Anforderungen ergeben könnte, zu einem bestimmten Zeitpunkt fixierte Daten aufzubewahren, da Datenänderungen (wenn auch nur für Berichtigungszwecke) eine Änderung der Beweismittel in der Streitsache bewirken würden.

Datensicherheit

Gemäß Artikel 17 der Richtlinie führt der für die Verarbeitung Verantwortliche alle geeigneten technischen und organisatorischen Maßnahmen durch, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust und die unberechtigte Weitergabe oder den unberechtigten Zugang erforderlich sind. Diese Maßnahmen müssen in einem angemessenen Verhältnis zu der Untersuchung der entsprechend den Sicherheitsvorschriften der einzelnen Mitgliedstaaten angesprochenen Fragen stehen. Diese Auflagen sollen nicht nur für den für die Verarbeitung Verantwortlichen gelten, sondern auch für Anwaltskanzleien, die mit der Streitsache befasst sind, sowie für Personen, die ihnen zuarbeiten, und alle anderen Experten, die an der Sammlung oder Überprüfung der Informationen beteiligt sind. Gleiches gilt für die Gerichte, da ein Großteil der relevanten personenbezogenen Daten, die für den Ausgang des Verfahrens erheblich sind, bei ihnen aufbewahrt werden.

Externe Dienstleister

Werden externe Dienstleister beispielsweise als sachverständige Zeugen im Streitverfahren eingesetzt, so bleibt der für die Verarbeitung Verantwortliche für die entsprechenden Verarbeitungen zuständig, da diese Dienstleister im Sinne der Richtlinie als Verarbeiter tätig sind.

Die externen Dienstleister müssen ebenfalls die Grundsätze der Richtlinie beachten. Sie haben sicherzustellen, dass die Informationen gemäß den Grundsätzen der Richtlinie gesammelt und verarbeitet werden und dass sie lediglich für die spezifische Zweckbestimmung verarbeitet werden, für die sie erhoben wurden.

Sie müssen sich insbesondere an die strikten Vertraulichkeitsbestimmungen halten und dürfen die verarbeiteten Informationen nur an bestimmte Personen weitergeben. Sie haben ferner die Aufbewahrungsfristen einzuhalten, die für den für die Verarbeitung Verantwortlichen gelten. Der für die Verarbeitung Verantwortliche muss auch regelmäßig überprüfen, ob die externen Dienstleister die Bestimmungen der Richtlinie einhalten.

Übermittlungen in Drittländer

Wenn personenbezogene Daten in Drittländer übermittelt werden, finden die Artikel 25 und 26 der Richtlinie Anwendung.

Gewährleistet das Drittland, in das die Daten übermittelt werden sollen, kein angemessenes Schutzniveau im Sinne von Artikel 25, so können die Daten unter folgenden Voraussetzungen übermittelt werden:

(1) Der Empfänger der personenbezogenen Daten ist ein Unternehmen mit Sitz in den USA, das die Grundsätze des „sicheren Hafens" (Safe Harbour Scheme) angenommen hat.

(2) Der Empfänger hat mit dem EU-Unternehmen, das die Daten übermittelt, einen Übermittlungsvertrag geschlossen, in dem das EU-Unternehmen ausreichende Garantien bietet, beispielsweise auf der Grundlage der Standardvertragsklauseln der Europäischen Kommission in ihren Entscheidungen vom 15. Juni 2001 oder vom 27. Dezember 2004.

(3) Der Empfänger hat verbindliche unternehmensinterne Datenschutzregelungen (BCR) eingeführt, die von den zuständigen Datenschutzstellen genehmigt wurden.

Handelt es sich bei der Übermittlung personenbezogener Daten für einen Rechtsstreit voraussichtlich um eine einzige Übermittlung aller relevanten Informationen, wäre ein möglicher Verarbeitungsgrund nach Artikel 26 Absatz 1 Buchstabe d der Richtlinie gegeben, wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich oder gesetzlich vorgeschrieben ist. Im Falle der Übermittlung einer signifikanten Datenmenge sollte die Anwendung der BCR oder der Grundsätze des „sicheren Hafens" in Betracht gezogen werden. Die Arbeitsgruppe bekräftigt jedoch ihre frühere Stellungnahme, dass Artikel 26 Absatz 1 Buchstabe d nicht zur Rechtfertigung der Übermittlung der Datensätze aller Angestellten der Muttergesellschaft für den Fall herangezogen werden kann, dass eines Tages ein Gerichtsverfahren in den USA angestrengt werden könnte[14].

[14] WP 114, S. 15.

Die Arbeitsgruppe erkennt an, dass ein Rechtshilfeersuchen auf der Grundlage des Haager Übereinkommens eine formelle Grundlage für die Übermittlung personenbezogener Daten darstellt, doch haben nicht alle Mitgliedstaaten das Haager Übereinkommen unterzeichnet und die, die es unterzeichnet haben, haben unter Umständen einen Vorbehalt erklärt.

Möglicherweise bestehen Bedenken aufgrund der möglichen Dauer eines solchen Rechtshilfeverfahrens, doch kennen sich die Gerichte, beispielsweise in den Vereinigten Staaten, mit der Anwendung des Haager Übereinkommens aus und können entsprechende Fristen im Streitverfahren berücksichtigen. Wo die Anwendung des Haager Übereinkommens möglich ist, fordert die Arbeitsgruppe, die Übermittlung von Informationen für prozessuale Zwecke zuerst auf der Grundlage des Übereinkommens in Erwägung zu ziehen.

Fazit

Dieses Arbeitspapier stellt eine erste Betrachtung der Übermittlung personenbezogener Daten zur Verwendung in grenzübergreifenden zivilrechtlichen Verfahren dar. Es ist als Einladung an alle Beteiligten, ausländische Gerichte und sonstige Akteure gedacht, sich an einer öffentlichen Konsultation zu beteiligen und in einen Dialog mit der Arbeitsgruppe einzutreten.

Brüssel, den 11.2.2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK

Stellungnahme 3/2009 über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter) (WP 161)

Angenommen am 5. März 2009

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

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

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

I. Einleitung

Unternehmen und Datenschutzbehörden haben mehrere Jahre lang mit den am 27. Dezember 2001[2] durch die Europäische Kommission angenommenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter, Entscheidung 2002/16/EG) gearbeitet.

Obgleich die Standardvertragsklauseln gemäß Entscheidung 2002/16/EG eine solide Grundlage für die Übermittlung personenbezogener Daten darstellen, wird seit mehreren Jahren der Ruf nach einer Aktualisierung immer lauter.

Der Hauptgrund für Überlegungen zur Aktualisierung der Standardvertragsklauseln gemäß Entscheidung 2002/16/EG kann vereinfacht mit der Entwicklung des

[1] ABl. 281 vom 23.11.1995, S. 31. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML

[2] ABl. L 6 vom 10.1.2002, S. 52. Siehe Stellungnahme der Arbeitsgruppe Nr.°7/2001, WP 47, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp47de.pdf

„globalen Outsourcing“ erklärt werden. Da Unternehmen ihre Daten immer häufiger nicht nur an einen Auftragsverarbeiter, sondern an „Unterauftragsverarbeiter“ übermitteln, die sie manchmal wiederum an „Unter-Unterauftragsverarbeiter“ weiterübermitteln, sind die Standardvertragsklauseln gemäß Entscheidung 2002/16/EG kein Instrument für die Bewältigung solch komplexer Weiterleitungsprozesse. Daher erachtet die Europäische Kommission eine Änderung der Standardvertragsklauseln gemäß Entscheidung 2002/16/EG durch eine neue Entscheidung auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG für erforderlich, um Verträge besser an die aktuellen Geschäftsvorgänge anpassen zu können.

II. Stellungnahme zum Entwurf einer Entscheidung der Kommission

1. Wesentliche Punkte

1.1. Vergabe an Unterauftragsverarbeiter innerhalb der EU vs. Vergabe an Unterauftragsverarbeiter außerhalb der EU

Die Datenschutzgruppe möchte Stellung nehmen zur internationalen Unterauftragsvergabe durch in der Europäischen Union/im EWR ansässige Auftragsverarbeiter an außerhalb des EWR ansässige Unterauftragsverarbeiter – ein Aspekt, der im Entwurf der Entscheidung der Kommission nicht enthalten ist, jedoch tatsächlich eine immer gängigere Praxis darstellt.

Die Datenschutzgruppe ist sich bewusst, dass die Verarbeitungsdienste hinsichtlich der Genehmigung nach Artikel 26 Absatz 2 der Richtlinie durch Annahme dieses Entscheidungsentwurfs wesentlich flexibler gestaltet werden könnten. Jedoch würde diese Flexibilität nicht gleichermaßen für alle Akteure eines immer globaleren Marktes gelten. Tatsächlich wäre es gemäß dem Entscheidungsentwurf der Kommission einem Auftragsverarbeiter in einem Drittland bereits bei Vorliegen einer Genehmigung des für die Verarbeitung Verantwortlichen möglich, Daten zur Verarbeitung an einen Unterauftragnehmer weiterzuleiten, während Auftragsverarbeiter innerhalb der EU/des EWR, die Teile ihrer Datenverarbeitung an Unterauftragnehmer in Drittländern übertragen möchten, weiterhin gemäß den aktuell geltenden Bestimmungen vorgehen müssten. Hierdurch könnten für europäische Unternehmen Wettbewerbsnachteile entstehen, da sie größere verwaltungstechnische Hindernisse überwinden müssten als ihre Konkurrenten in Drittländern, um als Dienstleister vergleichbare Verarbeitungsleistungen erbringen zu können.

Die Datenschutzgruppe kann jedoch die unterschiedliche Rechtsnatur von innergemeinschaftlichen und internationalen Datenübermittlungen nicht außer Acht

lassen. Dem wird in der Richtlinie, die diese Punkte in zwei verschiedenen Abschnitten regelt, Rechnung getragen.

Daher hält es die Datenschutzgruppe für erforderlich, eine rechtliche Lösung zu finden, die die internationale Unterauftragsvergabe durch innerhalb der EU/des EWR ansässige Auftragsverarbeiter ermöglicht, ohne dass es zu unnötigen Ungleichheiten am Markt kommt. Die Datenschutzgruppe fordert deshalb die Kommission auf, unverzüglich ein neues eigenständiges Rechtsinstrument zu schaffen, dass es innerhalb der EU ansässigen Auftragsverarbeitern ermöglicht, Aufträge international an Unterauftragsverarbeiter in Drittländern zu vergeben. Ein solches Instrument könnte zum Beispiel durch neue Standardvertragsklauseln geschaffen werden, mit welchen die in der EU/im EWR ansässigen für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter Unteraufträge in Drittländern vergeben und die für die Datenübermittlungen notwendigen und angemessenen Garantien gewährleisten könnten.

Die Datenschutzgruppe ist sich bewusst, dass die Erarbeitung eines solchen Instruments zeitaufwändig sein kann. Solange es dieses Instrument nicht gibt, muss die grenzüberschreitende Unterauftragsvergabe von Datenverarbeitungsleistungen durch Auftragsverarbeiter, die in der EU/im EWR ansässig sind, durch die nationalen Kontrollstellen geregelt werden. Unbeschadet der Rechte und Pflichten der nationalen Kontrollstellen, die in Artikel 26 Absatz 2 der Richtlinie vorgesehenen Genehmigungen gemäß ihrer innerstaatlichen Gesetzgebung zu erteilen, ermutigt die Datenschutzgruppe diese, bei im Rahmen einer internationalen Unterauftragsvergabe zwischen dem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter innerhalb der EU/des EWR geschlossenen Verträgen die analoge Anwendung der Prinzipien und Garantien der Standardvertragsklauseln als angemessene Garantien zu erachten. Verträge, die zwischen einem in der EU/dem EWR ansässigen Verantwortlichen für die Datenverarbeitung und einem ebenfalls dort ansässigen Datenverarbeiter geschlossen werden und mit denen der für die Datenverarbeitung Verantwortliche die Datenübermittlung an einen außerhalb der EU/des EWR ansässigen Unterauftragnehmer genehmigt, sollten also von den nationalen Datenschutzbehörden als Verträge erachtet werden, die den betroffenen Personen, deren Daten übermittelt werden, angemessenen Schutz bieten, wenn die Prinzipien und Garantien der Standardvertragsklauseln gemäß Entscheidung 2002/16/EG analog angewendet werden. Dies würde zu einer ähnlichen Regelung führen, wie sie der Entscheidungsentwurf der Kommission für außerhalb der EU ansässige Auftragsverarbeiter vorsieht.

Die Datenschutzgruppe bittet die Kommission zu prüfen, ob in die Kommissionsentscheidung zu den Standardvertragsklauseln eine erläuternde Erklärung und beispielsweise entsprechende Erwägungsgründe in die Entscheidung aufgenommen werden könnten, durch die es den Mitgliedstaaten ausdrücklich ermöglicht wird, auf der Grundlage der im Anhang der Kommissionsentscheidung auf-

geführten Standardvertragsklauseln Daten international an außerhalb der EU/des EWR ansässige Auftragsverarbeiter zu übermitteln, wenn sowohl der für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter innerhalb der EU/des EWR ansässig ist.

Hier sollte auch Erwähnung finden, dass es sinnvoll ist, diese Art der Unterauftragsvergabe nach einem Genehmigungsverfahren vorzunehmen, das mit dem für Auftragsverarbeiter außerhalb der EU/des EWR geltenden Verfahren identisch ist.

1.2. Mehrstufige Unterauftragsvergabe

Die Datenschutzgruppe ist sich bewusst, dass die Standardvertragsklauseln an die neue grenzübergreifende Dimension der Verarbeitung personenbezogener Daten angepasst werden müssen – insbesondere in Anbetracht der weit verbreiteten Unterauftragsvergabe bestimmter Verarbeitungsprozesse.

Die Datenschutzgruppe nimmt in diesem Zusammenhang zur Kenntnis, dass in den Standardvertragsklauseln „vom für die Verarbeitung Verantwortlichen zum Verarbeiter“ eine Klausel für die Unterauftragsvergabe eingefügt wurde, die mit dem Verfahren übereinstimmt, das in dem in Klausel 11 erwähnten Dokument vorgesehen ist (d.h.: schriftliche Vereinbarung zwischen Datenimporteur und Unterauftragnehmer, beruhend auf der vorherigen schriftlichen Einwilligung des Datenexporteurs und entworfen nach dem Vorbild der Standardvertragsklausel „vom für die Verarbeitung Verantwortlichen zum Verarbeiter“).

Die Unterauftragsvergabe von Verarbeitungsprozessen besteht hauptsächlich darin, in Drittländern ansässige Stellen als Datenverarbeiter zu benennen. Die betreffenden Drittländer sehen oftmals keine angemessenen Garantien vor, und die verarbeiteten Daten unterliegen darüber hinaus den dortigen Rechtsvorschriften.

Gleichzeitig ersucht die Datenschutzgruppe die Kommission, sorgfältig abzuwägen, ob es sinnvoll ist, auch Unterauftragsnehmern zu gestatten, ihrerseits Aufträge weiterzuvergeben; dies betrifft besonders Fälle, in denen sensible Daten verarbeitet werden oder Verarbeitungsprozesse mit bestimmten Risiken für die betroffenen Personen verbunden sind (z. B. biometrische Daten, genetische Informationen, justizielle Daten, Finanzdaten, Daten zu Kindern, Profilerstellung).

Dies hätte zur Folge, dass es lange Ketten von Unterauftragnehmern gibt, die möglicherweise unabhängig von den Anweisungen des für die Datenverarbeitung Verantwortlichen handeln; darüber hinaus wäre es schwierig, die Übersicht über alle Unterauftragnehmer zu behalten, besonders bei der Festlegung der ihnen jeweils obliegenden Aufgaben und Pflichten.

In ihrer Arbeitsunterlage „Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer“ legte die Datenschutzgruppe dar, dass Weiterübermittlungen an Gremien oder Organisationen, die nicht durch den Vertrag gebunden sind, vertraglich explizit ausgeschlossen sein sollten, *es sei denn, es ist möglich, derartige beteiligte Dritte vertraglich auf die Einhaltung derselben Datenschutzgrundsätze zu verpflichten*. Dieses Ziel verfolgt der Entscheidungsentwurf der Kommission.[3]

Die Datenschutzgruppe ist sich der aktuellen organisatorischen Struktur der weltweiten Märkte mit ihren langen Ketten von Unterauftragnehmern als Bestandteil der internationalen geschäftlichen Strukturen bewusst.

In diesem Zusammenhang trägt ein System von Standardvertragsklauseln, das lediglich eine einzige Ebene von Unterauftragnehmern (vom Datenexporteur zu einem Unterauftragnehmer) vorsieht, den bestehenden geschäftlichen Möglichkeiten nicht Rechnung.

Entsprechend hat die Datenschutzgruppe beschlossen, der Einführung einer Mehrstufenklausel zur Unterauftragsvergabe unter der Bedingung zuzustimmen, dass geeignete Garantien geschaffen werden, um die betroffenen Personen vor den oben näher bezeichneten Risiken zu schützen.

Die Anwendung von Vertragsklauseln auf alle unterschiedlichen Ebenen der in Auftrag gegebenen Verarbeitungsprozesse wird eine größere Einheitlichkeit im Geschäftsverkehr zur Folge haben, da alle auf den Standardvertragsklauseln beruhenden Vergabeverträge von Verarbeitungsprozessen denselben Klauseln und Bestimmungen unterliegen. Darüber hinaus wird die gegenwärtige Situation verbessert, indem die Rechtssicherheit gestärkt wird, da Datenimporteure, die ihre Daten zur Verarbeitung an Unterauftragnehmer weiterleiten, nicht zwingend vorab eine schriftliche Einwilligung des für die Datenverarbeitung Verantwortlichen einholen und vertragliche Verpflichtungen auferlegen, die denselben Datenschutz gewährleisten wie die Standardvertragsklauseln.

Dieser Argumentation zufolge wäre die Überlegung sicher angemessen, dass eine Mehrstufenklausel zur Unterauftragsvergabe zulässig sein kann, wenn die Entscheidung zur Vergabe von Verarbeitungsprozessen an Unterauftragnehmer einhergeht mit einer genauen Bewertung der spezifischen Anforderungen und Merkmale der Prozesse, die eine solche Entscheidung rechtfertigen. Diese Bewertung muss besonders genau erfolgen, wenn es besonders viele Ebenen

[3] Dokument WP 9 vom 22. April 1998:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp9_de.pdf.

der Unterauftragsvergabe gibt; auch dem Grundsatz der Zweckbindung sollte besonders Rechnung getragen werden, um sicherzustellen, dass der ursprüngliche Zweck, aus dem der für die Datenverarbeitung Verantwortliche die Daten zur Verarbeitung an den Datenimporteur übermittelt hat, nicht durch die verschiedenen möglichen Unteraufträge verfremdet wird.

Unter dieser Prämisse ist ein Auftragsvergabesystem, in welchem viele Unterauftragnehmer in Folge mit Teilen der Verarbeitung betraut werden, eine interessante Option, die auch die Datenschutzgruppe unterstützen könnte, sofern vorab sichergestellt ist, dass die oben beschriebenen spezifischen technischen und organisatorischen Erfordernisse durch den für die Datenverarbeitung Verantwortlichen erfüllt werden. Diesbezüglich sollte der Datenexporteur auch organisatorisch für Lösungen sorgen, die den betroffenen Personen eine Ausübung ihrer Rechte (Auskunft, Berichtigung, Widerspruch, Löschung, etc.) erleichtern. Dies kann zum Beispiel bedeuten, dass für die betroffenen Personen eine zentrale Anlaufstelle benannt wird, um ihre Zugriffsrechte ausüben zu können (am Hauptsitz des für die Datenverarbeitung Verantwortlichen), oder dass klare Verfahren entwickelt werden, die allen Auftrag- und Unterauftragnehmern bekannt zu geben sind, um den betroffenen Personen auf Antrag Auskunft über die sie betreffenden Daten zu geben.

Die Datenschutzgruppe ist der Auffassung, dass Klausel 11 des Entscheidungsentwurfs der Kommission – Unterauftragsvergabe – die notwendigen Elemente enthält, um angemessen sicherzustellen, dass das durch die Standardvertragsklauseln gewährleistete Schutzniveau in der gesamten Abfolge der möglichen Auftragsvergabe sichergestellt ist. Darüber hinaus stellen Klausel 4 (Pflichten des Datenexporteurs) und Klausel 5 (Pflichten des Datenimporteurs) sicher, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dieses Schutzniveau auf allen Ebenen der Unterauftragsvergabe gewährleisten. Diesbezüglich schlägt die Datenschutzgruppe vor, dass neben der dem Datenimporteur (Verarbeiter) obliegenden Verpflichtung, dem Datenexporteur von jedem abgeschlossenen Untervergabevertrag eine Kopie zu übermitteln, auch der Datenexporteur eine aktualisierte Liste der einzelnen Auftrag- und Unterauftragnehmer der „Vertragskette“ führt.

Ebenso wichtig ist, dass die Datenschutzbehörden Datenimporteure und deren Unterauftragnehmer überprüfen können, um sicherzustellen, dass Vertragsklauseln eingehalten werden und das erforderliche Schutzniveau von allen Unterauftragnehmern gewährleistet wird, die an den Verarbeitungsprozessen der nach Maßgabe der Standardvertragsklauseln übermittelten personenbezogenen Daten beteiligt sind.

2. Weitere Punkte

2.1. Prüfungen

Die vorgeschlagenen Standardvertragsklauseln würden die Möglichkeit beinhalten, den Datenschutzbehörden die Befugnis einzuräumen, die gesamte Unterauftragsvergabekette zu überprüfen – den (die) für die Datenverarbeitung Verantwortlichen, den (die) Datenverarbeiter mit Unterauftragnehmer(n) – sowie, falls erforderlich, diese betreffende verbindliche Entscheidungen zu treffen. Daher empfiehlt die Datenschutzgruppe die Annahme von Klausel 8 (Zusammenarbeit mit Kontrollstellen).

2.2. Anwendbares Recht

Klausel 9 der geltenden Vertragsklauseln sieht vor, dass das Recht des Mitgliedstaats maßgebend ist, in dem der Datenexporteur ansässig ist. Um Rechtssicherheit und Kohärenz zu gewährleisten, sollte festgelegt werden, dass auch für mit Unterauftragnehmern geschlossene Verträge das Recht des Mitgliedstaates gelten sollte, in dem der Datenexporteur ansässig ist.

2.3. Folgen für die alten Klauseln

Im Entscheidungsentwurf der Kommission wird die Aufhebung der Entscheidung 2002/16/EG vorgeschlagen. Es stellt sich die Frage, ob die zwischen den in der EU/im EWR ansässigen Verantwortlichen und den Datenverarbeitern aus Drittländern unter Anwendung der Standardvertragsklauseln der Entscheidung 2002/16/EG geschlossenenÜbermittlungsverträge auch aufgehoben und somit in die neuen Vertragsklauseln („vom Verantwortlichen zum Verarbeiter“) übergeführt werden müssten. Die Notwendigkeit einer Anpassung aller bestehenden, auf der Grundlage der Vertragsklauseln der Kommissionsentscheidung 2002/16/EG geschlossenen Verträge wäre für die Betroffenen und die Datenschutzbehörden eine erhebliche und unverhältnismäßig hohe Belastung.

Die Beibehaltung der durch die Entscheidung 2002/16/EG genehmigten Vertragsklauseln ist aber vielleicht gegenüber der Neugenehmigung nicht unbedingt die bessere Lösung, da hierdurch Rechtsunsicherheit entstehen könnte.

Die Datenschutzgruppe empfiehlt, dass die Kommission Übergangsvorschriften in die Entscheidung (möglicherweise in Artikel 6) aufnimmt und damit dafür Sorge trägt, dass die auf der Grundlage der aufgehobenen Entscheidung 2002/16/EG genehmigten internationalen Übermittlungen so lange genehmigt bleiben, wie die in den ursprünglich unterzeichneten Vertragsklauseln dargeleg-

ten Übermittlungen und Datenverarbeitungen nicht abgeändert werden. Sollten die Unternehmen, die die „alten“ Klauseln verwenden, diese jedoch abändern oder Vereinbarungen zur Untervergabe einführen wollen, obliegt es ihnen, diese Klauseln abzuändern, sie mit den neuen Standardvertragsklauseln in Einklang zu bringen und gemäß der national geltenden Gesetzgebung eine neue Genehmigung zu beantragen.

Schlussfolgerung

Vorbehaltlich der vorangehenden Empfehlungen gibt die Arbeitsgruppe eine positive Stellungnahme zu dem Entwurf der Entscheidung der Kommission über Standardvertragsklauseln zur Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern ab. Sie fordert den Ausschuss nach Artikel 31 auf, seine Arbeiten fortzuführen, damit dieser Entscheidungsentwurf der Kommission angenommen werden kann.

Brüssel, den 5. März 2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK

Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163)

Angenommen am 12. Juni 2009

Inhalt

Zusammenfassung

Diese Stellungnahme stellt auf die Frage ab, wie das Betreiben sozialer Vernetzungs-Websites mit den Bestimmungen des Datenschutzrechts der EU in Einklang zu bringen ist. Sie soll vor allem den Anbietern sozialer Netzwerkdienste (SNS) eine Richtschnur zu den Maßnahmen bieten, die zwecks der Vereinbarkeit mit dem EU-Recht verwirklicht sein müssen.

Die Stellungnahme hält fest, dass es sich bei den Anbietern sozialer Netzwerkdienste und in vielen Fällen auch bei den Drittanbietern von Anwendungs- und Softwaredienstleistungen um „für die Datenverarbeitung Verantwortliche" mit entsprechenden Verpflichtungen gegenüber den Nutzern sozialer Netzwerkdienste handelt. Die Stellungnahme macht klar, dass sich viele Nutzer in einem rein persönlichen Lebensbereich bewegen, indem sie im Rahmen der Besorgung ihrer persönlichen oder familiären Angelegenheiten bzw. ihrer privaten Haushaltsführung Kontakte zu anderen Menschen knüpfen und unterhalten. In diesen Fällen ist nach der Stellungnahme davon auszugehen, dass die „Ausnahmeklausel für Privathaushalte betreffend persönliche oder familiäre Tätigkeiten natürlicher Personen" Anwendung findet und die Vorschriften für die „für die Verarbeitung Verantwortlichen" somit nicht gelten. Die Stellungnahme führt auch Umstände auf, unter denen die Tätigkeiten eines Nutzers eines sozialen Netzwerkdienstes nicht unter die „Ausnahmeklausel für Privathaushalte" fallen. Die Verbreitung und die Verwendung von Informationen, die über soziale Netzwerkdienste verfügbar sind, zu anderweitigen, sekundären und unbefugten Zwecken gehört zu den besorgniserregenden Sicherheitsbedenken der Artikel-29-Datenschutzgruppe. Die Gruppe tritt in ihrer Stellungnahme daher für robuste sicherheits- und datenschutzfreundliche Standardeinstellungen als idealem Ausgangspunkt für alle angebotenen Dienstleistungen ein. Im Mittelpunkt der wachsenden Besorgnis stehen die Zugriffsmöglichkeiten auf Informationen aus Nutzerprofilen. Ebenso behandelt werden Themen wie die Verarbeitung sensibler Daten und Bildmaterialien, die zielgerichtete Werbung und die Direktwerbung über soziale Netzwerkdienste und die Probleme im Zusammenhang mit der Vorratsspeicherung von Daten.

Die Empfehlungen stellen im Kern auf die Verpflichtungen der Anbieter von sozialen Netzwerkdiensten ab, im Einklang mit den Vorschriften der Datenschutzrichtlinie zu handeln und die Rechte der Nutzer aufrechtzuerhalten und zu stärken. Von ganz entscheidender Bedeutung ist, dass die Anbieter von sozialen Netzwerkdiensten ihre Nutzer von Anfang an über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung personenbezogener Daten verbinden. Besondere Sorgfalt sollten die Anbieter von sozialen Netzwerkdiensten bei der Verarbeitung personenbezogener Daten von Minderjährigen walten lassen. Die Stellungnahme empfiehlt allen Nutzern, Bilder bzw. Informationen über andere Personen nur mit der konkreten Einwilligung der jeweils betroffenen Person in ein soziales Netzwerksystem hochzuladen, und gibt auch den Anbietern von sozialen Netzwerkdiensten zu bedenken, dass sie in der Pflicht sind, ihre Nutzer im Hinblick auf die Rechte der anderen auf Schutz ihrer Privatsphäre aufzuklären.

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

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

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

gestützt auf Artikel 255 EG-Vertrag und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

Bei der Entwicklung der Netzgemeinschaften und Webdienste, die durch Web-Anwendungen beherbergt werden, wie den sozialen Netzwerkdiensten („SNS"), handelt es sich um ein relativ neues Phänomen, wobei die Zahl der Nutzer dieser Websites ständig exponentiell zunimmt.

Die persönlichen Informationen, die ein Nutzer dabei online bekannt gibt, in Verbindung mit den Daten, die seine Tätigkeiten und Interaktionen mit anderen Menschen nachzeichnen, können ein reichhaltiges Persönlichkeitsprofil von den Aktivitäten und Interessen dieser Person entstehen lassen. Die auf den Webportalen sozialer Netzwerke veröffentlichten personenbezogenen Daten lassen sich von unbefugten Dritten für sehr vielfältige Vorhaben und Zielsetzungen ausnutzen, so auch für kommerzielle Zwecke, und bergen in sich mitunter größere Gefahren und Risiken, wie z. B. Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts-oder Erwerbsmöglichkeiten und Beeinträchtigung der körperlichen Unversehrtheit.

Die Berliner „International Working Group on Data Protection in Telecommunications" (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation) hat im März 2008 das *„Rom-Memorandum"*[2] verabschiedet, in dem sie die

[1] ABl. L 281 vom 23.11.1995, S. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

durch die sozialen Netzwerke entstandenen Risiken für die Privatsphäre und die Sicherheit analysiert und Empfehlungen für Gesetzgeber, Anbieter und Nutzer gibt. Auch die jüngst angenommene Entschließung zum Datenschutz in sozialen Netzwerkdiensten[3] stellt auf die mit diesen Diensten (SNS) einhergehenden Herausforderungen ab. Die Arbeitsgruppe berücksichtigt auch das von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Oktober 2007 veröffentlichte Positionspapier *„Security Issues and Recommendations for Online Social Networks"*[4] *(Sicherheitsfragen und Empfehlungen für Soziale Online-Netzwerke)*, das sich an Gesetzgeber, Anbieter und Nutzer sozialer Netzwerke richtet.

2. Definition für „soziale Netzwerkdienste (SNS)" und Geschäftsmodell

Soziale Netzwerkdienste definiert man gemeinhin als Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen. Im rechtlichen Sinne handelt es sich bei den sozialen Netzwerken um Dienstleistungen der Informationsgesellschaft im Sinne des Artikels 1 Nr. 2 der Richtlinie 98/34/EG in der durch die Richtlinie 98/48/EG geänderten Fassung. Allen sozialen Netzwerkdiensten sind bestimmte Merkmale gemein:

– die Nutzer werden aufgefordert, personenbezogene Daten zur Erstellung einer Beschreibung von sich selbst bzw. eines selbst generierten persönlichen „Profils" anzugeben;

– soziale Netzwerkdienste bieten auch Funktionen an, mit denen die Nutzer ihr eigenes Material (selbst generierte Inhalte wie z. B. Bilder oder Tagebucheinträge, Musik- und Videoclips oder Links zu anderen Websites[5]) dort veröffentlichen können;

– die Nutzung der sozialen Netzwerke erfolgt über die jedem Nutzer bereitgestellten Funktionen samt Kontaktliste bzw. Adressbuch, mittels derer die Verweise auf die anderen Mitglieder der Netzgemeinschaft verwaltet und zu Interaktionen mit diesen genutzt werden können.

---

[3] Angenommen auf der 30. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg am 17. Oktober 2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_de.pdf

[4] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[5] Wenn der SNS auch elektronische Kommunikationsdienstleistungen bereitstellt, finden die Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) Anwendung.

Soziale Netzwerkdienste erwirtschaften einen Großteil ihrer Einnahmen aus der Werbung, die auf den eingerichteten Webseiten eingeblendet und von den Nutzern aufgerufen wird. Nutzer, die im Rahmen der persönlichen Profildaten große Informationsmengen über ihre Interessen veröffentlichen, bieten einen spezifisch bereinigten und fein abgestimmten Markt für Werbende, die auf der Grundlage dieser Informationen zielgerichtete Werbemaßnahmen ergreifen wollen.

Es ist daher wichtig, dass soziale Netzwerkdienste so funktionieren, dass die Rechte und Freiheiten der Nutzer beachtet werden, da diese die legitime Erwartung haben, dass die von ihnen offengelegten personenbezogenen Daten im Einklang mit dem europäischen und dem einzelstaatlichen Datenschutzrecht sowie der einschlägigen Gesetzgebung zum Schutz der Privatsphäre verarbeitet werden.

3. Anwendung der Datenschutzrichtlinie

Die Bestimmungen der Datenschutzrichtlinie gelten in den meisten Fällen auch für die Anbieter von sozialen Netzwerkdiensten, und zwar sogar dann, wenn ihr Hauptsitz außerhalb des EWR liegt. Für weitere Leitlinien zu der Frage, inwieweit die Datenschutzrichtlinie und die aufgrund der Verarbeitung von IP-Adressen und der Verwendung von Cookies zum Tragen kommenden Rechtsvorschriften auf die Einrichtung und Nutzung solcher Funktionen Anwendung finden, verweist die Artikel-29-Datenschutzgruppe auf ihre frühere Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen.[6]

3.1. Wer ist der „für die Datenverarbeitung Verantwortliche“?

Anbieter sozialer Netzwerkdienste (SNS)

Die Anbieter sozialer Netzwerkdienste sind die „für die Verarbeitung von Benutzerdaten Verantwortlichen“ im Sinne der Datenschutzrichtlinie. Denn sie stellen die Mittel für die Verarbeitung der Benutzerdaten und alle „Basisdienste“ für die Benutzerverwaltung (z. B. Registrierung und Löschung von Profil- und Verkehrsdaten) bereit. Sie bestimmen auch Art und Umfang der etwaigen Nutzung der Benutzerdaten zu Werbe- und Vermarktungszwecken – so auch durch dritte Werbeanbieter.

[6] WP148, „Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen“.

Anbieter von Anwendungs-/Softwaredienstleistungen

Auch Softwaredienstleister/Anwendungsanbieter können „für die Verarbeitung von Benutzerdaten Verantwortliche" sein, wenn sie Anwendungen entwickeln, die zusätzlich zu denen der sozialen Netzwerkdienste laufen und Nutzer sich zur Verwendung der betreffenden Anwendung entscheiden.

Nutzer

In den meisten Fällen sind die Nutzer als „betroffene Personen" anzusehen. Die Pflichten des „für die Verarbeitung Verantwortlichen" finden nach der Datenschutzrichtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person *„zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten"* vorgenommen wird – sog. „Ausnahmeklausel für Privathaushalte". Unter gewissen Umständen fallen die Tätigkeiten eines Nutzers eines sozialen Netzwerkdienstes nicht unter die „Ausnahmeklausel für Privathaushalte", wobei dann vom Nutzer zu vermuten ist, dass er gewisse Pflichten des „für die Verarbeitung Verantwortlichen" übernommen hat. Einige dieser Fälle werden weiter unten dargestellt:

3.1.1. Art und Zweck des sozialen Netzwerkdienstes (SNS)

Bei den sozialen Netzwerkdiensten gibt es einen zunehmenden Trend zum *„Übergang von der „Nutzung von Web 2.0 zum Vergnügen" hin zur Nutzung von Web 2.0 für Produktivitäts- und Dienstleistungszwecke"*[7], wobei die Aktivitäten einiger Nutzer sozialer Netzwerkdienste unter Umständen über die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten hinausgehen, so z. B., wenn der soziale Netzwerkdienst als Anwendungsplattform für die Zusammenarbeit eines Verbands, einer Gesellschaft oder eines Unternehmens genutzt wird. Handelt ein Nutzer eines sozialen Netzwerkdienstes für einen Verband, eine Gesellschaft oder ein Unternehmen oder nutzt er den sozialen Netzwerkdienst hauptsächlich als Anwendungsplattform zur Förderung kommerzieller, politischer oder karitativer Zielsetzungen, so findet die Ausnahmeklausel keine Anwendung. Hier übernimmt der Nutzer die volle Verantwortung als „für die Verarbeitung Verantwortlicher", der einem anderen „für die Verarbeitung Verantwortlichen", nämlich dem sozialen Netzwerkdienst, und Dritten (anderen Nutzern des sozialen Netzwerkdienstes oder potenziell sogar anderen „für die Verarbeitung Verantwortlichen" mit Zugriffsmöglichkeiten auf die betreffenden Daten) personenbezogene Daten offenlegt. Unter diesen Umständen benötigt der Nutzer die

[7] „Internet of the future: Europe must be a key player" („Das Internet der Zukunft: Europa muss ein Leitakteur sein"), Rede von Frau Reding, Mitglied der Europäischen Kommission, zuständig für Informationsgesellschaft und Medien, am 2. Februar 2009 in Brüssel auf der Tagung zur Zukunft der Internetinitiative des Europäischen Rates von Lissabon.

Einwilligung der betroffenen Personen oder eine sonstige rechtliche Grundlage im Sinne der Datenschutzrichtlinie.

Typischerweise ist der Zugriff auf die von einem Nutzer beigetragenen Daten (Profildaten, publizierte Einträge, Darstellungen und Berichte…) auf die von ihm selbst ausgewählten Kontakte begrenzt. In gewissen Fällen kann ein Nutzer jedoch zu einer hohen Anzahl von Drittkontakten gelangen, von denen er einige unter Umständen gar nicht kennt. Eine hohe Anzahl von Kontakten könnte ein Anhaltspunkt dafür sein, dass die „Ausnahmeklausel für Privathaushalte" keine Anwendung findet und der Nutzer daher als „für die Verarbeitung Verantwortlicher" anzusehen ist.

3.1.2. Zugriff auf Nutzerprofilinformationen

Zum Schutz der Privatsphäre sollten sie sozialen Netzwerkdienste funktionstüchtige datenschutzfreundliche und unentgeltliche Standardeinstellungen sicherstellen, die die Zugriffsmöglichkeiten auf die vom Nutzer selbst ausgewählten Kontakte beschränken.

Reichen die Zugriffsmöglichkeiten auf Profilinformationen über die vom Nutzer selbst ausgewählten Kontakte hinaus, so z. B., wenn allen Mitgliedern des sozialen Netzwerks Zugriff auf ein Profil gewährt wird[8], oder wenn die betreffenden Daten von externen Suchmaschinen indexiert werden können, so geht der Zugriff über die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten hinaus. Ebenso kommen alle Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen zur Geltung, wenn ein Nutzer in voller Kenntnis der Sachlage die Entscheidung trifft, die Zugriffsmöglichkeit über den Kreis der von ihm selbst ausgewählten „Freunde" hinaus auszudehnen. Effektiv tritt dieselbe Rechtswirkung ein, wenn eine andere Person anderweitige Anwendungsplattformen und -technologien/Programmierschnittstellen benutzt, um personenbezogene Daten im Web zu veröffentlichen[9]. In mehreren Mitgliedstaaten bedeutet der Mangel an Zugriffsbeschränkungen (und somit die öffentliche Eigenschaft), dass die Datenschutzrichtlinie in dem Sinne Anwendung findet, dass der Internetnutzer die Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen erhält[10].

---

[8] Bzw. wenn dargelegt werden kann, dass bei der Akzeptierung von Kontakten keine wirkliche Auswahl getroffen wird, d. h. die Nutzer „Kontakte" unabhängig davon akzeptieren, dass sie mit diesen wirklich in Verbindung stehen.

[9] So z. B. bei Publikationsplattformen, die selbst keine SNS sind, oder bei selbst beherbergten Softwareanwendungen.

[10] In seinem Urteil Satamedia hat der EuGH in Randnr. 44 im Umkehrschluss für Recht erkannt: *„Demzufolge ist diese zweite Ausnahme dahin auszulegen, dass mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Privatpersonen gehören (vgl. Urteil Lindqvist, Randnr. 47). Dies ist bei den Tätigkeiten von Markkinapörssi und Satamedia, durch die die erfassten Daten einer unbegrenzten Zahl von Personen zur Kenntnis gebracht werden sollen, offensichtlich nicht der Fall."*

Zu bedenken ist, dass auch dann, wenn die „Ausnahmeklausel für Privathaushalte“ nicht greift, der Nutzer sozialer Netzwerkdienste unter weitere Ausnahmeregelungen fallen kann, so beispielsweise unter die Ausnahme der Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt. In diesen Fällen ist die Freiheit der Meinungsäußerung gegen das Recht auf Privatsphäre abzuwägen.

3.1.3. Verarbeitung personenbezogener Daten Dritter durch den Nutzer

Die Anwendbarkeit der „Ausnahmeklausel für Privathaushalte“ ist auch durch die Notwendigkeit eingeschränkt, die Rechte Dritter zu gewährleisten, so insbesondere im Hinblick auf sensible Daten. Ferner ist darauf hinzuweisen, dass auch dann, wenn die „Ausnahmeklausel für Privathaushalte“ anwendbar ist, ein Nutzer nach den allgemeinen Bestimmungen des einschlägigen nationalen Zivil- oder Strafrechts zur Verantwortung gezogen werden kann (so z. B. bei Verleumdung/übler Nachrede: Schadensersatzpflicht wegen Verletzung der Persönlichkeitsrechte, strafrechtliche Verantwortlichkeit).

3.2. Sicherheits- und datenschutzfreundliche Standardeinstellungen

Die Datensicherheit bei der Informationsverarbeitung ist ein entscheidender Faktor für das Vertrauen in soziale Netzwerkdienste. Die für die Verarbeitung personenbezogener Daten Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen treffen, und zwar „sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Datenverarbeitung“, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern, wobei das Schutzniveau den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen sein muss[11].

Ein wichtiger Faktor der Vorgaben und Vorkehrungen zum Schutz der Privatsphäre sind die Zugriffsmöglichkeiten auf die in einem Nutzerprofil enthaltenen personenbezogenen Daten. Wenn es keinerlei Beschränkungen für solche Zugriffsmöglichkeiten gibt, können Dritte entweder als Mitglied des sozialen Netzwerks oder mithilfe von Suchmaschinen allerlei Arten von ganz persönlichen Details über die Nutzer miteinander verknüpfen und zueinander in Beziehung setzen. Bei der Anmeldung bei einem Netzwerkdienst nimmt jedoch nur eine Minderheit von Nutzern Veränderungen an den Standard- und Datenschutzeinstellungen vor. Daher sollten die sozialen Netzwerkdienste datenschutzfreundliche Standardeinstellungen anbieten, die eine Nutzerkontrolle ermöglichen, bei

[11] Artikel 17 und Erwägungsgrund 46 der Datenschutzrichtlinie.

der der Nutzer in jeden Zugriff auf seine Profildaten, der über seine selbst ausgewählten Kontakte hinausreicht, ausdrücklich und ohne Einschränkung einwilligen muss, um somit das Risiko der rechtswidrigen Verarbeitung seiner Daten durch Dritte zu verringern. Die Nutzerprofilinformationen mit beschränkten Zugriffmöglichkeiten sollten nicht durch interne Suchmaschinen aufgespürt werden können, so auch nicht mittels Suchfunktionen nach Parametern wie Alters- oder Ortsangaben. Es darf keine impliziten Entscheidungen über die Ausdehnung der Zugriffsmöglichkeiten geben[12], beispielsweise im Wege einer „Opt-out-Möglichkeit" durch den für die Verarbeitung Verantwortlichen des sozialen Netzwerkdienstes.

3.3. Informationspflichten des sozialen Netzwerkdienstes (SNS)

Die Anbieter sozialer Netzwerkdienste sollten ihre Nutzer nach Maßgabe des Artikels 10 der Datenschutzrichtlinie über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung von personenbezogenen Daten verbinden. Dazu gehört zumindest

– die Nutzung der Daten zu Zwecken der Direktwerbung;

– die etwaige gemeinsame Nutzung der Daten mit Dritten, die von ihrer Kategorie her näher zu bezeichnen sind;

– eine Übersicht über die Nutzerprofile: ihre Erstellung und die wichtigsten Datenquellen;

– der Umgang mit sensiblen Daten.

Die Datenschutzgruppe empfiehlt, dass

– die Anbieter sozialer Netzwerkdienste ihre Nutzer beim Hochladen von personenbezogenen Informationen ins soziale Netzwerkprofil angemessen auf die Sicherheitsrisiken für sich und andere in Bezug auf den Schutz der Privatsphäre hinweisen;

[12] Bericht und Empfehlungen zum Datenschutz in sozialen Netzwerkdiensten („Rom-Memorandum") weisen auf die Risiken hin, wie z. B. auf den „irreführenden Begriff der ‚Gemeinschaft'", S. 2, auf die Tatsache, „es könnten mehr personenbezogene Informationen weitergegeben werden als man denkt", S. 3. Eine Computersicherheitsfirma spricht gegenüber einem bedeutenden SNS eine Warnung in Bezug auf Standardzugriffsmöglichkeiten auf Mitglieder im selben geografischen Gebiet aus:
http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

– die Nutzer sozialer Netzwerkdienste daran erinnert werden, dass das Hochladen von personenbezogenen Informationen über andere Personen deren Rechte auf Privatsphäre und auf informationelle Selbstbestimmung verletzen kann;

– die Nutzer sozialer Netzwerkdienste von diesen darauf aufmerksam gemacht werden, Bilder oder Informationen über andere Personen nur mit Einwilligung der betroffenen Person hochzuladen[13].

3.4. Sensible Daten

Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben gelten als sensible Daten. Sensible personenbezogene Daten dürfen nur mit der ausdrücklichen Einwilligung des Betroffenen im Internet veröffentlicht werden, es sei denn die betroffene Person hat die Daten offenkundig selbst öffentlich gemacht.[14]

In einigen EU-Mitgliedstaaten gelten die Bilder von betroffenen Personen als spezielle Kategorie personenbezogener Daten, da sie zur Unterscheidung der rassischen/ethnischen Herkunft bzw. zur Herleitung religiöser Überzeugungen oder gesundheitlicher Daten verwendet werden können. Die Datenschutzgruppe betrachtet Bilder im Internet im Allgemeinen nicht als sensible Daten[15], es sei denn die Bilder werden eindeutig zur Offenlegung von sensiblen Daten über Personen verwendet.

Als für die Verarbeitung Verantwortliche dürfen die sozialen Netzwerkdienste keinerlei sensible Daten über Mitglieder und Nichtmitglieder des sozialen Netzwerks ohne deren ausdrückliche Einwilligung verarbeiten[16]. Nimmt ein sozialer Netzwerkdienst in sein Formular zum Nutzerprofil etwaige Fragen zu sensiblen Daten auf, so hat er eindeutig darauf hinzuweisen, dass die Beantwortung dieser Fragen ohne jede Einschränkung auf freiwilliger Basis erfolgt.

---

[13] Dies ließe sich durch die Einführung von Kennzeichnungs- und Steuerungssystemen auf den Websites der sozialen Netzwerke vereinfachen, z. B. indem man in einem persönlichen Profil Bereiche ausweist, in denen auf gekennzeichnete Bilder oder Videos hingewiesen wird, da sie mit dem Namen eines Nutzers versehen sind und daher auf seine Einwilligung zur Veröffentlichung warten, oder in denen Verfallsdaten für gekennzeichnete Bilder oder Videos gesetzt werden, die keine Einwilligung der betroffenen Person erhalten haben.

[14] Die Mitgliedstaaten können Ausnahmeregelungen erlassen; siehe Artikel 8 Absatz 2 Buchstabe a) 2. Halbsatz und Artikel 8 Absatz 4 der Datenschutzrichtlinie.

[15] Die Veröffentlichung von Bildern im Internet erregt jedoch immer mehr Besorgnis im Hinblick auf den Schutz der Privatsphäre, da die Technologien der Gesichtserkennung immer besser werden.

[16] Die Einwilligung muss frei, informiert und spezifisch erfolgen.

3.5. Verarbeitung von Daten von Nichtmitgliedern

Viele soziale Netzwerkdienste gestatten ihren Nutzern Beiträge mit Daten über andere Personen, wie z. B. das Hinzufügen des Namens der abgebildeten Person(en) zum jeweiligen Bild, die Bewertung von Personen, die Erfassung der „Personen, die ich auf Veranstaltungen getroffen habe/gerne treffen möchte". Diese Kennzeichnung kann auch Nichtmitglieder des Netzwerks kenntlich machen. Jedoch darf die Verarbeitung solcher Nichtmitgliederdaten durch den sozialen Netzwerkdienst nur erfolgen, wenn eines der in Artikel 7 der Datenschutzrichtlinie festgelegten Kriterien erfüllt ist.

Ferner bedarf es für die Generierung von vorgefertigten persönlichen Profilen von Nichtmitgliedern mithilfe der Aggregation der Daten, die von den Nutzern des sozialen Netzwerkdienstes unabhängig voneinander beigetragen wurden, einschließlich der Erstellung von Daten über persönliche Beziehungen oder sachliche Zusammenhänge, die aus hochgeladenen Adressbüchern hergeleitet werden, einer Rechtsgrundlage.[17]

Selbst wenn der soziale Netzwerkdienst Mittel und Wege hätte, um Kontakt mit dem Nichtnutzer aufzunehmen und ihn über das Vorhandensein personenbezogener Daten über ihn zu informieren, würde eine etwaige Einladung an ihn per E-Mail, den sozialen Netzwerkdienst zwecks Zugriffsmöglichkeit auf diese personenbezogenen Daten zu besuchen, gegen das Verbot für das Versenden unerbetener elektronischer Nachrichten zu Zwecken der Direktwerbung nach Artikel 13 Absatz 4 der Datenschutzrichtlinie für elektronische Kommunikation verstoßen.

3.6. Zugriffsmöglichkeiten durch Dritte

3.6.1. Über den sozialen Netzwerkdienst (SNS) vermittelte Zugriffsmöglichkeiten

Neben ihrer eigentlichen Dienstleistung bieten die meisten sozialen Netzwerkdienste ihren Nutzern auch noch Zusatzanwendungen an, die von dritten Software-Entwicklern über Anwendungsprogrammierschnittstellen bereitgestellt werden; diese Drittanbieter verarbeiten ebenfalls personenbezogene Daten.

Die sozialen Netzwerkdienste sollten über Mittel und Wege verfügen, mit denen sichergestellt werden kann, dass die Anwendungen von Drittanbietern im Ein-

[17] Nach Erwägungsgrund 38 der Datenschutzrichtlinie gilt Folgendes: *„Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden".* Für einige SNS ist die Veröffentlichung von persönlichen Profilen von Nichtmitgliedern angeblich zu einem wichtigen Standbein der Vermarktung ihrer „Dienstleistungen" geworden.

klang mit der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen. Dies bedeutet insbesondere, dass die Drittanbieter den Nutzern eindeutige und spezifische Informationen über die Verarbeitung ihrer personenbezogenen Daten an die Hand geben, und dass sie nur Zugriff auf die unbedingt notwendigen personenbezogenen Daten haben. Daher sollten die sozialen Netzwerkdienste Drittanbietern abgestufte Zugriffsmöglichkeiten anbieten, so dass diese für ein stärker eingeschränktes Zugriffsverfahren optieren können. Außerdem sollten die sozialen Netzwerkdienste sicherstellen, dass den Nutzern einfache Mechanismen zur Verfügung stehen, mit denen sie ihre Bedenken und Beschwerden über die Anwendungen von Drittanbietern geltend machen können.

3.6.2. Über den Nutzer vermittelte Zugriffsmöglichkeiten Dritter

Die sozialen Netzwerkdienste gestatten ihren Nutzern manchmal den Zugriff und die Aktualisierung ihrer Daten mithilfe anderer Anwendungen. So können Nutzer mitunter

– von ihrem Mobiltelefon aus Nachrichten an das Netzwerk lesen und versenden;

– auf einem Desktop-PC die Kontaktdaten ihrer Freunde im sozialen Netzwerk mit ihrem Adressbuch synchronisieren;

– mittels einer anderen Website ihren Status oder Standort im sozialen Netzwerk automatisch aktualisieren.

Die sozialen Netzwerkdienste veröffentlichen Angaben dazu, wie die Software in Form einer „Anwendungsprogrammierschnittstelle" („API") beschaffen sein soll. Aufgrund dieser Informationen können Drittanbieter die Software für die Ausführung der betreffenden Aufgaben entwickeln und die Nutzer zwischen mehreren Drittanbietern frei auswählen[18]. Wird eine API angeboten, die den Zugriff auf Kontaktdaten ermöglicht, so sollte der soziale Netzwerkdienst

– für ein Granularitätsniveau sorgen, bei dem der Nutzer die Mindestzugriffsebene für den Dritten bestimmen kann, die gerade noch zur Durchführung einer bestimmten Aufgabe ausreicht.

Wird im Namen des Nutzers über die API eines Dritten auf personenbezogene Daten zugegriffen, so sollte der Drittanbieter

[18] Während es sich bei „API" um einen allgemeinen technischen Begriff handelt, ist unter API hier der Zugriff im Namen des betreffenden Nutzers gemeint, d. h. der Nutzer muss der Software seine Log-in-Berechtigung bekannt geben, damit diese in seinem Namen aktiv werden kann.

– die betreffenden Daten nicht länger verarbeiten und speichern als dies zur Ausführung der betreffenden Aufgabe nötig ist;

– außer der persönlichen Nutzung durch den Nutzer, der den Beitrag geleistet hat, keinerlei Bearbeitungen an den vom Nutzer eingebrachten Kontaktdaten vornehmen.

3.7. Rechtsgrundlagen für die Direktwerbung

Die Direktwerbung ist wesentlicher Bestandteil des Geschäftsmodells sozialer Netzwerkdienste, wobei diese verschiedene Werbemodelle verfolgen können. Jedoch sollte die Verwendung der personenbezogenen Daten ihrer Nutzer zu Werbezwecken im Einklang mit den einschlägigen Bestimmungen der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen[19].

Kontextbezogene Werbung ist auf die Inhalte zugeschnitten, die sich der Nutzer ansieht bzw. auf die er zugreift.[20]

Segmentbezogene Werbung versorgt gewisse Zielgruppen von Nutzern mit Werbeprojektionen[21]; wobei ein Nutzer der betreffenden Gruppe anhand der Informationen zugeordnet wird, die er dem sozialen Netzwerkdienst auf direktem Wege mitgeteilt hat.[22]

Verhaltensbezogene Werbung erfolgt, indem die Werbeprojektionen anhand der Beobachtung und Analyse der Aktivitäten ausgewählt werden, die der Nutzer über einen gewissen Zeitraum an den Tag legt. Je nach den einschlägigen Rechtsgrundlagen und den Merkmalen der eingesetzten Techniken unterliegen diese Techniken mitunter unterschiedlichen rechtlichen Anforderungen. Die Datenschutzgruppe empfiehlt, für verhaltensbezogene Werbemodelle keine sensiblen Daten zu verwenden, sofern nicht alle rechtlichen Anforderungen erfüllt sind.

Welches Modell oder welche Kombination von Modellen auch immer genutzt wird, können Werbeprojektionen entweder direkt durch den sozialen Netzwerkdienst (der Anbieter des sozialen Netzwerkdienstes handelt hierbei als Vermittler) oder durch einen dritten Werbeanbieter eingeblendet werden. Im ersten Fall müs-

---

19 Die Datenschutzgruppe beabsichtigt, die verschiedenen Aspekte der Onlinewerbung demnächst in einem eigenen Dokument zu behandeln.

20 Wenn beispielsweise die aufgerufene Seite den Begriff „Paris“ erwähnt, könnte die betreffende Werbung ein bestimmtes Restaurant in dieser Stadt anpreisen.

21 Jede Gruppe wird anhand einer Reihe von Kriterien definiert.

22 Z. B. anlässlich der Anmeldung und Registrierung beim Netzwerkdienst.

sen Dritten gegenüber keinerlei personenbezogene Daten des Nutzers offengelegt werden. Im zweiten Fall verarbeitet der Drittwerbeanbieter mitunter jedoch personenbezogene Daten über den Nutzer, so z. B., wenn er die IP-Adresse des Nutzers und ein auf dem Computer des Nutzers befindliches Cookie verarbeitet.

3.8. Vorratsspeicherung von Daten

Soziale Netzwerkdienste fallen nicht in den Geltungsbereich der Definition für elektronische Kommunikationsdienste nach Artikel 2 Buchstabe c) der Richtlinie 2002/21/EG (Rahmenrichtlinie). Die Anbieter sozialer Netzwerkdienste können zusätzliche Dienstleistungen anbieten, die in den Anwendungsbereich eines elektronischen Kommunikationsdienstes fallen, wie z. B. einen öffentlich zugänglichen E-Mail-Dienst. Solche Dienste unterliegen dann der Datenschutzrichtlinie für elektronische Kommunikation und der Datenvorratsspeicherungsrichtlinie.

Einige soziale Netzwerke gestatten ihren Nutzern die Versendung von Einladungen an Dritte. Das Verbot für das Versenden unerbetener elektronischer Nachrichten zu Zwecken der Direktwerbung gilt nicht für persönliche Mitteilungen. Um sich im Rahmen der Ausnahmeregelung für persönliche Mitteilungen zu bewegen, muss ein sozialer Netzwerkdienst die folgenden Kriterien erfüllen:

– weder dem Absender noch dem Empfänger wird ein Anreiz geboten;

– der Anbieter hat hinsichtlich der Empfänger der persönlichen Mitteilung keinerlei Auswahlmöglichkeit;[23]

– die Identität des absendenden Nutzers ist eindeutig anzugeben;

– der absendende Nutzer muss den Inhalt der Mitteilung, die in seinem Namen versandt wird, vollständig kennen.

Einige soziale Netzwerkdienste praktizieren auch eine Vorratsspeicherung von Daten zur Identifizierung der aus dem Netzwerk ausgeschlossenen Nutzer, um sicherzustellen, dass diese sich nicht erneut anmelden und registrieren können. In diesem Fall sind diese ehemaligen Nutzer darüber zu unterrichten, dass eine derartige Verarbeitung von Daten stattfindet. Ferner darf die Vorratsspeicherung nur die Identifizierungsdaten und nicht auch die Gründe für den Ausschluss dieser Personen betreffen. Diese Vorratsspeicherung sollte nicht länger als ein Jahr andauern.

[23] Beispielsweise ist auch die Praxis einiger sozialer Netzwerkdienste, die Einladungen des Nutzers unterschiedslos an sein gesamtes Adressbuch zu versenden, unzulässig.

Die von einem Nutzer bei der Anmeldung zum sozialen Netzwerk mitgeteilten personenbezogenen Daten sollten gelöscht werden, sobald entweder der Nutzer oder der Anbieter des sozialen Netzwerkdienstes sich entscheidet, das betreffende Nutzerprofil zu löschen.[24] Genauso sollte mit Informationen, die von einem Nutzer bei der Aktualisierung seines Nutzerprofils gelöscht wurden, keine Vorratsspeicherung erfolgen. Die sozialen Netzwerkdienste sollten ihre Nutzer vor dem Ergreifen solcher Maßnahmen mit den ihnen zur Verfügung stehenden Mitteln unterrichten und sie über den Zeitraum dieser Vorratspeicherung informieren. Aus Sicherheits- und Rechtsgründen könnte es in spezifischen Fällen gerechtfertigt sein, aktualisierte oder gelöschte Daten und Nutzerprofile für einen näher bestimmten Zeitraum zu speichern, um Vorgänge in böswilliger Absicht, die aus Identitätsdiebstahl und anderen strafbaren oder kriminellen Handlungen resultieren, verhindern zu helfen.

Benutzt ein Nutzer den sozialen Netzwerkdienst für einen bestimmten Zeitraum nicht mehr, so sollte sein Nutzerprofil in den inaktiven Zustand versetzt werden, d. h. für andere Nutzer oder die Außenwelt nicht mehr sichtbar sein; nach Ablauf eines weiteren Zeitraums sollten die Daten in dem aufgegebenen Nutzerprofil gelöscht werden. Die sozialen Netzwerkdienste sollten den Nutzer vor dem Ergreifen dieser Maßnahmen mit den ihnen zur Verfügung stehenden Mitteln unterrichten.

3.9. Rechte der Nutzer

Die sozialen Netzwerkdienste sollten die Rechte der von der Verarbeitung betroffenen Personen im Einklang mit den Bestimmungen der Artikel 12 und 14 der Datenschutzrichtlinie wahren.

Die Zugriffs- und Berichtigungsrechte der Nutzer sind nicht auf die jeweiligen Nutzer des sozialen Netzwerkdienstes begrenzt, sondern erstrecken sich auf alle natürlichen Personen, deren personenbezogene Daten verarbeitet werden.[25] Mitglieder und Nichtmitglieder müssen über Mittel und Wege verfügen, um ihre Rechte auf Zugriff, Berichtigung und Löschung geltend zu machen. Die Homepage des sozialen Netzwerkdienstes sollte klar und deutlich auf die „Beschwerdestelle" verweisen, die vom Anbieter des sozialen Netzwerkdienstes eingerichtet wurde, um Fragen und Probleme im Zusammenhang mit dem Datenschutz und dem Schutz der Privatsphäre zu klären und den Beschwerden von Mitgliedern wie auch von Nichtmitgliedern nachzugehen.

---

[24] Gemäß Artikel 6 Absatz 1 Buchstabe e) der Datenschutzrichtlinie müssen personenbezogene Daten *„nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person ermöglicht"*.

[25] Dies ist beispielsweise schon der Fall, wenn die E-Mail-Adresse einer Person vom sozialen Netzwerkdienst benutzt wird, um ihm eine Einladung zu schicken.

Nach Artikel 6 Absatz 1 Buchstabe c) der Datenschutzrichtlinie ist darauf zu achten, dass personenbezogene Daten *„den Zwecken entsprechen, für die sie erhoben und/oder verarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“*. In diesem Zusammenhang lässt sich feststellen, dass es für die sozialen Netzwerkdienste zwar erforderlich sein mag, einige Identifizierungsdaten über ihre Mitglieder zu registrieren, sich daraus aber noch nicht die Notwendigkeit ergibt, den wirklichen Namen ihrer Mitglieder im Internet zu veröffentlichen. Daher sollten die sozialen Netzwerkdienste sorgfältig abwägen, ob sie es rechtfertigen können, ihre Nutzer zu zwingen, im Rahmen ihrer echten Identität anstatt unter einem pseudonymen Profil zu handeln. Es gibt starke Argumente zugunsten einer diesbezüglichen Wahlmöglichkeit der Nutzer, und zumindest in einem Mitgliedstaat ist diese bereits gesetzliches Erfordernis. Besonderes Gewicht kommt diesen Argumenten bei sozialen Netzwerken mit großer Mitgliedschaft zu.

Nach Artikel 17 der Datenschutzrichtlinie hat der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen durchzuführen, die für den Schutz personenbezogener Daten erforderlich sind. Zu diesen Sicherheitsmaßnahmen zählen insbesondere Zugriffskontroll- und Authentifizierungsmechanismen, die auch bei der Verwendung von pseudonymen Profilen funktionieren.

4. Kinder und Minderjährige

Ein Großteil der sozialen Netzwerkdienste wird von Kindern/Minderjährigen genutzt. Die Stellungnahme der Datenschutzgruppe WP147[26] befasste sich mit der Anwendung der Datenschutzgrundsätze im Bereich der Schuldaten und Bildungseinrichtungen. In der Stellungnahme wurde die Notwendigkeit betont, das Wohl des Kindes vorrangig zu berücksichtigen, wie dies auch im UN-Übereinkommen über die Rechte des Kindes verankert ist. Die Datenschutzgruppe möchte die Bedeutung dieses zentralen Rechtsgrundsatzes auch im Zusammenhang mit den sozialen Netzwerkdiensten unterstreichen.

Weltweit wurden von den Datenschutzbehörden einige interessante Initiativen[27] unternommen, die sich in der Hauptsache mit der Aufklärung über soziale Netzwerkdienste und mit der Sensibilisierung für die möglichen Risiken ihrer Nut-

[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_de.pdf

[27] Z. B. die portugiesische Initiative „Dadus“: http://dadus.cnpd.pt/; die dänische Plakette für sicherheitsüberprüftes Chatten: http://www.fdim.dk/

zung befassten. Die Datenschutzgruppe fordert zu weitergehenden Forschungsmaßnahmen zu der Frage auf, wie die Schwierigkeiten im Zusammenhang mit einer geeigneten Altersüberprüfung und Nachweisführung über die informierte Einwilligung in Angriff genommen werden können, um diese Herausforderungen besser zu meistern.

Aufgrund der bisherigen Überlegungen vertritt die Datenschutzgruppe die Auffassung, dass eine Mehrfach-Strategie geeignet ist, den Schutz personenbezogener Daten von Kindern im Zusammenhang mit sozialen Netzwerkdiensten in den Griff zu bekommen. Diese Strategie könnte auf folgenden Faktoren beruhen:

– Aufklärungs- und Sensibilisierungsinitiativen; sie sind von grundlegender Bedeutung, um die aktive Einbeziehung der Kinder sicherzustellen (über die Schulen, die Aufnahme der Vermittlung von Datenschutz-Grundkenntnissen in die Lehrpläne für Schulen und Bildungseinrichtungen, die Anschaffung von eigens zu diesem Zweck ausgearbeiteten Lehr- und Unterrichtsmaterialien, die Zusammenarbeit der zuständigen nationalen Datenschutzeinrichtungen);

– einwandfreie und rechtmäßige Verarbeitung personenbezogener Daten im Hinblick auf Minderjährige, wie z. B. keinerlei Abfragen von sensiblen Daten in den Anmeldeformularen, keine speziell auf Minderjährige ausgerichtete Direktwerbung, Erfordernis der vorherigen Einwilligung der Eltern vor jeder Registrierung, geeignete Grade für die abgestufte Trennung zwischen den Datensätzen der Kinder- und der Erwachsenencommunity;

– Einführung von Technologien zur Stärkung des Schutzes der Privatsphäre (PETs) – z. B. datenschutzfreundliche Standardeinstellungen, Einblendung von Warnsignalen bei sicherheitsrelevanten Schritten, Software zur Altersüberprüfung);

– Selbstkontrolle und -regulierung durch die Anbieter von sozialen Netzwerkdiensten, Förderung der Annahme von praktischen Verhaltenskodexen mit wirksamen Zwangsmaßnahmen und disziplinierenden Wirkungen;

– gegebenenfalls Ad-hoc-Gesetzgebungsmaßnahmen zur Verhinderung unfairer und/oder irreführender Praktiken im Zusammenhang mit sozialen Netzwerkdiensten.

5. Zusammenfassung der Rechte und Pflichten

Anwendbarkeit der EG-Richtlinien

1. Die Datenschutzrichtlinie findet im Allgemeinen auf die Verarbeitung personenbezogener Daten durch soziale Netzwerkdienste (SNS) auch dann Anwendung, wenn diese ihren Hauptsitz außerhalb des EWR haben.

2. Die Anbieter sozialer Netzwerkdienste gelten als für die Verarbeitung Verantwortliche im Sinne der Datenschutzrichtlinie.

3. Die Anbieter von Anwendungssoftware sind unter Umständen als für die Verarbeitung Verantwortliche im Sinne der Datenschutzrichtlinie anzusehen.

4. Die Nutzer gelten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten durch die sozialen Netzwerkdienste als betroffene Personen.

5. Die Verarbeitung personenbezogener Daten durch die Nutzer fällt in den meisten Fällen unter die Ausnahmeklausel für Privathaushalte. Es gibt jedoch auch Fälle, in denen die Tätigkeiten eines Nutzers nicht unter diese Ausnahmeregelung fallen.

6. Soziale Netzwerkdienste fallen nicht in den Geltungsbereich der Definition für elektronische Kommunikationsdienste; somit findet die Datenvorratsspeicherungsrichtlinie auf soziale Netzwerkdienste keine Anwendung.

Pflichten der sozialen Netzwerkdienste (SNS)

7. Die sozialen Netzwerkdienste sollten ihre Nutzer über ihre Identität aufklären und umfassende und eindeutige Informationen über ihre Zielsetzungen sowie über die verschiedenen Möglichkeiten vorlegen, wie sie die personenbezogenen Daten verarbeiten wollen.

8. Die sozialen Netzwerkdienste sollten datenschutzfreundliche Standardeinstellungen anbieten.

9. Die sozialen Netzwerkdienste sollten den Nutzern ausreichende Informationen und geeignete Warnhinweise zu den Risiken für den Schutz ihrer Privatsphäre an die Hand geben, die mit dem Hochladen von personenbezogenen Daten ins soziale Netzwerkprofil verbunden sind.

11. Die Nutzer sollten vom sozialen Netzwerkdienst darauf hingewiesen werden, dass Bilder oder Informationen über dritte Personen nur mit der Einwilligung der betroffenen Person ins soziale Netzwerkprofil eingestellt werden sollten.

12. Die Homepage des sozialen Netzwerkdienstes sollte zumindest einen Link zu einer Beschwerdestelle aufweisen, die sich mit den Datenschutzfragen der Mitglieder wie auch der Nichtmitglieder befasst.

13. Sämtliche Werbemaßnahmen müssen im Einklang mit den einschlägigen Bestimmungen der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen.

14. Die sozialen Netzwerkdienste müssen sich festlegen, wie lange die Vorratsspeicherung von Daten inaktiver Nutzer im Höchstfall zulässig ist. Aufgegebene Nutzerprofile sind zu löschen.

15. Im Hinblick auf Minderjährige sollten die sozialen Netzwerkdienste geeignete Maßnahmen zur Begrenzung der Risiken ergreifen.

<u>Rechte der Nutzer</u>

16. Sowohl die Mitglieder als auch die Nichtmitglieder von sozialen Netzwerkdiensten genießen gegebenenfalls die Rechte der betroffenen Person im Sinne der Artikel 10 bis 14 der Datenschutzrichtlinie.

17. Sowohl den Mitgliedern als auch den Nichtmitgliedern sollte im Rahmen des sozialen Netzwerkdienstes ein leicht handhabbares Beschwerdeverfahren zur Verfügung stehen.

18. Den Nutzern sollte es im Allgemeinen gestattet sein, ein Pseudonym anzunehmen.

Brüssel, den 12. Juni 2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK

Die Zukunft des Datenschutzes

Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten (WP 168)

Annahme am 1. Dezember 2009

Zusammenfassung

Am 9. Juli 2009 hat die Kommission ein Konsultationsverfahren zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, insbesondere angesichts neuer Technologien und angesichts der Globalisierung. Die Kommission erwartet Beiträge zu den Fragen, ob der aktuelle Rechtsrahmen den Herausforderungen gewachsen ist und welche zukünftigen Aktionen erforderlich sind, um die ermittelten Herausforderungen in Angriff zu nehmen. Das vorliegende Dokument enthält die gemeinsame Stellungnahme der Artikel-29-Arbeitsgruppe (WP29) und der Arbeitsgruppe Polizei und Justiz (WPPJ) zu diesem Konsultationsverfahren.

Dieser Beitrag stellt in erster Linie fest, dass die wichtigsten Grundsätze des Datenschutzes trotz der neuen Technologien und der Globalisierung nach wie vor gültig sind. Das Datenschutzniveau in der EU kann von einer besseren Anwendung der bestehenden Datenschutzgrundsätze profitieren. Das bedeutet nicht, dass keine Gesetzesänderungen erforderlich sind. Ganz im Gegenteil ist es sinnvoll, die Gelegenheit zu ergreifen, um:

- die Anwendung einiger Grundregeln und Grundsätze des Datenschutzes (wie Einwilligung und Transparenz) zu klären;
- dem Rechtsrahmen durch zusätzliche Grundsätze (wie z. B. „Privacy by Design“ und „Rechenschaftspflicht“) Neuerungen hinzuzufügen;
- die Wirksamkeit des Systems durch die Modernisierung von Bestimmungen der Richtlinie 95/46/EG zu stärken (z. B. durch eine Einschränkung der bürokratischen Hindernisse);
- die Grundsätze des Datenschutzes in einem umfassenden Rechtsrahmen zusammenzufassen, der auch bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Anwendung findet.

Kapitel 1 enthält eine Einleitung mit einem kurzen Überblick über den Hintergrund und den Kontext des Datenschutzes in der EU.

In Kapitel 2 wird die Einführung eines umfassenden Rechtsrahmens vorgeschlagen. Die Notwendigkeit spezieller Gesetze (leges speciales) wird erkannt, vorausgesetzt, sie passen zu dem Konzept eines umfassenden Rechtsrahmens und erfüllen die wichtigsten Grundsätze. Die wichtigsten Garantien und Grundsätze des Datenschutzes sollten auf die Datenverarbeitung in allen Sektoren Anwendung finden.

In den Kapiteln 3 und 4 werden die wichtigsten Herausforderungen an den Datenschutz diskutiert.

In Kapitel 3 zur Globalisierung wird festgestellt, dass der Datenschutz gemäß dem Gemeinschaftsrecht ein Grundrecht ist. Die EU und ihre Mitgliedstaaten sollten jedem dieses Grundrecht garantieren, insoweit es in ihre Zuständigkeit fällt. Natürliche Personen sollten die Möglichkeit haben, Schutz einzufordern, auch wenn ihre Daten außerhalb der EU verarbeitet werden. Deshalb ist die Kommission dazu aufgerufen, Initiativen zu einer weiteren Entwicklung der internationalen globalen Standards zum Schutz personenbezogener Daten zu ergreifen. Des Weiteren ist es erforderlich, das Konzept der Angemessenheit zu überdenken. Außerdem können internationale Abkommen angemessene Instrumente für den Schutz personenbezogener Daten in einem globalen Kontext darstellen. Der zukünftige Rechtsrahmen könnte die Voraussetzungen für Abkommen mit Drittländern nennen. Die Verarbeitung von Daten außerhalb der EU kann auch durch verbindliche unternehmensinterne Datenschutzregelungen (BCR) geschützt werden. In den neuen Rechtsrahmen sollte eine gestärkte Regelung zu den BCR aufgenommen werden. Die WP29 plant, die Kommission im kommenden Jahr über das anzuwendende Recht zu beraten.

In Kapitel 4 über die technologischen Änderungen wird festgestellt, dass die Richtlinie 95/46/EG aufgrund ihrer soliden und technologisch neutralen Grundsätze und Konzepte dem Zustrom technologischer Änderungen gut standgehalten hat. Diese Grundsätze und Konzepte bleiben in der heutigen vernetzten Welt gleichermaßen maßgeblich, gültig und anwendbar. Die technologischen Änderungen haben die Risiken für die Privatsphäre des Einzelnen und für den Datenschutz erhöht. Als Gegengewicht zu diesen Risiken sollte der Grundsatz „Privacy by Design“ in den neuen Rechtsrahmen eingebracht werden: Bei der Planung von Informations- und Kommunikationstechnologien sollten der Privatsphäre und dem Datenschutz Rechnung getragen werden. Die Anwendung dieses Grundsatzes würde die Notwendigkeit zur Einführung von Technologien zum Schutz der Privatsphäre, von „Privacy by Default“-Einstellungen und der erforderlichen Tools betonen, damit die Nutzer ihre personenbezogenen Daten besser schützen können. Der Grundsatz „Privacy by Design“ sollte also nicht nur für die für die Datenverarbeitung Verantwortlichen bindend sein, sondern auch für die Entwickler und Hersteller der Technologien. Darüber hinaus sollten soweit erforderlich in Bezug auf bestimmte technologische Kontexte Verordnungen erlassen werden,

welche die Verankerung von Grundsätzen des Datenschutzes und der Privatsphäre vorschreiben.

In den Kapiteln 5, 6 und 7 wird dargelegt, dass diese wichtigsten Herausforderungen an den Datenschutz eine stärkere Rolle der verschiedenen Akteure erfordern.

Die Änderungen im Verhalten und in der Rolle der betroffenen Personen sowie die Erfahrungen mit der Richtlinie 95/46/EG machen eine stärkere Position der Betroffenen in dem Datenschutzrechtsrahmen erforderlich. Kapitel 5 enthält Vorschläge, wie die Betroffenen gestärkt werden können, so dass sie eine aktivere Rolle spielen. Dies erfordert unter anderem eine Verbesserung des Rechtsschutzes: mehr Möglichkeiten für die Betroffenen, ihre Rechte auszuüben und geltend zu machen, einschließlich der Einführung von Sammelklagen; einfacher zugängliche, wirkungsvollere und kostengünstigere Beschwerdeverfahren sowie alternative Verfahren zur Streitbeilegung. Darüber hinaus sollte der neue Rechtsrahmen alternative Lösungen zur Erhöhung der Transparenz bereitstellen sowie die generelle Meldung von Datenschutzverletzungen einführen. Die „Einwilligung" ist eine wichtige Grundlage für die Verarbeitung, die dem Betroffenen unter bestimmten Umständen eine stärkere Position geben könnte. Derzeit wird die Einwilligung jedoch häufig fälschlicherweise als maßgeblicher Grund für die Verarbeitung angegeben, da die Voraussetzungen für die Einwilligung nicht vollumfänglich erfüllt werden. Deshalb sollten die Voraussetzungen für eine „Einwilligung" in dem neuen Rechtsrahmen genauer festgelegt werden. Außerdem muss die Harmonisierung verbessert werden, da die Stärkung der Rolle des Betroffenen derzeit durch eine fehlende Harmonisierung der innerstaatlichen Gesetze, mit denen die Richtlinie 95/46/EG umgesetzt wird, untergraben wird. Ein weiteres Problem ist die Rolle der Betroffenen im Internet. Angesichts des neuen Rechtsrahmens sollte hier eine weitere Klärung erfolgen. Jedenfalls sollte jeder, der Privatpersonen Dienste anbietet, dazu verpflichtet sein, für die Sicherheit und in angemessenem Rahmen für die Vertraulichkeit der durch die Nutzer hochgeladenen Informationen bestimmte Garantien zu geben, unabhängig davon, ob der Kunde für die Datenverarbeitung verantwortlich ist oder nicht.

Kapitel 6 zielt auf eine Stärkung der Verantwortung der für die Datenverarbeitung Verantwortlichen ab. Der Datenschutz sollte zuallererst in Organisationen verankert werden. Er sollte Teil der gemeinsamen Werte und Praktiken von Organisationen werden, und es sollten ausdrücklich für den Datenschutz Verantwortliche benannt werden. Dies wird auch die nationalen Datenschutzbehörden bei ihren Kontroll- und Durchsetzungsaufgaben unterstützen und so die Wirksamkeit des Schutzes der Privatsphäre stärken. Die für die Datenverarbeitung Verantwortlichen müssen verschiedene proaktive und reaktive Maßnahmen ergreifen, die in diesem Kapitel genannt werden. Darüber hinaus wäre es angemessen, in den um-

fassenden Rechtsrahmen den Grundsatz der Rechenschaftspflicht einzuführen, so dass die für die Datenverarbeitung Verantwortlichen zur Durchführung der Maßnahmen verpflichtet sind, mit denen sichergestellt werden kann, dass die wesentlichen Grundsätze und Verpflichtungen gemäß der geltenden Richtlinie bei der Bearbeitung der personenbezogenen Daten beachtet werden. Die für die Datenverarbeitung Verantwortlichen sollten auch dazu verpflichtet werden, die erforderlichen internen Mechanismen einzuführen, mit denen gegenüber externen Stellen, einschließlich der Datenschutzbehörde, die Einhaltung der Grundsätze und Verpflichtungen nachgewiesen werden kann. Die Meldungen von Datenverarbeitungsoperationen an nationale Datenschutzbehörden könnten vereinfacht oder eingeschränkt werden. Es sollte untersucht werden, ob und in welchem Ausmaß die Meldungen auf diejenigen Fälle beschränkt werden könnten, in denen eine ernstzunehmende Gefahr für den Datenschutz besteht. Dies würde den Datenschutzbehörden die Möglichkeit geben, selektiver vorzugehen und ihre Anstrengungen auf die vorgenannten Fälle zu konzentrieren sowie auf Wege zur Rationalisierung der Meldungen.

Kapitel 7a sieht eine stärkere und eindeutigere Rolle der nationalen Datenschutzbehörden vor. Derzeit bestehen große Unterschiede zwischen den Mitgliedstaaten, unter anderem bezüglich der Position, den Ressourcen und den Befugnissen der einzelnen Datenschutzbehörden. Die neuen Herausforderungen an den Datenschutz machen einestrikte, einheitlichere und effektive Überwachung durch die Datenschutzbehörden erforderlich. Der neue Rechtsrahmen sollte folglich hochrangig und richtunggebend einheitliche Standards in Bezug auf Unabhängigkeit und effektive Befugnisse garantieren sowie den Datenschutzbehörden eine beratende Rolle im Gesetzgebungsverfahren geben sowie die Möglichkeit, die Geschäftsordnung selbst festzulegen, insbesondere durch das Setzen von Prioritäten bei der Behandlung von Beschwerden.

In Kapitel 7b wird dargelegt, wie die Zusammenarbeit zwischen den Datenschutzbehörden verbessert werden sollte. Die europäischen Datenschutzbehörden sind in der WP29 zusammengefasst. Als erste Priorität sollte sichergestellt werden, dass alle Fragen bezüglich der Verarbeitung personenbezogener Daten insbesondere im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in die Maßnahmen der aktuellen WP29 eingeschlossen werden. Darüber hinaus sollten die Arbeitsmethoden der WP29 weiter verbessert werden. Soweit erforderlich, sollten die Mitglieder der WP29 zur Umsetzung der Ansichten der WP29 in den jeweiligen Mitgliedstaaten in die Praxis aufgefordert werden. Die Beziehungen zwischen der WP29 und der Kommission, die die Sekretariatsgeschäfte für die WP29 wahrnimmt, können durch das Festlegen der wichtigsten Rollen der beiden Akteure in einem Memorandum of Understanding weiter verbessert werden. Die WP29 wird im Jahr 2010 mit der Kommission Beratungen zu diesem Memorandum aufnehmen.

Kapitel 8 schließlich beschäftigt sich mit den Datenschutzherausforderungen im Bereich der Strafverfolgung, die ein ganz spezielles Problemfeld darstellen. Der Kontext im Bereich Strafverfolgung hat sich in der EU mit dem Inkrafttreten des Vertrags von Lissabon geändert. Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, kann als erster Schritt zu einem allgemeinen Rechtsrahmen in der ehemaligen dritten Säule angesehen werden. Dieser Schritt ist jedoch noch lange nicht abgeschlossen. In den letzten Jahren gab es einen dramatischen Anstieg bei der Speicherung und dem Austausch personenbezogener Daten in Bezug auf die Tätigkeiten im Polizei- und Justizbereich. Denn um den neuen Bedrohungen entgegenzutreten, die aus dem Terrorismus und dem organisierten Verbrechen entstanden sind, gibt es – gefördert durch die technologischen Entwicklungen – einen wachsenden Bedarf an der Nutzung dieser Daten. Vor diesem Hintergrund sind die Herausforderungen an den Datenschutz immens und sollten in dem zukünftigen Rechtsrahmen angesprochen werden. Kapitel 8 legt die Bedingungen für die Rechtsetzung und Politikgestaltung in Bezug auf den Datenschutz im Bereich der Strafverfolgung dar: eine einheitliche Strategie als Grundlage des Informationsaustauschs; regelmäßige Bewertung der bestehenden Maßnahmen, der Rechtsinstrumente und ihrer Anwendung; Transparenz und Auskunfts- und Berichtigungsrechte im grenzüberschreitenden Kontext; Transparenz und demokratische Kontrolle im Gesetzgebungsverfahren; die Architektur der Systeme für die Speicherung und den Austausch der personenbezogenen Daten; ein eindeutiger Rechtsrahmen als Grundlage für die Beziehungen mit Drittländern, der für alle Parteien bindend ist und auf dem Konzept der Angemessenheit basiert; besondere Aufmerksamkeit auf die groß angelegten Informationssysteme in der EU; richtiges Herangehen an eine unabhängige Kontrolle, an die justizielle Aufsicht und an die Rechtsmittel; Stärken der Zusammenarbeit zwischen den Datenschutzbehörden.

1. Einleitung

Die Konsultation

1. Am 9. Juli 2009 hat die Kommission ein Konsultationsverfahren zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, insbesondere angesichts neuer Technologien und angesichts der Globalisierung. Die Kommission erwartet Beiträge zu den Fragen, ob der aktuelle Rechtsrahmen den Herausforderungen gewachsen ist und welche zukünftigen Aktionen erforderlich sind, um die ermittelten Herausforderungen in Angriff zu nehmen.

2. Dieses Papier enthält die gemeinsame Stellungnahme der Artikel-29-Arbeitsgruppe (WP29) und der Arbeitsgruppe Polizei und Justiz (WPPJ) zu diesem Konsultationsverfahren.

Hintergrund und Kontext

3. Das Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108)[1] kann als erster europäischer Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten angesehen werden. Das Recht auf Datenschutz ist eng verbunden mit dem Anspruch auf Achtung des Privatlebens gemäß Artikel 8 der Europäischen Menschenrechtskonvention, ist jedoch nicht identisch mit diesem. Das Recht auf Datenschutz wird in Artikel 8 der Charta der Grundrechte der Europäischen Union als eigenständiges Grundrecht anerkannt.

4. Die Grundsätze des Übereinkommens 108 wurden in der Richtlinie 95/46/EG[2] weiterentwickelt, die den Grundbaustein des Datenschutzrechts in der EU bildet. Das hauptsächliche Ziel des Konsultationsverfahrens der Kommission ist die (zukünftige) Wirksamkeit der Richtlinie. Weitere Rechtsakte der EU für den Datenschutz sind die Verordnung (EG) Nr. 45/2001[3], anwendbar bei der Datenverarbeitung durch Organe und Einrichtungen der EU, Richtlinie 2002/58/EC[4] über die Privatsphäre und die elektronische Kommunikation und Rahmenbeschluss 2008/977/JI[5] über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.

5. Mit dem Vertrag von Lissabon hat der Datenschutz signifikant an Bedeutung gewonnen. Es wurde nicht nur die EU-Grundrechtecharta bindend, sondern es wurde auch Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) als neue Rechtsgrundlage für den Datenschutz

---

1 STE Nr. 108, 28.1.1981.

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, ABl. 1995, L 281, S. 31.

3 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001, L 8, S. 1.

4 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002, L 201, S. 37, in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung.

5 Rahmenbeschluss 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008, L 350, S. 60, der bis zum 27. November 2010 in innerstaatliches Recht umgesetzt sein muss.

eingeführt, die bei jeglicher Verarbeitung personenbezogener Daten im privaten und im öffentlichen Bereich anzuwenden ist sowie bei der Verarbeitung von Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit und bei der gemeinsamen Außen- und Sicherheitspolitik. Artikel 16 gibt dem Datenschutz neue Impulse.

6. In diesem Zusammenhang muss auch das „Stockholmer Programm" erwähnt werden. Dieses Mehrjahresprogramm der EU widmet dem Datenschutz und damit dem Schutz der Bürger in einem Raum der Freiheit, der Sicherheit und des Rechts viel Aufmerksamkeit.[6]

Hauptaussage

7. Das Konsultationsverfahren der Kommission wird angesichts der wichtigen neuen Herausforderungen durch die neuen Technologien und durch die Globalisierung sowie angesichts des Vertrags von Lissabon zum passenden Zeitpunkt durchgeführt.

8. In erster Linie ist festzustellen, dass die wichtigsten Grundsätze des Datenschutzes trotz dieser wichtigen Herausforderungen nach wie vor gültig sind. Das Datenschutzniveau in der EU kann von einer besseren Anwendung der bestehenden Datenschutzgrundsätze profitieren. Das bedeutet nicht, dass keine Gesetzesänderungen erforderlich sind. Ganz im Gegenteil ist es sinnvoll, die Gelegenheit zu ergreifen, um:

   - die Anwendung einiger Grundregeln und Grundsätze des Datenschutzes (wie Einwilligung und Transparenz) zu klären;
   - dem Rechtsrahmen durch zusätzliche Grundsätze (wie z. B. „Privacy by Design" und „Rechenschaftspflicht") Neuerungen hinzuzufügen;
   - die Wirksamkeit des Systems durch die Modernisierung von Bestimmungen der Richtlinie 95/46/EG zu stärken (z. B. durch eine Einschränkung der bürokratischen Hindernisse);
   - die Grundsätze des Datenschutzes in einem umfassenden Rechtsrahmen zusammenzufassen, der auch bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Anwendung findet.

[6] Das Stockholmer Programm: ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, durch den Europäischen Rat im Dezember 2009 anzunehmen.

2. Ein umfassender Rechtsrahmen

Der aktuelle Rechtsrahmen

9. Der Datenschutz wurde als binnenmarktbezogenes Thema in den Rechtsrahmen der Europäischen Union eingebracht. Die Richtlinie 95/46/EG basiert auf Artikel 95 EG-Vertrag. Die Richtlinie verfolgt zwei Zwecke. Für das Errichten und das Funktionieren eines Binnenmarkts müssen personenbezogene Daten frei von einem Mitgliedstaat in einen anderen übertragen werden können, während gleichzeitig ein hohes Schutzniveau in Bezug auf die Grundrechte der natürlichen Personen gewährleistet sein sollte.

10. Richtlinie 95/46/EG ist als allgemeiner Rechtsrahmen gedacht, der für bestimmte Sektoren durch besondere Regelungen zum Datenschutz ergänzt werden kann. Bis jetzt wurde eine einzige Sonderregelung angenommen, nämlich im Bereich des Datenschutzes bei der elektronischen Kommunikation (derzeit Richtlinie 2002/58/EG). Außerdem enthalten einige sektorbezogene Rechtsvorschriften besondere Bestimmungen zur Verarbeitung personenbezogener Daten ([7]zur Geldwäsche, Zollvorschriften oder Vorschriften zu VIS, EURODAC oder SIS II).

11. Die Anwendung von Artikel 95 EG-Vertrag hat sich auf den Anwendungsbereich der Richtlinie 95/46/EG ausgewirkt. Obwohl die Richtlinie als allgemeiner Rechtsrahmen für den Datenschutz gedacht war und in vielen Aspekten auch als solcher funktioniert, deckt sie weder die Datenverarbeitung durch Einrichtungen der Gemeinschaft ab, noch Verarbeitungen, die außerhalb des Bereichs der ehemals ersten Säule (hauptsächlich die ehemalige dritte Säule) fallen. Für die Verarbeitung durch Einrichtungen der Gemeinschaft (insofern sie sich innerhalb der ersten Säule bewegen) wurde die Verordnung 45/2001 angenommen, die der Richtlinie 95/46/EG in großen Abschnitten ähnelt. Die derzeitige Situation in Bezug auf die ehemals dritte Säule kann als Stückwerk von Datenschutzregelungen beschrieben werden, die in unterschiedlichen Situationen anzuwenden sind. Einige Unterschiede zwischen diesen Regelungen haben ihren Ursprung in den Besonderheiten des abgedeckten Bereichs, andere sind lediglich die Folgen der unterschiedlichen gesetzlichen Hintergründe. Der Rahmenbeschluss 2008/977/JI kann als erster Schritt zu einem allgemeineren Rechtsrahmen gesehen werden.

12. Die Situation ist insbesondere für die dritte Säule nicht zufriedenstellend:

---

[7] Z. B. Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. 2005, L 309, S. 15 und verschiedene Rechtsinstrumente für die groß angelegten Informationssysteme SIS, VIS und EURODAC.

- Der Datenschutz wird inzwischen in zunehmendem Maße als allgemeines Anliegen der Europäischen Union erkannt und ist nicht mehr zwangsläufig ein rein binnenmarktbezogenes Thema. Dies zeigt sich z. B. in Artikel 8 der Charta der Grundrechte der Europäischen Union.
- In den vergangenen Jahren und sicherlich nach den Terroranschlägen in den USA vom 11.9.2001 wurde der Austausch personenbezogener Daten unter den Mitgliedstaaten ein wesentlicher Bestandteil der polizeilichen und justiziellen Zusammenarbeit, der natürlich einen angemessenen Schutz erforderlich macht.
- Die ehemalige Aufteilung zwischen den Säulen spiegelt nicht die Realität des Datenschutzes wider, in der die personenbezogenen Daten in säulenübergreifenden Situationen genutzt werden. Dies wird durch die Entscheidungen des Europäischen Gerichtshofs zu den PNR und zu der Vorratsdatenspeicherung an Fällen gezeigt, in denen Daten, die ursprünglich in einem Wirtschaftskontext erhoben wurden, für die Strafverfolgung genutzt wurden.

Die Notwendigkeit eines neuen Rechtsrahmens

13. Die Unzulänglichkeiten des aktuellen Systems erfordern das Nachdenken über „einen umfassenden und einheitlichen Rechtsrahmen zum Datenschutz, der für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt".[8] Der Vertrag von Lissabon sieht eine neue horizontale Herangehensweise an den Datenschutz und den Schutz der Privatsphäre vor und stellt die erforderliche Rechtsgrundlage (Art. 16 AEUV)[9] bereit, um die bestehenden Unterschiede und Abweichungen abzuschaffen, die einen nahtlosen, einheitlichen und wirkungsvollen Schutz aller natürlichen Personen beeinträchtigen.

14. Die wichtigsten Garantien und Grundsätze sollten auf die Datenverarbeitung in allen Sektoren angewendet werden und ein ganzheitliches Vorgehen sowie einen nahtlosen, einheitlichen und wirkungsvollen Schutz sicherstellen.

15. Richtlinie 95/46/EG sollte als Richtschnur für einen umfassenden Rechtsrahmen dienen, dessen Hauptziele Wirksamkeit und ein wirkungsvoller Schutz des Einzelnen sind. Die bestehenden Grundsätze des Datenschutzes müssen bestätigt und mit Maßnahmen ergänzt werden, um diese Grundsätze

[8] Wortlaut der Kommission in KOM 262 endgültig.

[9] Artikel 16 AEUV erstreckt sich – insoweit als die Einrichtungen der Gemeinschaft personenbezogene Daten verarbeiten – nicht nur auf die dritte, sondern auch auf die zweite Säule (gemeinsame Außen- und Sicherheitspolitik). Artikel 39 EU-Vertrag sorgt für eine besondere Rechtsgrundlage für die Datenverarbeitung in der zweiten Säule durch die Mitgliedstaaten. Das ist z. B. wichtig in Bezug auf die Terroristenlisten, die durch die EU und die Mitgliedstaaten erstellt wurden. Dieser Punkt wird in dem vorliegenden Kapitel jedoch nicht näher angesprochen.

auf eine wirkungsvollere Weise zu erfüllen (und um einen wirkungsvolleren Schutz der personenbezogenen Daten der Bürger sicherzustellen).

16. Die wichtigsten Grundsätze des Datenschutzes sollten das Rückgrat eines umfassenden Rechtsrahmens sein: Schlüsselbegriffe (wer/für die Datenverarbeitung Verantwortlicher – was/personenbezogene Daten) und Grundsätze sollten bestätigt werden, darunter insbesondere die Grundsätze der Rechtmäßigkeit, Billigkeit, Verhältnismäßigkeit, Zweckbindung und Transparenz, die Rechte der betroffenen Personen sowie eine unabhängige Kontrolle durch die Behörden. Das Überdenken des Rechtsrahmens ist also auch eine Gelegenheit zur Klärung der Anwendung einiger Kernkonzepte wie:

    - Einwilligung: Unübersichtlichkeit zwischen Opt-in und Opt-out sollte vermieden werden sowie die Verwendung der Einwilligung in Situationen, in denen sie nicht die angemessene Rechtsgrundlage darstellt (siehe auch Kapitel 5);
    - Transparenz: Sie ist eine Voraussetzung für eine faire Verarbeitung. Es muss klar sein, dass Transparenz nicht unbedingt zur Einwilligung führt, aber eine Voraussetzung für eine gültige Einwilligung und die Ausübung der Rechte der Betroffenen ist (siehe auch Kapitel 5).

    Das Ziel sollte sein, den Datenschutz auf internationaler Ebene im Einklang mit den in der Richtlinie 95/46/EG niedergelegten Grundsätzen und Rechten zu verbessern, während gleichzeitig das aktuelle Schutzniveau aufrechterhalten wird (siehe auch Kapitel 3).

17. Die Annahme eines umfassenden Rechtsrahmens würde auch einige nützliche Erneuerungen der geltenden Bestimmungen ermöglichen. Dies könnte auch die Einführung des allgemeinen Grundsatzes „Privacy by Design" als Ausweitung der geltenden Bestimmungen zu den organisatorischen und technischen Sicherheitsmaßnahmen (siehe auch Kapitel 4) bedeuten und des allgemeinen Grundsatzes der Rechenschaftspflicht (siehe auch Kapitel 6).

Die Architektur eines umfassenden Rechtsrahmens

18. Ein umfassender Rechtsrahmen – gemäß dem Vertrag von Lissabon basierend auf einer einzigen Rechtsgrundlage – bedeutet nicht unbedingt, dass es innerhalb des Geltungsbereichs des allgemeinen Rechtsrahmens keinen Raum für Flexibilität und Unterschiede zwischen den Sektoren und den Mitgliedstaaten gibt. Spezielle Gesetze (leges speciales) könnten als Ergänzung dienen und das Schutzniveau verbessern, vorausgesetzt, dass sie zu dem Konzept eines umfassenden Rechtsrahmens passen und die vorgenannten wichtigsten Grundsätze erfüllen.

19. Es könnten zusätzliche sektorbezogene Vorschriften und Sondervorschriften vorgesehen werden, so z. B. in Bezug auf:

    - bestimmte Sektoren, wie z. B. das Gesundheitswesen, die Beschäftigung oder intelligente Verkehrssysteme;
    - Privacy Tools und Leistungen, wie z. B. Gütesiegel und Audits (siehe auch Kapitel 4 und 6);
    - Sicherheitsverletzungen (als Ergänzung des Grundsatzes der Sicherheit; siehe auch Kapitel 5 und 6);
    - polizeiliche und justizielle Zusammenarbeit, wie sie ausdrücklich in der Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon vorgesehen ist (siehe auch Kapitel 8);
    - innerstaatliche Sicherheitspolitik, wie ausdrücklich vorgesehen in der Erklärung Nr. 20 im Anhang zum Vertrag von Lissabon.

20. Es könnten zusätzliche innerstaatliche Verordnungen ins Auge gefasst werden, die den kulturellen Unterschieden und der innerstaatlichen Organisation der Mitgliedstaaten Rechnung tragen, vorausgesetzt, sie beeinträchtigen die Harmonisierung nicht, die in einer Europäischen Union ohne Binnengrenzen benötigt wird.

21. Als Teil eines eindeutigen und unmissverständlichen Rechtsrahmens wird eine weitere Harmonisierung benötigt. Dies schließt jedoch nicht aus, dass ein gewisses Maß an Flexibilität zusätzlichen Wert haben kann. Dies wird derzeit unter der Richtlinie 95/46/EG anerkannt, wenn dies z. B. aufgrund von kulturellen Unterschieden erforderlich ist. Es könnte auch Raum gelassen werden für innerstaatliches Recht, um die Zuweisung der Verantwortlichkeiten und die Anerkennung der unterschiedlichen Rollen des öffentlichen und des privaten Sektors festzulegen.

3. Globalisierung

Kontext und derzeitiger Rechtsrahmen

22. Im EU-Recht ist der Datenschutz ein Grundrecht, das gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union geschützt wird (siehe auch Kapitel 1). In anderen Teilen der Welt ist die Notwendigkeit des Datenschutzes weitgehend anerkannt, dieser hat aber nicht unbedingt den Status eines Grundrechts.

23. Die EU und die Mitgliedstaaten sollten jedem dieses Grundrecht garantieren, sofern sie zuständig sind. In einer globalisierten Welt bedeutet das, dass natürliche Personen auch dann Schutz fordern können, wenn ihre Daten außerhalb der Europäischen Union verarbeitet werden.

24. Richtlinie 95/46/EG behandelt diesen Schutzbedarf in Artikel 4. Die Richtlinie ist überall bei der Datenverarbeitung anzuwenden und folglich auch außerhalb der EU[10] (a) wenn der für die Datenverarbeitung Zuständige seinen Sitz in der EU hat und (b) wenn der für die Datenverarbeitung Zuständige seinen Sitz außerhalb der EU hat, aber Ausrüstung innerhalb der EU nutzt.

25. Darüber hinaus enthalten Artikel 25 und 26 der Richtlinie 95/46/EG eine Sonderregelung für die Übermittlung personenbezogener Daten an Drittländer. Die Grundregel von Artikel 25 sieht vor, dass die Übermittlung nur an solche Drittländer zulässig ist, die ein angemessenes Schutzniveau gewährleisten. Artikel 26 sieht eine Reihe von Ausnahmen zu dieser Vorschrift vor. Bekannte Konzepte wie die verbindlichen Unternehmensregelungen (BCR) und Standardvertragsklauseln setzen diese Vorschrift um.

Anzuwendendes Recht

26. Der genaue Geltungsbereich der Richtlinie 95/46/EG ist jedoch nicht ausreichend klar. Es ist nicht immer eindeutig, ob EG-Recht anzuwenden ist, welches Recht der Mitgliedstaaten anzuwenden ist und welche Rechtsvorschrift(en) im Falle mehrerer Niederlassungen eines multinationalen Unternehmens in verschiedenen Mitgliedstaaten anzuwenden wäre(n). Artikel 4 der Richtlinie, der festlegt, wann die Richtlinie in Bezug auf die Datenverarbeitung anzuwenden ist, lässt hier Raum für unterschiedliche Auslegungen.

27. Darüber hinaus gibt es Situationen, die außerhalb des Anwendungsbereichs der Richtlinie liegen. Das ist der Fall, wenn ein nicht in der EU niedergelassener für die Datenverarbeitung Verantwortlicher Daten von EU-Bürgern verarbeitet und das zur Erhebung und Weiterverarbeitung von personenbezogenen Daten führt. Das ist z. B. bei Online-Verkäufern und dergleichen der Fall, die bestimmte Werbungen mit Lokalkolorit verwenden oder Webseiten, die sich direkt an EU-Bürger wenden (indem sie die Landessprache verwenden usw.). Wenn sie dies tun, ohne technisches Gerät in der EU zu verwenden, findet die Richtlinie 95/46/EG keine Anwendung.

[10] In diesem Kontext versteht sich EU einschließlich der EFTA-Länder.

28. Derzeit schreibt die WP29 eine Stellungnahme zu dem Konzept des anzuwendenden Rechts. Die WP29 plant, die Europäische Kommission im kommenden Jahr zu dieser Frage zu beraten. Dieser Rat könnte weitere Empfehlungen für den zukünftigen Rechtsrahmen enthalten.

Internationale Normen und die Madrid-Resolution

29. Weltweite Normen zum Datenschutz werden unverzichtbar. Weltweite Normen würden auch die grenzüberschreitenden Datenströme erleichtern, die aufgrund der Globalisierung eher zur Regel werden, statt eine Ausnahme zu sein. Solange keine weltweiten Standards existieren, bleibt die Diversität bestehen. Grenzüberschreitende Datenströme müssen erleichtert werden, während gleichzeitig ein hohes Schutzniveau für die personenbezogenen Daten sichergestellt wird, wenn diese in Drittländer übermittelt und dort verarbeitet werden.

30. Die „Madrid-Resolution", ein konzertierter Vorschlag zu internationalen Normen für den Schutz der Privatsphäre, der am 6. November 2009 durch die Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre angenommen wurde, verdient Unterstützung. Der konzertierte Vorschlag enthält den Entwurf für eine weltweite Norm und bündelt alle möglichen Ansätze für den Schutz personenbezogener Daten und der Privatsphäre, wobei er die Rechtsprechung von fünf Kontinenten integriert. Er umfasst eine Reihe von Grundsätzen, Rechten und Verpflichtungen, die die Grundlage für den Datenschutz in allen Rechtssystemen in der ganzen Welt sein sollten und demonstriert, dass weltweite Normen, die ein angemessenes Schutzniveau bieten, zur gegebenen Zeit möglich sind.

31. Die Kommission wird dazu aufgerufen:

- Initiativen für die weitere Entwicklung internationaler globaler Normen bezüglich des Schutzes personenbezogener Daten mit der Absicht zu ergreifen, einen internationalen Rechtsrahmen für den Datenschutz zu fördern und folglich den grenzüberschreitenden Datenstrom zu erleichtern, während gleichzeitig ein angemessenes Schutzniveau der Betroffenen gewährleistet wird. Diese Initiativen sollten eine Prüfung der Durchführbarkeit eines bindenden internationalen Rechtsrahmens umfassen.
- in Ermangelung von globalen Normen die Entwicklung von Rechtsvorschriften zum Datenschutz, die ein angemessenes Schutzniveau bieten, sowie die Gründung unabhängiger Datenschutzbehörden in Ländern, die nicht der Europäischen Union angehören, zu fördern. Die wichtigsten Datenschutzgrundsätze, so wie sie in der „Madrid-Resolution" niedergelegt wurden, sollten die allgemeine Grundlage dieser Rechtsvorschriften bilden.

In dem zukünftigen Rechtsrahmen sollten diese besonderen Aufgaben der Kommission aufgeführt werden.

Verbesserung der Entscheidungen zur Angemessenheit

32. In dem globalisierten Umfeld finden immer mehr Verarbeitungsvorgänge personenbezogener Daten statt. Es wird immer wichtiger, sicherzustellen, dass die Ströme personenbezogener Daten frei fließen und gleichzeitig das Schutzniveau der Rechte des Einzelnen zu garantieren. Deshalb ist es erforderlich, den Prozess der Angemessenheit umzugestalten:

    - Präzisere Definition der Kriterien zur rechtlichen Verankerung des Grundsatzes der „Angemessenheit". Hierbei sollte gebührende Aufmerksamkeit auf das Vorgehen der WP29[11] gerichtet werden sowie auf die verschiedenen anderen Ansätze zum Datenschutz in der ganzen Welt und insbesondere auf die Rechte und Grundsätze, die im konzertierten Vorschlag zu Internationalen Normen für den Schutz der Privatsphäre niedergelegt wurden;
    - Rationalisieren der Analyseverfahren in Bezug auf die Rechtssysteme von Drittländern, damit mehr Entscheidungen zur Angemessenheit des Schutzniveaus getroffen werden können.

    Der zukünftige Rechtsrahmen sollte diese Themen näher darlegen.

Internationale Abkommen

33. Die Aktivitäten der hochrangigen Kontaktgruppe EU–USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten wurden zur Kenntnis genommen. Diese Aktivitäten könnten zu einem transatlantischen Abkommen mit gemeinsamen Grundsätzen zur Privatsphäre und zum Datenschutz führen, das bei einem Informationsaustausch mit den Vereinigten Staaten im Kampf gegen den Terrorismus und die transnationale Schwerkriminalität anzuwenden wäre.[12]

34. Internationale Abkommen sind angemessene Instrumente zum Schutz personenbezogener Daten in einem globalen Kontext, vorausgesetzt, dass das gewährte Schutzniveau den vorgenannten globalen Normen mindestens entspricht und dass jede natürliche Person einen einfachen und wirkungsvollen

[11] Siehe insbesondere Arbeitspapier 12 der WP 29: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, angenommen am 24. Juli 1998.

[12] In dieser Hinsicht bleibt das transatlantische Problem hinsichtlich des Rechtsschutzes zu lösen.

Zugang zu Rechtsmitteln hat, einschließlich des gerichtlichen Rechtsbehelfs. Es müssen besondere Garantien in Bezug auf den Zweck, für den die personenbezogenen Daten herangezogen werden, bestehen.

35. Unter diesen Bedingungen könnte das vorhergesehene transatlantische Abkommen als Modell für den Austausch mit anderen Drittländern und für andere Zwecke dienen. Der zukünftige Rechtsrahmen könnte die Bedingungen für Abkommen mit Drittländern aufführen.

36. Darüber hinaus sollte die EU die Zusammenarbeit zwischen internationalen Datenschutzbehörden ermutigen, zum Beispiel auf transatlantischer Ebene. Eine solche Zusammenarbeit ist ein erfolgreiches Mittel zur Förderung des Datenschutzes außerhalb der EU.

Verbindliche unternehmensinterne Datenschutzregelungen / Rechenschaftspflicht

37. Die Verarbeitung von Daten außerhalb der EU kann auch durch verbindliche unternehmensinterne Datenschutzregelungen (BCR), also internationale Verhaltenskodizes für multinationale Unternehmen, geschützt werden, die dieweltweite Übertragung innerhalb eines multinationalen Unternehmens gestatten. Die WP29 hat BCR im Jahr 2003 eingeführt. Sowohl Datenschutzbehörden als auch multinationale Unternehmen sind der Ansicht, dass BCR ein gutes Mittel zur Vereinfachung der internationalen Datenströme sind und gleichzeitig den Schutz der personenbezogenen Daten gewährleisten. Die Richtlinie 95/46/EG hat die BCR jedoch nicht wirklich berücksichtigt. Infolgedessen erfordert der Prozess für die Genehmigung der BCR, der auf Artikel 26 Absatz 2 der Richtlinie 95/46/EG basiert, die Zustimmung aller durch eine BCR betroffenen Mitgliedstaaten. Folglich benötigt die Bewertung und die Genehmigung der BCR viel Zeit. Die WP29 hat beträchtliche Anstrengungen unternommen, die Anwendung und die Genehmigung der BCR in dem gültigen Rechtsrahmen zu fördern und zu vereinfachen. Zur Verbesserung des Prozesses haben bislang neunzehn Datenschutzbehörden einem „gegenseitige Anerkennung“ genannten Verfahren zur Anerkennung von BCR zugestimmt.

38. Vor diesem Hintergrund sollte eine Vorschrift zu den BCR weiter gestärkt und in den neuen Rechtsrahmen eingefügt werden. Dies würde mehrere Zwecke erfüllen:

    - Anerkennung der BCR als passendes Mittel zur Bereitstellung angemessener Schutzmaßnahmen;
    - Definieren der wichtigsten materiell- und verfahrensrechtlichen Elemente der BCR in Anlehnung an die diesbezügliche Stellungnahme der WP29.

39. Allgemein gesehen, könnte dem neuen Rechtsrahmen eine neue Vorschrift hinzugefügt werden, nach welcher die für die Datenverarbeitung Verantwortlichen für die personenbezogenen Daten, die sie verarbeiten, rechenschaftspflichtig und verantwortlich bleiben, selbst wenn diese an andere für die Datenverarbeitung Verantwortliche außerhalb der EU übermittelt wurden (siehe „Rechenschaftspflicht" allgemeiner in Kapitel 6).

Abschließende Bemerkung

40. Im vorliegenden Kapitel wird die Globalisierung an sich diskutiert. Auf die eine oder andere Weise behandeln aber alle Kapitel dieses Beitrags dieses Thema. Wenn man an „Globalisierung" denkt, denkt man häufig an Wirtschaft. In einer globalisierten Welt finden aber immer mehr Verarbeitungen von personenbezogenen Daten statt. Auch wenn der Einzelne häufig ein örtlich begrenztes Leben führt, kann er immer häufiger online angetroffen werden, und dort werden seine Daten global verarbeitet. Globalisierung ist folglich mit Technologie verknüpft (Kapitel 4), mit der Stellung der betroffenen Personen (Kapitel 5), dem für die Datenverarbeitung Verantwortlichen (Kapitel 6), den Datenschutzbehörden / der WP29 (Kapitel 7) und der Strafverfolgung (Kapitel 8).

4. Technologische Änderungen; Privacy by Design als neuer Grundsatz

41. Die grundlegenden Konzepte der Richtlinie 95/46/EG wurden in den Siebzigerjahren entwickelt, als Datenverarbeitung von Karteikästen, Lochkarten und Großrechnern geprägt war. Heute sind Computer allgegenwärtig, global und vernetzt. IT-Geräte werden zunehmend kleiner und mit Netzkarten, Wi-Fi oder sonstigen Funkschnittstellen ausgerüstet. In fast allen Büros und Familien können die Nutzer global über das Internet kommunizieren. Web 2.0-Dienste und Cloud Computing verschleiern die Unterscheidung zwischen für die Datenverarbeitung Verantwortlichen, Auftragsverarbeitern und betroffenen Personen.

42. Richtlinie 95/46/EG hat dem Zustrom technologischer Änderungen aufgrund ihrer soliden und technologisch neutralen Grundsätze und Konzepte gut standgehalten. Diese Grundsätze und Konzepte bleiben in der heutigen vernetzten Welt gleichermaßen maßgeblich, gültig und anwendbar.

43. Während es zwar klar ist, dass die oben beschriebenen technologischen Entwicklungen gut für die Gesellschaft sind, haben sie dennoch die Risiken für die Privatsphäre des Einzelnen und für den Datenschutz erhöht. Um diese Risiken auszugleichen, sollte der Rechtsrahmen zum Datenschutz ergänzt

werden. Als Erstes sollte dem Rechtsrahmen der Grundsatz „Privacy by Design“ beigefügt werden. Als Zweites sollten soweit erforderlich in Bezug auf bestimmte technologische Kontexte Verordnungen erlassen werden, welche die Verankerung von Grundsätzen des Datenschutzes und der Privatsphäre in diese Kontexte vorschreiben.

Grundsatz „Privacy by Design“

44. Die Idee, in Informations- und Kommunikationstechnologien („IKT“) Datenschutzmaßnahmen zu integrieren, ist nicht ganz neu. Richtlinie 95/46/EG enthält bereits verschiedene Bestimmungen, gemäß denen die für die Datenverarbeitung Verantwortlichen verpflichtet sind, bei der Planung und dem Einsatz von IKT Sicherheitstechniken zu integrieren. So legt Artikel 17 die Verpflichtung des für die Datenverarbeitung Verantwortlichen fest, angemessene technische und organisatorische Maßnahmen durchzuführen. Erwägungsgrund Nr. 46 fordert, dass diese Maßnahmen sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt des eigentlichen Verarbeitens getroffen werden. Artikel 16 legt die Vertraulichkeit der Verarbeitung fest. Dieser Grundsatz hat in den einschlägigen Verordnungen zur IT-Sicherheit seinen Niederschlag gefunden bzw. wird durch diese ergänzt. Abgesehen von diesen Artikeln finden auch die Grundsätze in Bezug auf die Datenqualität Anwendung, die in Artikel 6 niedergelegt sind (Rechtmäßigkeit und Billigkeit, Zweckbindung, Erheblichkeit, sachliche Richtigkeit, Begrenzung der Speicherdauer, Verantwortung).

45. Während die vorgenannten Bestimmungen der Richtlinie „Privacy by Design“ unterstützen, haben sie in der Praxis nicht ausgereicht, um sicherzustellen, dass der Schutz der Privatsphäre in IKT verankert wird. Die Nutzer von IKT-Diensten – Unternehmen, der öffentliche Sektor und ganz sicher Einzelpersonen – sind nicht dazu in der Lage, die erforderlichen Sicherheitsmaßnahmen selbst zu ergreifen, um ihre eigenen und die personenbezogenen Daten anderer zu schützen. Deshalb sollten diese Dienste und Technologien mit „Privacy by Default“-Voreinstellungen ausgestattet werden.

46. Aus diesem Grund muss der neue Rechtsrahmen eine Bestimmung enthalten, die die geltenden, eng gefassten Anforderungen in den breiteren und einheitlichen Grundsatz Privacy by Design umwandelt. Dieser Grundsatz sollte sowohl für die Entwickler und Hersteller der Technologien, als auch für die für die Datenverarbeitung Verantwortlichen, die über den Erwerb und die Nutzung der IKT zu entscheiden haben, verbindlich sein. Sie sollten dazu verpflichtet sein, bereits in der Planungsphase der Informations- und Kommunikationsverfahren und -systeme Technologien zum Datenschutz zu berücksichtigen. Sowohl die Anbieter solcher Systeme oder Dienstleistungen als auch die für die Datenverarbeitung Verantwortlichen sollten zeigen,

dass sie alle erforderlichen Maßnahmen ergriffen haben, um diese Anforderungen zu erfüllen.

47. Dieser Grundsatz sollte die Umsetzung des Datenschutzes bei IKT („Privacy by Design" oder „PbD") erforderlich machen, die für die Verarbeitung personenbezogener Daten geplant sind oder für diese genutzt werden. Er sollte die Anforderung enthalten, dass IKT nicht nur die Sicherheit aufrechterhalten, sondern auch so geplant und entwickelt werden sollten, dass sie die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich halten oder deren Verarbeitung ganz vermeiden. Dies entspricht der kürzlich in Deutschland ergangenen Rechtsprechung.[13]

48. Die Anwendung eines solchen Grundsatzes würde die Notwendigkeit für den Einsatz von Technologien zum Schutz der Privatsphäre (PET), von „Privacy by Default"-Voreinstellungen und der erforderlichen Tools unterstreichen, die die Nutzer dazu befähigen, ihre personenbezogenen Daten besser zu schützen (z. B. Zugangskontrollen, Verschlüsselung). Dies sollte eine wesentliche Anforderung an Produkte und Dienstleistungen sein, die Dritten und Einzelkunden bereitgestellt werden (z. B. WiFi-Router, soziale Netzwerke und Suchmaschinen). Dies würde den Datenschutzbehörden im Gegenzug mehr Befugnisse bei der tatsächlichen Durchsetzung solcher Maßnahmen geben.

49. Ein solcher Grundsatz sollte auf eine *technologisch neutrale* Weise definiert werden, damit er in einem sich schnell ändernden technologischen und sozialen Umfeld lange Bestand hat. Er sollte auch *flexibel* genug sein, damit die für die Datenverarbeitung Verantwortlichen und die Datenschutzbehörden die Möglichkeit haben, ihn je nach Fall in konkrete Datenschutzmaßnahmen umzusetzen.

50. Der Grundsatz sollte wie der geltende Erwägungsgrund Nr. 46 die Notwendigkeit betonen, dass ein solcher Grundsatz *so früh wie möglich* angewendet wird: „zum Zeitpunkt der Planung des Verarbeitungssystems und zum Zeitpunkt der eigentlichen Verarbeitung". Schutzmaßnahmen, die in einer späten Phase umgesetzt werden, sind in Bezug auf die Forderung nach einem wirkungsvollen Schutz der Rechte und Freiheiten der betroffenen Personen inkonsistent und unzureichend.

[13] Eine neuere Entscheidung des Deutschen Bundesverfassungsgerichts (Entscheidung vom 27. Februar 2008 – 1 BvR 370/07; 1 BvR 595/07 –) hat ein Verfassungsrecht in Bezug auf die Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Systeme, die dazu in der Lage sind, sensible personenbezogene Daten zu schaffen, zu verarbeiten oder zu speichern, sind besonders zu schützen. Dieser Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme ist anzuwenden bei Systemen, die allein oder in ihrer technischen Vernetzung personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen wesentlichen Einblick in das Privatleben einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Zu diesen Systemen zählen z. B. Personal Computer und Laptops, Handys und elektronische Kalender.

51. Software- und Hardwareentwickler sollten während der Phase der Systemanalyse technologische Standards entwickeln und berücksichtigen, so dass Schwierigkeiten bei der Definierung und Spezifizierung der Anforderungen aus dem Grundsatz „Privacy by Design" minimiert werden. Solche Standards können in Bezug auf verschiedene Verarbeitungszwecke und -technologien sowohl genereller als auch spezifischer Natur sein.

52. Die folgenden Beispiele zeigen, wie PdB zu einem besseren Datenschutz beitragen kann:

    - Biometrische Identifikatoren sollten nicht in externen Datenbanken gespeichert werden, sondern stattdessen auf Speichermedien, über die die betroffene Person selbst die Kontrolle hat (d. h. intelligente Chipkarten „Smart Cards").
    - Die Videoüberwachung in öffentlichen Verkehrssystemen sollte so konzipiert sein, dass die Gesichter der aufgezeichneten Personen nicht erkennbar sind oder es sollten andere Maßnahmen ergriffen werden, um die Risiken für die Betroffenen zu verringern. Natürlich müssen unter besonderen Umständen Ausnahmen gemacht werden, z. B., wenn die betreffende Person einer Straftat verdächtigt wird.
    - Die Namen von Patienten und sonstige Personen-Identifikatoren, die in den Informationssystemen von Krankhäusern gespeichert werden, sollten von Daten über den Gesundheitszustand und über medizinische Behandlungen getrennt werden. Sie sollten nur insoweit kombiniert werden, wie es für medizinische oder andere angemessene Gründe in einem sicheren Umfeld erforderlich ist.
    - Gegebenenfalls sollte eine Funktion integriert werden, die es den Betroffenen erleichtert, ihr Recht auf Widerruf der Einwilligung auszuüben, mit der daraus resultierenden Löschung der Daten auf allen betreffenden Servern (einschließlich Proxies und Mirrors).

53. In der Praxis erfordert die Umsetzung des Grundsatzes „Privacy by Design" die Bewertung verschiedener konkreter Aspekte oder Ziele. Insbesondere bei der Entscheidung über die Entwicklung, den Erwerb oder den Betrieb eines Verarbeitungssystems sollten die folgenden allgemeinen Aspekte/Ziele berücksichtigt werden:

    - Datensparsamkeit: Die Entwicklung und Auswahl der Datenverarbeitungssysteme muss mit dem Ziel übereinstimmen, überhaupt keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
    - Kontrollierbarkeit: Ein IT-System sollte den Betroffenen wirkungsvolle Mechanismen für die Kontrolle ihrer personenbezogenen Daten zur Verfü-

gung stellen. Die Möglichkeiten bezüglich Einwilligung und Widerspruch sollten durch technologische Mittel unterstützt werden.

- Transparenz: Sowohl die Entwickler als auch die Betreiber von IT-Systemen müssen sicherstellen, dass die Betroffenen ausreichend über die Wirkungsweise des Systems informiert sind. Elektronische Auskunft/Information sollten ermöglicht werden.
- Anwenderfreundliche Systeme: Funktionen und Einrichtungen mit Bezug zur Privatsphäre sollten anwenderfreundlich sein, d. h., sie sollten in ausreichendem Umfang Hilfefunktionen und einfache Schnittstellen für die Nutzung durch weniger erfahrene Anwender bereitstellen.
- Datenvertraulichkeit: IT-Systeme müssen so entwickelt und gesichert werden, dass nur autorisierte Stellen Zugang zu personenbezogenen Daten haben.
- Datenqualität: Die für die Datenverarbeitung Verantwortlichen müssen die Datenqualität mit Hilfe technischer Mittel unterstützen. Die entsprechenden Daten sollten zugänglich sein, wenn sie für Rechtszwecke benötigt werden.
- Verwendungsbeschränkung: IT-Systeme, die für verschiedene Zwecke genutzt werden können oder die in einer Mehrbenutzerumgebung (d. h. virtuelle verbundenen Systeme wie Data-Warehouses, Cloud Computing, digitale Identifikatoren) betrieben werden, müssen sicherstellen, dass Daten und Prozesse, die für verschiedene Aufgaben oder Zwecke genutzt werden, auf eine sichere Weise voneinander getrennt werden können.

Verordnungen über bestimmte technologische Kontexte

54. Der Grundsatz „Privacy by Design" reicht möglicherweise nicht aus, um in allen Fällen sicherzustellen, dass die angemessenen technologischen Datenschutzmaßnahmen ordnungsgemäß in die IKT integriert sind. Es könnte Fälle geben, in denen ein aktiveres Vorgehen erforderlich wäre. Um die Umsetzung solcher Maßnahmen zu erleichtern, sollte ein neuer Rechtsrahmen eine Bestimmung enthalten, die die Umsetzung bestimmter Verordnungen für bestimmte technologische Kontexte ermöglicht, die die Eingliederung von Grundsätzen zum Schutz der Privatsphäre erfordern.

55. Das ist kein neues Konzept: Artikel 14 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation enthält eine ähnliche Bestimmung: „Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation (10) Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer

Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist."

56. Obenstehendes würde in bestimmten Fällen den Erlass besonderer normativer Akte erleichtern und dabei das Konzept „Privacy by Design" verankern und gleichzeitig sicherstellen, dass angemessene Spezifikationen bereitgestellt werden. Dies könnte z. B. bei der RFID-Technologie, bei sozialen Netzwerken, personalisierter Werbung usw. der Fall sein.

Abschließende Bemerkungen

57. Die wachsende Bedeutung des Datenschutzes beim Erstellen und Betreiben von IT-System stellt an IT-Spezialisten zusätzliche Anforderungen. Also muss der Datenschutz fest in die Lehrpläne von IT-Berufen verankert werden.

58. Die Grundsätze des technologischen Datenschutzes und die daraus resultierenden konkreten Kriterien sollten im Rahmen von Datenschutzaudits[14] als Grundlage für die Vergabe von Gütesiegeln (Zertifizierungssystemen) genutzt werden.

5. Stärkung der betroffenen Personen

59. Das Potential, das die Richtlinie 95/46/EG der Stellung der betroffenen Person einräumt, wurde nicht vollständig ausgeschöpft. Darüber hinaus haben sich sowohl das Verhalten der Bürger als auch die Rolle der Betroffenen in Bezug auf den Datenschutz gewandelt. Dies war unter anderem wegen soziologischer Veränderung der Fall und da bei der Erhebung von Daten neue Wege beschritten werden (z. B. für Zwecke der Profilerstellung). Die Betroffenen gehen manchmal recht sorglos mit ihrer Privatsphäre um. Manchmal sind sie dazu bereit, die Privatsphäre gegen vermeintliche Vorteile einzutauschen. Auf der anderen Seite haben sie immer noch hohe Erwartungen an diejenigen, mit denen sie Geschäfte tätigen. Außerdem spielen die Betroffenen selbst in steigendem Maße eine aktive Rolle bei der Verarbeitung personenbezogener Daten, insbesondere im Internet.

60. Änderungen im Verhalten und in der Rolle der Betroffenen und die Erfahrungen mit der Richtlinie 95/46/EG machen es erforderlich, dass die Posi-

[14] Das ist z. B. bei dem Projekt EuroPriSe der Fall.

tion der Betroffenen in dem Datenschutzrechtsrahmen gestärkt wird.[15] Die weitere Stärkung der Betroffenen ist unerlässlich, so dass sie eine aktivere Rolle spielen können.

Verbesserung der Rechtschutzmechanismen

61. Eine Stärkung des Betroffenen erfordert, dass er mehr Möglichkeiten hat, seine Rechte auszuüben und geltend zu machen. Da Gerichtsverfahren manchmal sehr schwierig sein können und ein finanzielles Risiko in sich bergen, sollte in die Richtlinie 95/46/EG die Möglichkeit einer Sammelklage aufgenommen werden.[16]

62. Darüber hinaus sollten die für die Datenverarbeitung Zuständigen für Beschwerdeverfahren sorgen, die leichter zugänglich, effektiver und bezahlbar sind (siehe auch Kapitel 6). Wenn diese Verfahren den Streit zwischen dem Betroffenen und dem für die Datenverarbeitung Verantwortlichen nicht lösen, sollte der Betroffene die Möglichkeit haben, auf alternative Verfahren der Streitbeilegung zurückzugreifen. Diese werden hauptsächlich in der Industrie angeboten.[17] Diese Möglichkeiten sollten in einen neuen Rechtsrahmen integriert werden.

Transparenz

63. Transparenz ist eine weitere Grundvoraussetzung. Sie gibt dem Betroffenen *„ex ante"* ein Mitspracherecht, also vor der Verarbeitung. Das Erstellen von Profilen, Data Mining und technologische Entwicklungen, welche die Austauschbarkeit personenbezogener Daten vereinfachen, machen es für die Betroffenen noch wichtiger, dass sie wissen, durch wen, auf welcher Grundlage, von wo aus, für welche Zwecke und mit welchen technischen Mitteln die Daten verarbeitet werden. Es ist wichtig, dass diese Informationen verständlich sind. Die Pflicht, den Betroffenen zu informieren (Artikel 10 und 11 der Richtlinie 95/46/EG) wird jedoch nicht immer ordnungsgemäß umgesetzt. Ein neuer Rechtsrahmen sollte alternative Lösungen zur Förderung der Transparenz bieten. So sollten z. B. in Bezug auf die personalisierte Werbung neue Wege zum Informieren des Betroffenen entwickelt werden.

---

[15] Dies ist insbesondere dann der Fall, wenn Kinder betroffen sind. Wenn Entscheidungen über die personenbezogenen Daten von Kindern getroffen werden, ist das Wohl des Kindes vorrangig zu berücksichtigen, wie in der UN-Kinderrechtskonvention (http://www2.ohchr.org/english/law/crc.htm) und in weiteren speziellen internationalen Vertragswerken und im innerstaatlichen Recht niedergelegt ist.

[16] Im Umweltrecht beispielsweise besteht die Möglichkeit einer Sammelklage.

[17] Dadurch darf dem Einzelnen natürlich nicht das Recht auf das Einlegen geeigneter Rechtsmittel vor einem Gericht oder einer Datenschutzbehörde genommen werden.

64. Darüber hinaus erfordert Transparenz, dass betroffene Personen benachrichtigt werden, wenn eine Datenschutzverletzung eintritt, die vermutlich negative Auswirkungen auf ihre personenbezogenen Daten und ihre Privatsphäre haben. Das würde dem Betroffenen die Möglichkeit geben, einen Versuch zur Kontrolle des erlittenen Schadens zu unternehmen (in bestimmten Fällen sollten auch die Behörden informiert werden, siehe auch Kapitel 6). In den neuen Rechtsrahmen sollte eine allgemeine Meldung von Datenschutzverletzungen eingefügt werden (siehe auch Kapitel 6).[18]

Einwilligung

65. Gemäß Richtlinie 95/46/EG ist die Einwilligung eine rechtmäßige Grundlage für die Datenverarbeitung (Artikel 7 und 8 der Richtlinie 95/46/EG). Die Einwilligung ist und bleibt eine wichtige Grundlage für die Verarbeitung, die unter bestimmten Umständen die Stellung des Betroffenen stärken könnte. Die Einwilligung muss jedoch ohne Zwang, in Kenntnis der Sachlage und für den konkreten Fall gegeben werden (Artikel 2 Buchstabe h Richtlinie 95/46/EG).

66. Es gibt viele Fälle, in denen die Einwilligung nicht ohne Zwang gegeben werden kann, insbesondere wenn ein deutliches Ungleichgewicht zwischen der betroffenen Person und dem für die Datenverarbeitung Verantwortlichen besteht (z. B. bei einem Beschäftigungsverhältnis oder wenn die personenbezogenen Daten öffentlichen Behörden erteilt werden müssen).

67. Darüber hinaus wird bei der Forderung, dass die Einwilligung ohne Zwang zu erfolgen hat, von der Annahme ausgegangen, dass die betroffene Person in vollem Umfang verstehen muss, was bei ihrer Einwilligung in die Bearbeitung ihrer Daten passiert. In vielen Fällen jedoch übersteigt die Komplexität von Datenerhebungsverfahren, Wirtschaftsmodellen, Käufer–Verkäuferbeziehungen und technologischen Anwendungen die Fähigkeit oder Bereitschaft des Einzelnen, aktiv über die Verwendung und gemeinsame Nutzung der Informationen zu entscheiden.[19]

68. In beiden Hypothesen ist die Einwilligung eine unangemessene Grundlage für die Verarbeitung. Sie wird aber dennoch häufig fälschlicherweise als die

---

[18] In der „Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre in der elektronischen Kommunikationen (Datenschutzrichtlinie für die elektronische Kommunikation)“ hat die WP29 eine empfohlene Vorgehensweise im Zusammenhang mit der Meldung von bestimmten Datenschutzverletzungen, die in der Datenschutzrichtlinie für die elektronische Kommunikation behandelt werden, festgestellt. Dieselben Empfehlungen gelten auch für die Einführung allgemeiner Meldungen von Datenschutzverletzungen.

[19] Siehe „Data Protection Accountability: The essential Elements – A Document for Discussion”, Centre for Information Policy Leadership, als die Sekretariatsgeschäfte des Galway-Projekts wahrnehmende Stelle, Oktober 2009, S. 4

anzuwendende Grundlage angegeben. Die technologischen Entwicklungen fordern auch eine genaue Erwägung der Einwilligung. In der Praxis wird Artikel 7 der Richtlinie 95/46/EG nicht immer richtig angewendet. Dies ist insbesondere im Umfeld des Internet der Fall, wo eine stillschweigende Einwilligung nicht immer zu einer eindeutigen Einwilligung führt (wie dies in Artikel 7 Buchstabe a der Richtlinie gefordert wird). Wenn die Position der betroffenen Personen jedoch *„ex ante"*, also vor der Verarbeitung ihrer personenbezogenen Daten durch Dritte, gestärkt wird, muss die Einwilligung ausdrücklich (und deshalb ein Opt-in) für alle Verarbeitungen erfolgen, die auf der Einwilligung basieren.[20]

69. Der neue Rechtsrahmen sollte die Voraussetzung der Einwilligung näher darlegen und dabei die oben gemachten Anmerkungen berücksichtigen.

Harmonisierung

70. Derzeit wird eine Stärkung der Position der betroffenen Parteien durch die mangelnde Harmonisierung der innerstaatlichen Gesetze untergraben, mit denen die Richtlinie 95/46/EG umgesetzt wird. Verschiedene Elemente der Richtlinie, die essentiell für die Stellung der betroffenen Personen sind, wie die Bestimmung zur Haftung und die Möglichkeit, immaterielle Schäden einzuklagen[21], wurden nicht von allen Mitgliedstaaten umgesetzt. Abgesehen von diesen Unterschieden bei der Umsetzung der Richtlinie 95/46/EG, wird die Richtlinie in den Mitgliedstaaten nicht immer einheitlich ausgelegt. Bei einer wachsenden Globalisierung schwächen diese Unterschiede die Position der betroffenen Personen immer weiter. Eine Verbesserung der Harmonisierung ist deshalb von größter Bedeutung (siehe auch Kapitel 7). Sofern erforderlich sollte dies durch den Erlass von Rechtsvorschriften geschehen.

Die Rolle der betroffenen Personen im Internet

71. Natürliche Personen laden ihre eigenen personenbezogenen Daten in steigendem Maße im Internet hoch (soziale Netzwerke, Cloud Computing-Dienste usw.). Die Richtlinie 95/47/EG findet jedoch keine Anwendung auf Personen, die die Daten aus „ausschließlich persönlichen" Gründen oder „bei der Ausübung einer familiären Tätigkeit"[22] hochladen. Vertretbarer-

[20] Bezüglich der Einwilligung und Opt-in / Opt-out siehe auch Kapitel 2, in dem festgestellt wird, dass eine Verwechslung zwischen Opt-in und Opt-out vermieden werden sollte sowie die Verwendung der Einwilligung in Situationen, in denen sie nicht die angemessene Rechtsgrundlage darstellt.

[21] In den meisten Fällen, in denen die betroffenen Personen Schaden erlitten haben, handelt es sich um einen immateriellen Schaden, wie das Gefühl, sich nicht länger im öffentlichen und privaten Sektor bewegen zu können, ohne dabei beobachtet zu werden. Dieses Problem wird in der aktuellen „Überwachungsgesellschaft" größer.

[22] Für ein besseres Verständnis, ob eine Tätigkeit unter die „Ausnahmeklausel für Privathaushalte" fällt oder nicht, siehe Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163).

weise findet sie auch auf die Organisationen keine Anwendung, die den Dienst anbieten, d. h., die von einem Einzelnen hochgeladenen Informationen hosten und verfügbar machen (sofern der Dienst keine Daten für seine eigenen Zwecke verarbeitet), da der Service Provider nicht als für die Datenverarbeitung Verantwortlicher angesehen werden kann.[23] Das Ergebnis ist eine Situation, in der Garantien fehlen. Dies müsste möglicherweise geklärt werden, insbesondere angesichts der steigenden Zahl solcher Situationen. In diesem Zusammenhang sollte jeder, der einer Privatperson Leistungen anbietet, zur Bereitstellung bestimmter Schutzgarantien sowie, sofern angemessen, zur Bereitstellung von Garantien bezüglich der Vertraulichkeit der durch die Nutzer hochgeladenen Informationen verpflichtet sein, unabhängig davon, ob der Kunde ein für die Datenverarbeitung Verantwortlicher ist oder nicht. Zusätzlich sollte darüber nachgedacht werden, ob die Betroffenen mehr Möglichkeiten zur Ausübung ihrer Rechte im Internet erhalten sollten. Dazu gehört auch der Schutz der Rechte Dritter, deren personenbezogenen Daten verarbeitet werden könnten (z. B. soziale Netzwerke). Da es noch mehr ungelöste Fragen in diesem Zusammenhang geben könnte,[24] sollte angesichts eines neuen Rechtsrahmens die Rolle der betroffenen Person im Internet weiter geklärt werden.

6. Stärken der Verantwortung des für die Datenverarbeitung Verantwortlichen

72. Gemäß Richtlinie 95/46/EG obliegt es in erster Linie dem für die Datenverarbeitung Verantwortlichen, für die Einhaltung der Grundsätze und Verpflichtungen zu sorgen, die der Sicherstellung des Schutzes der personenbezogenen Daten von Einzelnen dienen. Die Richtlinie setzt implizit und in vielen Fällen auch explizit voraus, dass der für die Datenverarbeitung Verantwortlicher die Datenschutzgrundsätze einhält und bestimmte andere Verpflichtungen erfüllt.[25] Beispiele für die letztgenannten Verpflichtungen sind die Meldung an und die Vorabprüfung der Verarbeitung durch nationale Stellen.[26] Damit die Einhaltung der Datenschutzrechte des Einzelnen sicherge-

[23] Dieses Problem tritt nicht auf, wenn Organisationen – sowohl im öffentlichen als auch im privaten Sektor – Cloud Computing Anwendungen verwenden, denn die Richtlinie findet auf sie und ihre Verarbeitungsoperationen Anwendung, die „im Rahmen der Tätigkeit einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche" in der EU besitzt (siehe Artikel 4 Absatz 1 Buchstabe a). Kapitel 5 findet folglich Anwendung, unabhängig davon, ob der Service Provider seinen Sitz in der EU hat oder nicht.

[24] Z. B. in Bezug auf die Einwilligung von Kindern und/oder ihren Eltern, Auskunftsforderungen durch Strafverfolgungsbehörden, Informationsrechte in Bezug auf Internetaccounts durch Erben und Anwendungen von Drittanbietern.

[25] Artikel 6 Absatz 2 legt ausdrücklich Folgendes fest: „Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen." Dieser bezieht sich auf die wichtigsten Grundsätze zur Datenqualität.

[26] Siehe Artikel 18–21 der Richtlinie 95/46/EG.

stellt wird, müssen dem für die Datenverarbeitung Zuständigen bestimmte Pflichten wie die Informationspflicht auferlegt werden.[27]

73. Diese Verpflichtungen bestehen direkt oder indirekt auch für den Auftragsverarbeiter, wenn der für die Datenverarbeitung Verantwortliche einen Teil oder alle Datenverarbeitungsvorgänge auf diesen übertragen hat. Die WP29 verfasst derzeit eine interpretative Stellungnahme, um eine Orientierungshilfe zum Konzept des für die Datenverarbeitung Verantwortlichen und des Auftragsverarbeiters zu geben. Die WP29 möchte die Kommission bald zu diesem Thema beraten. Der Ratschlag könnte weitere Empfehlungen für einen zukünftigen Rechtsrahmen enthalten.

Einbetten des Datenschutzes in Organisationen

74. Die einschlägigen Bestimmungen der Richtlinie 95/46/EG bilden zweifellos eine solide Grundlage für den Schutz personenbezogener Daten und sollten beibehalten werden. Die Einhaltung der bestehenden Rechtsvorschriften ist jedoch häufig nicht richtig in die interne Praxis von Organisationen eingebettet. Die Privatsphäre ist häufig nicht in den Informationsverarbeitungstechnologien und -systemen verankert. Darüber hinaus ist das Management – und darunter fallen auch die Manager auf höchster Ebene – im allgemeinen nicht in ausreichendem Maße mit den Datenverarbeitungspraktiken ihrer eigenen Organisation vertraut und kann folglich auch keine aktive Verantwortung übernehmen. Die Datenschutzskandale der letzten Jahre in den Mitgliedstaaten lassen diese Besorgnis noch wachsen.

75. Solange der Datenschutz nicht Teil der gemeinsamen Werte und Praktiken einer Organisation wird, und solange die Verantwortung für den Datenschutz nicht ausdrücklich zugewiesen wird, ist die tatsächliche Einhaltung der Vorschriften gefährdet und es wird weiterhin zu Pannen kommen. Das wiederum wird das öffentliche Vertrauen in Unternehmen und öffentliche Verwaltungen gleichermaßen untergraben. Darüber hinaus würde eine Verankerung des Datenschutzes in die Organisationskultur den nationalen Datenschutzbehörden die Ausübung ihrer Kontroll- und Rechtsdurchsetzungsaufgaben erleichtern, da dies – wie in Kapitel 7 weiter ausgeführt – die Wirksamkeit des Datenschutzes erhöhen würde.

76. Die Grundsätze und Vorschriften der Richtlinie 95/46/EG sollten das kulturelle Gefüge von Organisationen auf allen Ebenen durchdringen, statt nur als

[27] Andere Beispiele für die Rechte der Betroffenen sind unter anderem das Auskunftsrecht, das Recht auf Berichtigung, Löschung oder Sperrung sowie das Recht, Widerspruch gegen die Verarbeitung personenbezogener Daten einzulegen (Artikel 10–12 und 14). Diese Rechte ziehen die Verpflichtung für den für die Datenverarbeitung Verantwortlichen nach sich, für ihre Einhaltung zu sorgen.

eine Reihe von gesetzlichen Anforderungen gesehen zu werden, die von der Rechtsabteilung abgehakt werden. Die Anforderungen der Richtlinie sollten zur tagtäglichen Anwendung konkreter Datenschutzvorkehrungen führen. In die Planung von Informationstechnologien und -systemen sollte die Kontrolle der Privatsphäre integriert werden (siehe auch Kapitel 4). Darüber hinaus sollte innerhalb der Organisationen sowohl im öffentlichen als auch im privaten Sektor die interne Verantwortung für den Datenschutz in geeigneter Weise anerkannt, gestärkt und ausdrücklich zugewiesen werden.

77. Die Wirksamkeit der Bestimmungen der Richtlinie 95/46/EG hängt von den Anstrengungen der für die Datenverarbeitung Verantwortlichen ab, diese Ziele zu erreichen. Das macht die folgenden proaktiven Maßnahmen erforderlich:

- *Einführung interner Strategien und Verfahren durch die für die Datenverarbeitung Verantwortlichen*, um die Forderungen der Richtlinie nach der Durchführung spezieller Verarbeitungsvorgänge durch den für die Verarbeitung Verantwortlichen umzusetzen. Diese internen Strategien und Verfahren sollten auf höchster Organisationsebene genehmigt werden und folglich für alle Mitarbeiter bindend sein.
- *Einführung von Mechanismen zur Ausführung der internen Strategien und Verfahren einschließlich Beschwerdeverfahren (siehe auch Kapitel 5)*, damit diese Strategien in der Praxis wirkungsvoll sind. Dazu kann auch die Sensibilisierung für den Datenschutz gehören sowie die Ausbildung des Personals und Schulungen.
- *Abfassen von Berichten über die Einhaltung der Vorschriften, das Durchführen von Audits, der Erhalt von Bescheinigungen einer neutralen Partei und/oder von Gütesiegeln*, als Kontrolle und Bewertung, ob die angenommenen internen Maßnahmen, mit denen die Einhaltung der Vorschriften sichergestellt werden soll, die personenbezogenen Daten wirkungsvoll verwalten, schützen und sichern (siehe auch Kapitel 4).
- Durchführen von *Datenschutz-Verträglichkeitsprüfungen*, insbesondere für bestimmte Datenverarbeitungsvorgänge, von denen angenommen wird, dass sie z. B. aufgrund ihrer Natur, ihres Umfangs oder ihres Zwecks besondere Risiken für die Rechte und Freiheiten der Betroffenen darstellen.
- *Übertragung der Verantwortung für den Datenschutz* an hierfür ernannte Personen, die die direkte Verantwortung dafür tragen, dass ihre Organisation die Datenschutzgesetze einhält.
- *Bescheinigungen der Führungskräfte des Unternehmens über das Einhalten der Bestimmungen*, in denen bestätigt wird, dass angemessene Maßnahmen für den Schutz der personenbezogenen Daten ergriffen wurden.

- *Transparenz dieser eingeführten Maßnahmen* gegenüber den Betroffenen undder Öffentlichkeit im Allgemeinen. Transparenz-Anforderungen tragen zur Rechenschaftslegung der für die Datenverarbeitung Verantwortlichen bei (z. B. Veröffentlichung der Datenschutzerklärung im Internet, Transparenz in Bezug auf interne Beschwerdeverfahren und die Veröffentlichung in Jahresberichten).

78. Artikel 17 Absatz 1 der Richtlinie 95/46/EG verlangt von den für die Datenverarbeitung Verantwortlichen bereits in gewissem Umfang sowohl technische als auch organisatorische Maßnahmen (der für die Datenverarbeitung Verantwortliche muss *„die geeigneten technischen und organisatorischen Maßnahmen durchführen, die für den Schutz gegen […] jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind"*). Diese Maßnahmen können einige der oben genannten Maßnahmen umfassen. In der Praxis hat Artikel 17 Absatz 1 jedoch nicht erfolgreich dazu beigetragen, den Datenschutz in Organisationen ausreichend effizient zu gestalten. Dies liegt auch an dem unterschiedlichen Vorgehen bei den nationalen Umsetzungsmaßnahmen.

Grundsatz der Rechenschaftspflicht[28]

79. Zur Bekämpfung dieses Problems wäre es angebracht, in den umfassenden Rechtsrahmen den Grundsatz der Rechenschaftspflicht aufzunehmen. Dieser Grundsatz würde die für die Datenverarbeitung Verantwortlichen dazu verpflichten, die notwendigen Maßnahmen zu ergreifen, um *sicherzustellen*, dass die wesentlichen Grundsätze und Verpflichtungen der geltenden Richtlinie bei der Verarbeitung personenbezogener Daten *eingehalten werden*. Eine solche Bestimmung würde die Forderung unterstreichen, dass Strategien und Mechanismen eingeführt werden müssen, mit denen die wesentlichen Grundsätze und Verpflichtungen der geltenden Richtlinie wirkungsvoll werden. Sie würde den Bedarf an wirkungsvollen Schritten unterstreichen, die zu einer wirkungsvollen internen Durchführung der wesentlichen Verpflichtungen und Grundsätze führen, die in der aktuellen Richtlinie verankert sind. Darüber hinaus würde der Grundsatz der Rechenschaftspflicht von den für die Datenverarbeitung Verantwortlichen verlangen, dass sie Rechenschaftspflicht für die notwendigen internen Mechanismen sorgen, damit sie gegenüber externen interessierten Parteien, einschließlich der nationalen Datenschutzbehörden, die *Einhaltung beweisen* können. Die daraus resultierende Forderung nach Beweisen für die für Einhaltungszwecke durchgeführten angemessenen Maßnahmen wird die Durchsetzung von anzuwendenden Vorschriften sehr vereinfachen.

[28] Zur Rechenschaftspflicht siehe auch Punkt 39.

80. Die Maßnahmen, die von den für die Datenverarbeitung Verantwortlichen erwartet werden, sollten jedenfalls anpassbar sein und unter anderem die Art des Unternehmens berücksichtigen, seine Größe, ob es eine GmbH ist und die Art, Natur und Menge der zu verarbeitenden personenbezogenen Daten.

Mehr Optionen: proaktiv oder reaktiv

81. Einige der oben beschriebenen Maßnahmen könnten als übliche bewährte Praktiken angesehen werden, mit denen der Grundsatz der Rechenschaftspflicht beim Umsetzen in die Praxis erfüllt wird. Es könnte per Gesetz eine integrierte Belohnungsstruktur vorgesehen werden, um die Organisationen zur Umsetzung anzuregen.

82. Eine alternative Lösung hätte eher den Charakter einer Vorschrift. Artikel 17 Absatz 1 könnte z. B. so ausgearbeitet werden, dass zusätzliche proaktive Maßnahmen wie die vorgenannten niedergelegt werden, die durch die für die Datenverarbeitung Verantwortlichen umgesetzt werden müssen. Diese Maßnahmen könnten auf bestimme Resultate abzielen und sollten technologisch neutral sein.

83. Andere Maßnahmen hätten einen mehr reaktiven Charakter. Sie würden im Fall einer unrechtmäßigen Verarbeitung personenbezogener Daten angewendet werden und könnten unter anderem Folgendes beinhalten:

    - *Einführen einer zwingend vorgeschriebenen Pflicht zur Meldung von Sicherheitsverletzungen* (siehe auch Kapitel 2 und 5).
    - *Stärken der Durchsetzungsbefugnisse der Datenschutzbehörden*, einschließlich der Befugnis, konkrete Forderungen zur Sicherstellung eines effektiven Schutzes zu stellen (siehe auch Kapitel 7 Buchstabe a).

Vereinfachung der Meldungen

84. Die Meldungen von Datenverarbeitungsvorgängen an die nationalen Datenschutzbehörden könnten vereinfacht oder ihre Zahl verringert werden. In diesem Zusammenhang sollte die Verbindung zwischen der Einhaltung der oben genannten Anforderungen und der Möglichkeit einer weiteren Abstufung der behördlichen Anforderungen, insbesondere zur Meldung von Datenverarbeitungsvorgängen an die nationalen Datenschutzbehörden, untersucht werden.

85. Meldungen tragen zur Sensibilisierung in Bezug auf die Datenverarbeitungsvorgänge und die Datenschutzgepflogenheiten in einer Organisation

bei.[29] Sie geben den Datenschutzbehörden auch einen Überblick über die Datenverarbeitungsvorgänge. Eine bessere Datenverwaltung und Rechenschaftspflichten könnten jedoch denselben Zweck erfüllen. Diese Mechanismen könnten dabei helfen, die notwendigen Maßnahmen durchzuführen, um die wesentlichen Grundsätze und Verpflichtungen zu beachten, die in der geltenden Richtlinie verankert sind und die Beweise für eine solche Einhaltung zu liefern.

86. Es sollte untersucht werden, ob und in welchem Umfang die Meldungen auf solche Fälle eingeschränkt werden könnten, in denen ein ernsthaftes Risiko für den Datenschutz besteht. Das würde den Datenschutzbehörden die Möglichkeit geben, mehr Auswahl zu treffen und ihre Anstrengungen auf solche Fälle zu konzentrieren. Selbst in solchen Fällen könnten den Meldungen rationalisiert werden, z. B., indem die Ergebnisse von Datenschutz-Verträglichkeitsprüfungen oder die Ergebnisse von Audits durch eine neutrale Partei bereitgestellt würden. Dies könnte mit einem Meldesystem verbunden werden, bei dem alle für die Datenverarbeitung Verantwortlichen in ein von den Datenschutzbehörden geführtes Verzeichnis eingetragen würden. Somit würde im Bedarfsfall die einfache Ermittlung der organisatorischen Instanzen für eine effiziente und wirkungsvolle Durchsetzung gewährleistet werden.

7. Eine stärkere und eindeutigere Rolle für die Datenschutzbehörden und ihre Zusammenarbeit in der EU

7a. Datenschutzbehörden

87. Derzeit gibt es große Unterschiede in Bezug auf die Positionen der Datenschutzbehörden in den 27 Mitgliedstaaten. Der Grund hierfür liegt in den Unterschieden in der geschichtlichen Entwicklung, der Rechtsprechung, Kultur und den internen Organisationen der Mitgliedstaaten, aber auch daran, dass es Artikel 28 der Richtlinie 95/46/EG in mehrerlei Hinsicht an Präzision mangelt. Außerdem wurde die Richtlinie in einigen Gebieten bis zu einem gewissen Grad schlecht umgesetzt. Das hat zu großen Unterschieden zwischen den Mitgliedstaaten geführt, unter anderem bezüglich der Position, den Ressourcen und den Befugnissen der Datenschutzbehörden.

88. Die neuen Herausforderungen an den Datenschutz (Globalisierung und die technologischen Änderungen, Kapitel 3 und 4) machen eine strikte, einheit-

[29] Diese Ansichten werden durch den Bericht der Artikel-29-Gruppe WP106 über die Meldepflicht an die nationalen Kontrollstellen, zur bestmöglichen Nutzung der Ausnahmen und Vereinfachungen und zur Rolle von Datenschutzbeauftragten in der Europäischen Union bestätigt, der am 18. Januar 2005 angenommen wurde.

lichere und effektivere Überwachung erforderlich. Der neue Rechtsrahmen sollte folglich hochrangig und richtunggebend einheitliche Standards in Bezug auf Unabhängigkeit und effektive Befugnisse garantieren sowie den Datenschutzbehörden eine beratende Rolle im Gesetzgebungsverfahren geben und die Möglichkeit, die Geschäftsordnung selbst festzulegen, insbesondere durch das Setzen von Prioritäten bei der Behandlung von Beschwerden.

89. Datenschutzbehörden müssen gänzlich unabhängig sein. Der geltende Artikel 28 Absatz 1 der Richtlinie 95/46/EG ist in dieser Hinsicht unklar, wie der Fall C-584/07 (Kommission gegen Deutschland) zeigt, der derzeit vor dem Europäischen Gerichtshof verhandelt wird. In dem neuen Rechtsrahmen sollten die Datenschutzbehörden:

- über eine vollumfängliche institutionelle Unabhängigkeit verfügen und keiner anderen Regierungsbehörde unterstehen;
- über eine funktionale Unabhängigkeit verfügen und nicht Anweisungen oder Kontrollen in Bezug auf die Art und den Umfang ihrer Tätigkeiten unterliegen;
- über finanzielle Unabhängigkeit verfügen. Sie sollten über eine Infrastruktur verfügen, die den reibungslosen Ablauf ihrer Tätigkeiten ermöglicht und insbesondere über eine angemessene Finanzierung. Den Datenschutzbehörden sollten in ausreichendem Umfang Ressourcen zugewiesen werden.

90. Die Aufgaben der Datenschutzbehörden zur Rechtsdurchsetzung werden immer wichtiger. Sie sollten stark, mutig und strategisch bei ihrem Eingreifen und bei der Rechtsdurchsetzung sein. Der aktuelle Wortlaut von Artikel 28 der Richtlinie 95/46/EG hat zu großen Unterschieden in den Befugnissen zur Rechtsdurchsetzung geführt. Der neue Rechtsrahmen sollte ein einheitlicheres Vorgehen der Mitgliedstaaten bei der Ausstattung der Datenschutzbehörden mit den erforderlichen Befugnissen fordern und er sollte diesbezüglich spezifischere Angaben machen als die Richtlinie 95/46/EG. Die erforderlichen Befugnisse sollten unter anderem das Recht auf Verhängung von Geldbußen gegen die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter umfassen.

91. Die beratende Funktion der Datenschutzbehörden im Gesetzgebungsprozess ist unabdingbar. Denn für eine Verbesserung der (Datenschutz)-Gesetzgebung ist häufig das Wissen der Datenschutzbehörden aus Ermittlungen und Rechtssetzungsaktion erforderlich. Die beratende Rolle sollte alle Maßnahmen und Verordnungen zum Schutz der Rechte und Freiheiten des Einzelnen in Bezug auf die Verarbeitung personenbezogener Daten umfassen und nicht

nur „Rechtsverordnungen und Verwaltungsvorschriften".[30] Die Datenschutzbehörden sollten um Rat gefragt werden, bevor die Gesetzgebungsvorlage angenommen wird. Darüber hinaus sollte der neue Rechtsrahmen sicherstellen, dass die Datenschutzbehörden gegenüber ihren nationalen Parlamenten und/oder gegenüber anderen zuständigen innerstaatlichen Einrichtungen eine beratende Rolle haben, wenn die letztgenannten mit dem Gesetzgebungsprozess für neue EU-Rechtsvorschriften befasst sind.

92. Datenschutzbehörden müssen ihre eigene Geschäftsordnung machen können, wenn sie die Prioritäten unter anderem in Bezug auf die Abwicklung von Beschwerden regeln. Dazu gehört auch die Art und Weise, in der auf Beschwerden reagiert wird.[31] Die Datenschutzbehörden sollten auf jeden Fall in Betracht ziehen können, ob die Bearbeitung einer Beschwerde in ausreichendem Maße zum Schutz der personenbezogenen Daten beiträgt.[32] Der neue Rechtsrahmen sollte den Datenschutzbehörden die Möglichkeit geben „selektiv zu sein, um effektiv zu sein".

93. Auf der anderen Seite müssen die Datenschutzbehörden für die Art und Weise rechenschaftspflichtig sein, in welcher sie ihre stärkere Überwachungsrolle ausüben. Sie sollten diesbezüglich transparent sein und öffentlich über ihre Vorgehensweise und ihre Prioritäten berichten. Der aktuelle Wortlaut von Artikel 28 Absatz 5 der Richtlinie 95/46/EG muss diesbezüglich in dem neuen Rechtsrahmen präzisiert werden.

7b. Zusammenarbeit der Datenschutzbehörden

Der geltende Rechtsrahmen

94. Artikel 29 der Richtlinie 95/46/EG hat die Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (WP29) als institutionelle Einrichtung für die Zusammenarbeit zwischen den nationalen Datenschutzbehörden eingesetzt. Die WP29 ist unabhängig und hat eine beratende Funktion. Ihre Aufgaben sind in Artikel 30 Absatz 1 der Richtlinie festgelegt. Sie soll zu einer einheitlichen Anwendung der Richtlinie beitragen, indem sie Fragen im Zusammenhang mit den einzelstaatlichen Vorschriften prüft, Stellung nimmt zum Schutzniveau in der Gemeinschaft und

30 Artikel 28 Absatz 2 der Richtlinie 95/46/EG.

31 Die Möglichkeit selektiv zu sein, kann auf verschiedene Weise in die Praxis umgesetzt werden, z. B. durch die Einführung von „Schnellverfahren" für geringfügigere Beschwerden.

32 Bei der Frage, ob eine Beschwerde bearbeitet werden sollte, können z. B. die folgenden Kriterien angewendet werden: Betrifft die Situation viele Personen, betrifft die Beschwerde eine Verletzung eines wichtigen Datenschutzgesetzes oder ist es nur ein Zufall, wird die Bearbeitung vermutlich erfolgreich sein und wird sie nicht unverhältnismäßig hohe Anstrengungen erfordern?

in Drittländern und (auch auf eigene Initiative hin) bei Vorschlägen zu Gemeinschaftsrecht mit Auswirkungen auf den Datenschutz oder bei anderen Angelegenheiten des Schutzes von Personen mit Bezug auf die Verarbeitung personenbezogener Daten in der Gemeinschaft berät. Die Kommission ist Mitglied der WP29 und nimmt die Sekretariatsgeschäfte der Gruppe wahr.

95. Die WP29 erfüllt ihre Aufgabe im Anwendungsbereich der Richtlinie, wie in Artikel 3 Absatz 2 dargelegt. Im Bereich der polizeilichen und justiziellen Zusammenarbeit haben die europäischen Datenschutzbehörden im Jahr 2007 die Arbeitsgruppe Polizei und Justiz (WPPJ) gegründet, welche eine ähnliche Rolle wie die WP29 erfüllt, jedoch ohne Rechtsgrundlage und ohne dass die Sekretariatsgeschäfte durch eine Gemeinschaftsinstitution übernommen werden. Der Rahmenbeschluss 2008/977/JI, der in diesem Bereich Datenschutzgrundsätze einführt, sieht keine institutionalisierte Zusammenarbeit mit den Datenschutzbehörden vor.

Die Arbeitsweise der WP29

96. Die WP29 besteht seit nunmehr über 10 Jahren und hat signifikant zum Erreichen der Ziele gemäß Artikel 30 der Richtlinie 95/46/EG beigetragen. Das Ergebnis vieler Aktivitäten dieser Arbeitsgruppe kann auf der Webseite nachgelesen werden.[33]

97. Die WP29 hat konstant an einer Verbesserung ihre Wirksamkeit gearbeitet und sollte weiterhin das Augenmerk auf ihre eigene Arbeitsweise richten. Hierbei sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Wie kann die WP29 wirksam zu einer einheitlichen Umsetzung der EU-Rechtsvorschriften in innerstaatliche Gesetze und zu einer einheitlichen Anwendung derselben beitragen?
- Wie kann sie ihre Wirksamkeit gegenüber den EU-Institutionen und insbesondere gegenüber der Kommission verbessern und dabei gleichzeitig die hybride Rolle der Kommission berücksichtigen, die Mitglied der WP29 ist, deren Sekretariatsgeschäfte führt und gleichzeitig auch der Empfänger vieler der Stellungnahmen der WP29 ist.

Folgen für die Zukunft

98. Als oberste Priorität sollte sichergestellt werden, dass alle Fragen bezüglich der personenbezogenen Daten, insbesondere im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in die Aktivitäten der ak-

[33] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue

tuellen WP29 einbezogen werden. Ein umfassender Rechtsrahmen sollte einen Gesamtberater und eine effektive Zusammenarbeit zwischen den Kontrollbehörden beinhalten. In der Übergangszeit bis zur Umsetzung der Gesetzesänderungen, müssen angemessene Formen für eine Zusammenarbeit zwischen der WP29 und der WPPJ gefunden werden.

99. Andere Verbesserungen setzen keine Gesetzesänderungen voraus.

- Die einheitliche Anwendung des innerstaatlichen Rechts, mit dem die Richtlinie 95/46/EG umgesetzt wird, kann mit dem geltenden Rechtsrahmen erreicht werden, indem die Arbeitsmethoden der Arbeitsgruppe weiter verbessert werden und soweit erforderlich, die Mitglieder der WP29 zur Umsetzung der Ansichten der Gruppe in nationale Praxis aufgefordert werden.
- Gemäß Artikel 29 der Richtlinie 95/46/EG übernimmt die Kommission die Sekretariatsgeschäfte der WP29. Das Sekretariat sollte eng mit dem Vorsitz der WP29 und dem Stab zusammenarbeiten. Die Aufgaben des Sekretariats und des Vorsitzes ergänzen sich, und sie sollten eng zusammenarbeiten, um der WP29 so die Möglichkeit zu geben, ihre Aufgaben auf die wirkungsvollste Weise zu erfüllen. Während das Sekretariat die logistischen Aspekte der Arbeit der WP29 regelt und die Arbeitsgruppe bei der Vorbereitung ihrer Stellungnahmen und Dokumente unterstützt, konzentrieren sich der Vorsitz (und der stellvertretende Vorsitz) hauptsächlich auf den Entscheidungsfindungsprozess und auf die Strategie der WP29.
- Die Beziehungen zwischen der WP29 und der Kommission, die die Sekretariatsgeschäfte für die WP29 wahrnimmt, können durch das Niederlegen der wichtigsten Rollen der beiden Akteure in einem Memorandum of Understanding weiter verbessert werden. Dieses Memorandum sollte auch die der WP29 zur Verfügung stehenden Geldmittel ansprechen, so dass diese bei der Ausübung ihrer Aufgaben auf ihre vollen Ressourcen zurückgreifen kann. Schließlich sollte auch die Arbeitsweise des Sekretariats angesprochen werden, so dass sowohl die WP29 als auch das Sekretariat über ausreichende Mittel verfügen, um die Stellungnahmen und Arbeitsdokumente der WP29 vorzubereiten. Die WP29 wird im Jahr 2010 Beratungen mit der Kommission zu Obenstehendem aufnehmen.

8. Datenschutzherausforderungen im Bereich der Strafverfolgung

100. Der Datenschutz im Bereich Polizei und Justiz ist ein spezielles Thema, dem besondere Aufmerksamkeit gewidmet werden muss. Dabei muss der komplexen Beziehung zwischen den Aktivitäten des Staates zur Wahrung der Sicherheit und dem Schutz der personenbezogenen Daten des Einzelnen

Rechnung getragen werden. Die Besonderheit dieses Themas ist nicht nur das Ergebnis der vormaligen Säulenstruktur der ehemaligen EU-Verträge, sondern sie ist in größerem Umfang anerkannt (siehe z. B. die Ausnahmen in Artikel 13 der Richtlinie 95/47/EG und die Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon).

Der sich ändernde Kontext innerhalb der EU

101. Mit dem Inkrafttreten des Vertrags von Lissabon werden im Bereich des Datenschutzes neue Perspektiven für die Gesetzgebung geschaffen. Die Säulenstruktur wird abgeschafft, und mit Artikel 16 AEUV wird für den Datenschutz in fast allen Bereichen des EU-Rechts eine einheitliche Rechtsgrundlage geschaffen (siehe Kapitel 2). Das heißt nicht unbedingt, dass die Datenschutzgrundsätze für Polizei und Justiz mit denselben Vorschriften umgesetzt werden sollte, wie in anderen Teilen der Gesellschaft. Die Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon besagt, dass es „sich als erforderlich erweisen könnte", im Bereich der Strafverfolgung spezifische Vorschriften zu erlassen.

102. Der Datenschutz und der Datenaustausch werden wichtige Kernpunkte des Stockholmer Programms sein. Die Beschlussfassung wird auf dem Konzept der richtigen Balance zwischen den Erfordernissen der Strafverfolgung und den Anforderungen des Datenschutzes beruhen. Neue Maßnahmen sollten erst nach einer angemessenen Bewertung des geltenden Rechtsrahmens ergriffen werden.

103. Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss von den Mitgliedstaaten bis zum 27. November 2010 umgesetzt werden. Dieser Rahmenbeschluss kann als erster Schritt in Richtung eines allgemeinen Rechtsrahmens in der ehemaligen dritten Säule angesehen werden. Er ist jedoch alles andere als vollständig. Er ist lediglich in grenzüberschreitenden Situationen anwendbar. Ihm scheinen die essentiellen Elemente und Mittel zu fehlen, um effektiv mit den sich ändernden Arbeitsmethoden im Bereich der Strafverfolgung umzugehen.

Die sich ändernde Gewichtung bei der Strafverfolgung

104. In den letzten Jahren zeigte sich eine Verschiebung bei der Gewichtung der Arbeitsmethoden der Polizei und der Strafverfolgungsbehörden in Bezug auf die Verwendung (personenbezogener) Informationen. Zu dieser Verschiebung kam es, da die Nutzung von Informationen immer wichtiger wurde, um den neuen Bedrohungen aus dem Terrorismus und der organi-

sierten Kriminalität entgegenzutreten. Sie ist das Ergebnis der technologischen Entwicklungen der letzten Jahre.

105. Die Schwerpunktverschiebung hat mehrere Dimensionen:

- Die Nutzung der Informationen konzentriert sich auf frühere Phasen der Kette: Zusätzlich zu der traditionellen Verwendung der Informationen für die Ermittlungen und das Aufdecken einer bestimmten Straftat werden Informationen erhoben und ausgetauscht, um mögliche Straftaten zu verhindern („vorbeugende Überwachung").
- Die Nutzung der Informationen konzentriert sich auf eine größere Personengruppe. Die Informationen werden nicht nur von Personen erhoben und ausgetauscht, die in indirekter Verbindung zu einer Straftat stehen wie Verdächtige oder Zeugen, sondern auch von größeren Populationsgruppen, die nicht Gegenstand von Ermittlungen sind (z. B. Reisende, Personen, die Zahlungsdienste in Anspruch nehmen usw.).
- Die genutzten Informationen basieren immer stärker auf Technologie. Technologie verbindet selbst verschiedene Faktoren, um so das zukünftige Verhalten von Personen mit Hilfe von automatisierten Mitteln (Data Mining, Erstellen von Profilen) vorherzusagen.
- Die genutzten Informationen sind unterschiedlicher Natur. Hierbei wird nicht nur auf objektiv ermittelte Informationen (Fakten und Zahlen) gebaut, sondern auch auf Informationen, die auf Bewertungen und Analysen aus dem Gefüge einer Ermittlung stammen (weiche Daten). Außerdem kann die Unterscheidung zwischen den beiden Informationsarten je nach Mitgliedstaat variieren.
- Die steigende Nutzung personenbezogener Informationen aus dem Privatsektor für vorbeugende Maßnahmen, wie z. B. Bank- oder Finanzdaten und Fluggastdaten, die durch Luftfahrtgesellschaften und CRS erhoben werden.
- Informationen, die für einen bestimmten, rechtmäßigen Grund erhoben werden, werden in zunehmendem Maße für andere teilweise unvereinbare Zwecke verwendet. Die Zwecke gleichen sich immer weiter an. Interoperabilität zwischen den Systemen ist eine wichtige Entwicklung, die jedoch kein rein technisches Thema ist, insbesondere im Hinblick auf die Gefahren der Verbindung von Datenbanken, die unterschiedlichen Zwecken dienen.
- An der Nutzung der Informationen sind mehr Behörden beteiligt, nicht nur die Polizei und die Justizbehörden stricto sensu, sondern auch andere öffentliche Behörden wie Grenzkontrollbehörden, Finanzbehörden und nationale Sicherheitsdienste.

106. Dieser Wandel in der Gewichtung bei der Strafverfolgung hat zu einem dramatischen Anstieg bei der Speicherung und dem Austausch personenbezogener Daten in Bezug auf Aktivitäten der Polizei und des Justizsektors geführt. Die technologische Möglichkeit, Informationen einfach zu kombinieren, hat möglicherweise tiefgreifende Auswirkungen auf die Privatsphäre und den Datenschutz aller Bürger sowie auf ihre Möglichkeit, ihre Grundrechte wirklich wahrzunehmen und auszuüben, insbesondere das Recht, sich frei zu bewegen sowie die Rede- und Meinungsfreiheit.

Herausforderungen für den Datenschutz

107. Angesichts dieses Hintergrunds sind die Herausforderungen an den Datenschutz immens. Ein zukünftiger Rechtsrahmen sollte auf jeden Fall die folgenden Punkte angehen:

- Die Tendenzen könnten zu einer mehr oder weniger ständigen Überwachung aller Bürger führen. Das wird häufig als Überwachungsgesellschaft bezeichnet. Ein Beispiel wäre die kombinierte Nutzung von intelligenten Cctv-Kameras und von anderen Instrumenten wie der automatischen Nummernschilderkennung, mit der alle Autos registriert werden, die in ein bestimmtes Gebiet einfahren oder es verlassen.
- Datenbanken können für Data Mining genutzt werden, und auf der Grundlage des Erstellens von Profilen Einzelner können Risikobewertungen einzelner Personen durchgeführt werden. Dies könnte Personen mit einem bestimmten Hintergrund stigmatisieren.
- Bei Analysen, die auf der Grundlage genereller Kriterien erstellt werden, besteht das Risiko großer Ungenauigkeiten, was zu einer großen Anzahl an falschen Negativ- oder falschen Positivergebnissen führt.
- Die Verarbeitung personenbezogener Daten von Personen, die nicht verdächtig sind, wird immer wichtiger. Bestimmte Bedingungen und Garantien werden benötigt, damit ihre Legitimität und die Proportionalität bewertet werden und um Vorurteile gegenüber Personen zu vermeiden, die nicht (aktiv) an einer Straftat beteiligt sind.
- Es ist eine erhöhte Verwendung biometrischer Daten, einschließlich der DNA zu verzeichnen. Dies stellt ein gewisses Risiko dar.

Forderungen an die Rechtsetzung und die Politikgestaltung

108. Die wachsende Zahl sektorspezifischer Initiativen, die angenommen oder geplant wurden, könnte leicht zum Überlappen oder sogar zur Verzerrung von Maßnahmen führen. Deshalb könnte es wertvoll sein, den Informationsaustausch auf eine einheitliche Strategie zu stützen, vorausgesetzt, dass der

Datenschutz vollumfänglich berücksichtigt wird und ein wesentlicher Bestandteil der Strategie ist.[34]

109. Es ist von größter Wichtigkeit, die bestehenden Rechtsinstrumente und ihre Anwendung zu bewerten. Dabei sollten die Kosten für die Privatsphäre berücksichtigt werden. Die Bewertung der bestehenden Maßnahmen sollte vor der Ergreifung neuer Maßnahmen erfolgen. Darüber hinaus sollte eine regelmäßige Überprüfung der bestehenden Maßnahmen stattfinden.

110. Transparenz ist ein grundlegendes Element. Den Betroffenen sollten verständliche Informationen über die Verwendung der erhobenen Daten und über die Logik der Verarbeitung zur Verfügung stehen. Diese Informationserteilung sollte lediglich in individuellen Fällen eingeschränkt werden, um laufende Ermittlungen nicht zu gefährden und sollte zeitlich eingeschränkt sein. Die Informations- und Berichtigungsrechte der betroffenen Personen sollten in einem grenzüberschreitenden Kontext angegangen werden, damit die Betroffenen nicht die Kontrolle verlieren.

111. Besondere Aufmerksamkeit muss der Transparenz und der demokratischen Kontrolle bei der Gesetzgebung gewidmet werden. Datenschutz-Verträglichkeitsprüfungen, angemessene Formen der Beratung mit Datenschutzbehörden und eine effektive parlamentarische Debatte sowohl auf nationaler als auch auf gemeinschaftlicher Ebene sollten eine wichtige Rolle spielen.

112. Die Architektur jedes Systems für die Speicherung und den Austausch personenbezogener Daten sollte gut ausgearbeitet sein. Es folgen einige allgemeine Überlegungen:

- Die Architektur sollte durch „Privacy by Design“ und Technologien zum Schutz der Privatsphäre (Zertifizierungsprogramm) bestimmt werden. In einem Raum der Freiheit, der Sicherheit und des Rechts, in dem die Behörden die wichtigsten Akteure sind und in dem sich jede Initiative, die auf eine wachsende Überwachung des Einzelnen und ein steigendes Einholen und Verarbeiten von personenbezogenen Daten abzielt, direkt auf das Grundrecht auf Privatsphäre und Datenschutz auswirken könnte, könnten solche Anforderungen zur zwingenden Vorschrift werden.
- Zweckbindung und Datensparsamkeit sollten als Leitgrundsätze bestehen bleiben.
- Der Zugang zu großen Datenbanken muss so konfiguriert werden, dass generell Online kein direkter Zugriff auf gespeicherte Daten gestattet ist.

[34] Eine europäische Informationsmanagement-Strategie, wie sie derzeit vom Rat erarbeitet wird, könnte sich in diesem Kontext als nützliches Instrument herausstellen, sofern sie richtig erstellt wird.

Ein Treffer/kein Treffer-System oder ein Index-System gilt allgemein als vorzuziehen.

- Die Entscheidung zwischen Modellen mit einem Zentralspeicher, also Systemen mit einer zentralen Datenbank auf EU-Ebene und mit einer dezentralisierten Speicherung sollte aufgrund transparenter Kriterien getroffen werden. Das Ergebnis dieser Entscheidung sollte jedenfalls die Rolle und die Verantwortung des/der für die Datenverarbeitung Verantwortlichen klar und solide definieren und eine angemessene Überwachung durch die zuständigen Datenschutzbehörden sicherstellen.
- Biometrische Daten sollten nur dann genutzt werden, wenn die Verwendung anderen, weniger intrusiven Materials nicht dieselben Ergebnisse liefert.

113. Die externe Dimension. Es sollte vermeiden werden, dass das strikte System für den Austausch personenbezogener Daten innerhalb der EU umgangen wird. Die Beziehungen zu Drittländern sollten auf einen klaren Rechtsrahmen gestützt werden, der für alle Parteien und im Hinblick auf das Konzept der Angemessenheit bindend ist. Das System der Angemessenheit sollte nach einer Beurteilung durch die nationalen Datenschutzbehörden bewertet werden und sofern erforderlich, durch gemeinsame Mechanismen, die eine einheitliche Umsetzung und Wirksamkeit sicherstellen.

114. Groß angelegten Informationssystemen in der EU muss besondere Aufmerksamkeit gewidmet werden, dazu gehören, sofern erforderlich, maßgeschneiderte Garantien für den Datenschutz.

115. Eine unabhängige Kontrolle, die justizielle Aufsicht und die Rechtsmittel sollten ordnungsgemäß durchgeführt werden. Dazu gehören in jedem Fall angemessene Ressourcen und Kompetenzen für eine unabhängige Kontrolle.

116. Die Datenschutzbehörden, die die Rechtmäßigkeit der Datenverarbeitung sicherstellen müssen, sollten in allen Bereichen gestärkt und in den Rechtsrahmen integriert werden, auch indem stabile Mechanismen ins Auge gefasst werden, ähnlich denen, die derzeit auf Angelegenheiten der ersten Säule angewendet werden, um ein harmonisiertes Vorgehen in der gesamten EU und darüber hinaus zu fördern.

Für die Artikel-29-Arbeitsgruppe

Der Vorsitzende
Alex Türk

Für die Arbeitsgruppe Polizei und Justiz

Der Vorsitzende
Francesco PIZZETTI

V. Internationale Konferenz der Datenschutzbeauftragten

31. Konferenz vom 4.–6. November 2009 in Madrid

Entschließung über Internationale Standards zum Schutz der Privatsphäre

– Übersetzung –

Berücksichtigend, dass:

- die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Strassburg einstimmig den Beschluss über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Richtlinien zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten fasste;

- die Konferenz die „Agencia Española de Protección de Datos“ (im Folgenden: die spanische Datenschutzbehörde, d. Übers.) in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz damit beauftragte, eine Arbeitsgruppe, die sich aus den interessierten Datenschutzbehörden zusammensetzen sollte, mit dem Ziel zu bilden, einen Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten auszuarbeiten;

- die spanische Datenschutzbehörde gemäß diesem Auftrag eine Arbeitsgruppe bildete und die Arbeiten zur Erstellung eines Gemeinsamen Vorschlags für die Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten förderte und koordinierte;

- die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten insbesondere auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards und Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren, entwickelte;

- bei der Erarbeitung des Gemeinsamen Vorschlags davon ausgegangen wurde, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen könnten und dass die Arbeitsgruppe die Erweiterung dieser Ansätze durch spezifische

Lösungen und Standards anstrebte, die trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre als anwendbar betrachtet wurden.

Im Einklang damit beschließt die Konferenz Folgendes:

1. Sie begrüßt den Gemeinsamen Vorschlag zur Abfassung der Internationalen Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von personenbezogenen Daten, der diesem Beschluss als Anlage beiliegt. Der Gemeinsame Vorschlag belegt zum angemessenen Zeitpunkt die Möglichkeit der Festlegung solcher Standards als einen neuen Schritt in Richtung auf die Ausarbeitung eines international verbindlichen Instruments.

2. Sie bestätigt, dass der Gemeinsame Vorschlag Grundsätze, Rechte, Verpflichtungen und Verfahrensweisen enthält, die zum Datenschutz und zum Schutz der Privatsphäre von allen Rechtssystemen angestrebt werden sollten. Auf diese Weise könnte die Verarbeitung personenbezogener Daten im öffentlichen und privaten Sektor weltweit einheitlicher erfolgen, und zwar:

   a. fair, rechtmäßig und angemessen im Hinblick auf bestimmte explizite und legitime Zwecke;

   b. auf der Grundlage einer transparenten Politik, mit angemessenen Informationen für die Interessierten und ohne willkürliche Diskriminierungen, die diesen Grundsätzen widersprächen;

   c. die Genauigkeit, Vertraulichkeit und Sicherheit der Daten sowie die Legitimität der Datenverarbeitung und die Rechte der Betroffenen auf Einsehen, Richtigstellung und Löschung der Daten sowie auf Widerspruch gegen eine bestimmte Datenverarbeitung gewährleistend;

   d. unter Anwendung des Haftungsprinzips, einschließlich der Schadenshaftung, was auch die Datenverarbeitung durch Dienstleistungserbringer, die im Auftrag des Verantwortlichen handeln, einschließt;

   e. mit geeigneteren Garantien, wenn es sich um sensible Daten handelt;

   f. mit der Gewährleistung, dass international übertragene Daten unter dem in den genannten Standards vorgesehenen Schutz stehen;

   g. indem die Datenverarbeitung unter die Kontrolle von unabhängigen und unparteiischen Aufsichtsbehörden gestellt wird, die über die angemessenen Befugnisse und Ressourcen verfügen müssen und zur Zusammenarbeit verpflichtet sind;

   h. durch die Schaffung eines neuen und modernen Bezugsrahmens proaktiver Maßnahmen, deren Ziel insbesondere die Vorbeugung und Feststellung von

Verstößen ist und die auf der Ernennung von Beauftragten für den Datenschutz und den Schutz der Privatsphäre, wirksamen Audits und Datenschutz-Folgenabschätzungen beruhen.

3. Sie ermutigt die bei der Internationalen Konferenz akkreditierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre zur Verbreitung des Gemeinsamen Vorschlags zur Abfassung Internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten.

4. Sie beauftragt die für die Organisation der 31. und 32. Internationalen Konferenz Verantwortlichen mit dem Aufbau einer Kontaktgruppe, an der die interessierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre teilnehmen sollen. Diese Gruppe soll folgende Aufgaben in Angriff nehmen:

   a. Die Förderung und die Verbreitung des Gemeinsamen Vorschlags unter privaten Instanzen, Experten sowie in- und ausländischen öffentlichen Stellen, insbesondere unter den in der Erklärung von Montreux aufgeführten Institutionen und Organisationen als Grundlage für die zukünftige Arbeit an einem verbindlichen universellen Abkommen; sowie

   b. die Untersuchung und Information über weitere Möglichkeiten der Verwendung des Gemeinsamen Vorschlags als Grundlage für die Entwicklung eines weltweiten Verständnisses und einer internationalen Kooperation im Bereich des Datenschutzes und des Schutzes der Privatsphäre, insbesondere im Kontext der internationalen Übertragung personenbezogener Daten, bei der die Rechte und Freiheiten der Individuen geschützt werden müssen.

5. Die Kontaktgruppe soll:

   a. ihre Arbeit mit der Steuerungsgruppe der Konferenz koordinieren und über ihre Vertretung auf Sitzungen internationaler Organisationen entscheiden sowie

   b. die 32. Internationale Konferenz über ihre Fortschritte informieren, damit die Aufmerksamkeit dauerhaft auf das Thema des vorliegenden Beschlusses gerichtet wird.

Erläuterung

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre fasste in Strassburg einstimmig die **Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten**. Diese wurde gemeinsam von den Datenschutzbehör-

den der Schweiz und Spaniens vorgelegt und von zwanzig weiteren Behörden unterstützt.

In dieser Entschließung erinnert die Konferenz daran, dass diverse Erklärungen und Beschlüsse in den letzten zehn Jahren darauf abzielten, den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre zu stärken und zur Erstellung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten aufzurufen.

Außerdem betont der Beschluss, dass die Internationale Konferenz der Ansicht ist, das Recht auf Datenschutz und den Schutz der Privatsphäre sei ein Grundrecht der Menschen, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz. Gleichzeitig stellt sie fest, dass die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden.

Deshalb wird in dem Beschluss die Überzeugung der Konferenz zum Ausdruck gebracht, dass die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt.

In diesem Sinne unterstützt der Beschluss der Internationalen Konferenz die Anstrengungen des Europarats, die Grundrechte auf den Datenschutz und den Schutz der Privatsphäre zu fördern, und sie fordert die Staaten – unabhängig davon, ob sie Mitglieder dieser Organisation sind oder nicht – auf, das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und das Zusatzprotokoll zu ratifizieren. Gleichzeitig unterstützt die Konferenz die Initiativen der APEC, der OECD sowie anderer regionaler Organisationen und internationaler Foren, wirksame Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre zu entwickeln.

Die Konferenz beauftragte die spanische Datenschutzbehörde in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz, eine Arbeitsgruppe zu bilden, die sich aus den interessierten Datenschutzbehörden zusammensetzen soll und deren Ziel es ist, einen Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten zu entwickeln.

Der Beschluss enthält eine Reihe von Kriterien, die den Prozess zur Ausarbeitung dieses gemeinsamen Vorschlags lenken, insbesondere dass öffentliche und pri-

vate Organisationen und Instanzen zu einer breiten Beteiligung ermutigt werden sollen, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen.

Gemäß diesem Auftrag bildete die spanische Datenschutzbehörde die Arbeitsgruppe, auf die sich der Beschluss bezieht, und förderte und koordinierte die Arbeiten zur Erstellung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards.

Die spanische Datenschutzbehörde lud alle bei der Internationalen Konferenz akkreditierten Behörden für den Datenschutz und den Schutz der Privatsphäre zur Teilnahme ein. Die im Anhang II aufgeführten Instanzen bekundeten ihren Willen, an dieser Arbeitsgruppe teilzunehmen, und versammelten sich daraufhin.

Die Arbeitsgruppe kam im Januar und Juni 2009 zusammen. Auf der ersten Sitzung wurde die Vorgehensweise zur Abfassung des Gemeinsamen Vorschlags und dessen inhaltliche Reichweite beschlossen und auf der zweiten Sitzung wurde eine fortgeschrittene Entwurfsversion besprochen, die später an die 31. Internationale Konferenz weitergeleitet werden sollte.

Die spanische Datenschutzbehörde leistete auf der Grundlage des Straßburger Beschlusses und der in der Arbeitsgruppe festgelegten Kriterien und Arbeitsmethoden eine gründliche Arbeit: Es wurde eine Reihe von Arbeitspapieren verfasst, an deren Ausarbeitung Beauftragte für den Datenschutz und den Schutz der Privatsphäre und andere mit dem Datenschutz verbundene öffentliche Instanzen sowie Experten aus privaten Unternehmen, Juristen, Wissenschaftler sowie internationale Organisationen und Nicht-Regierungs-Organisationen beteiligt waren.

Insbesondere entwickelte die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards oder Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren.

Bei der Erarbeitung des Gemeinsamen Vorschlags wurde davon ausgegangen, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen. Ziel der Arbeitsgruppe war die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards, die aber trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre anwendbar sind.

Anlage

Gemeinsamer Vorschlag zur Erstellung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten

Teil I: Allgemeine Bestimmungen

1. Ziel

Das Ziel des vorliegenden Dokuments ist:

a) Die Definition einer Reihe von Grundsätzen und Rechten, die den tatsächlichen und einheitlichen Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten weltweit garantieren; und

b) die Erleichterung des internationalen Flusses von personenbezogenen Daten – das ist eine Notwendigkeit in einer globalisierten Welt.

2. Definitionen

Das vorliegende Dokument versteht unter:

a) „Personenbezogene Daten“: Jegliche Information bezüglich einer identifizierten natürlichen Person bzw. einer natürlichen Person, die mit den vernünftigerweise einzusetzenden Mitteln identifiziert werden kann.

b) „Verarbeitung“: Jeglicher Vorgang oder eine Reihe von Vorgängen, die automatisiert sein können oder nicht und die auf personenbezogene Daten angewendet werden, das betrifft insbesondere deren Erhebung, Aufbewahrung, Enthüllung oder Löschung.

c) „Betroffener“: Eine natürliche Person, deren personenbezogene Daten verarbeitet werden.

d) „Verantwortliche Person“: Eine natürliche oder juristische Person, öffentlich oder privat, die allein oder in Zusammenarbeit mit anderen über die Verarbeitung entscheidet.

e) „Dienstleistungserbringer“: Eine natürliche oder juristische Person, die nicht die verantwortliche Person ist und die personenbezogenen Daten im Auftrag der besagten verantwortlichen Person verarbeitet.

3. Anwendungsbereich

1. Das vorliegende Dokument gilt für jegliche Verarbeitung personenbezogener Daten, die voll- oder teilautomatisch oder andernfalls in strukturierter Form im öffentlichen oder im privaten Sektor vollzogen wird.

2. Die jeweilige nationale Gesetzgebung kann festlegen, dass die Bestimmungen des vorliegenden Dokuments nicht auf die Verarbeitung personenbezogener Daten anzuwenden ist, wenn diese von einer natürlichen Person im Rahmen von ausschließlich privaten bzw. familiären Tätigkeiten ausgeführt wird.

4. Zusätzliche Maßnahmen

1. Die Staaten können das in dem vorliegenden Dokument definierte Schutzniveau um zusätzliche Maßnahmen, die einen besseren Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten garantieren, ergänzen.

2. Die Bestimmungen des vorliegenden Dokuments bilden eine geeignete Grundlage für die grenzüberschreitende Übermittlung personenbezogener Daten, wenn dies gemäß den Vorgaben des Artikels 15 des vorliegenden Dokuments geschieht.

5. Ausnahmen

Die Staaten können die Reichweite der in den Artikeln 7 bis 10 und 16 bis 18 enthaltenen Bestimmungen einschränken, wenn dies in einer demokratischen Gesellschaft notwendig ist, um die nationale Sicherheit, die öffentliche Sicherheit, den Schutz der öffentlichen Gesundheit oder den Schutz der Rechte und Freiheiten anderer zu gewährleisten. Solche Einschränkungen müssen im nationalen Recht ausdrücklich vorgesehen sein, das heißt, ihre Grenzen müssen festgelegt werden und es muss angemessene Garantien zum Schutz der Rechte der Betroffenen geben.

Teil II: Grundlegende Prinzipien

6. Prinzipien der Rechtmäßigkeit und Fairness

1. Die Verarbeitung personenbezogener Daten muss fair ausgeführt werden, wobei die anwendbare nationale Gesetzgebung sowie die Rechte und Freiheiten der Menschen im Einklang mit den Inhalten des vorliegenden Dokuments und den Zielen und Grundsätzen der Allgemeinen Erklärung der Menschenrechte und

dem Internationalen Pakt über bürgerliche und politische Rechte eingehalten werden müssen.

2. Insbesondere eine Verarbeitung personenbezogener Daten, die eine ungerechte oder willkürliche Diskriminierung der Betroffenen darstellt, wird als unredlich angesehen.

7. Prinzip der Zweckgebundenheit

1. Die Verarbeitung personenbezogener Daten muss sich auf die Erfüllung bestimmter, expliziter und legitimer Zwecke, die die verantwortliche Person verfolgt, beschränken.

2. Die verantwortliche Person darf keine Verarbeitungen durchführen, die nicht den Zwecken, für die die personenbezogenen Daten erhoben wurden, entsprechen, außer sie verfügt über das eindeutige Einverständnis des Betroffenen.

8. Verhältnismäßigkeitsprinzip

1. Die Verarbeitung der personenbezogenen Daten muss sich auf solche beschränken, die für die im vorherigen Absatz beschriebenen Zwecke angemessen, relevant und nicht exzessiv sind.

2. Insbesondere muss die verantwortliche Person angemessene Anstrengungen leisten, um die verarbeiteten personenbezogenen Daten auf ein notwendiges Mindestmaß zu reduzieren.

9. Qualitätsprinzip

1. Die verantwortliche Person muss jederzeit sicherstellen, dass die personenbezogenen Daten exakt sind und dass sie so vollständig und aktuell gehalten werden, wie es für die Erfüllung der Zwecke, für die sie verarbeitet werden, notwendig ist.

2. Die verantwortliche Person muss die Aufbewahrungszeit der verarbeiteten personenbezogenen Daten auf die erforderliche Mindestzeit beschränken. Wenn also die personenbezogenen Daten für die Erfüllung der Zwecke, die ihre Verarbeitung legitimierten, nicht mehr notwendig sind, müssen sie gelöscht oder anonymisiert werden.

10. Transparenzprinzip

1. Jede verantwortliche Person muss die von ihr durchgeführte Verarbeitung personenbezogener Daten in einer Datenschutzerklärung transparent machen.

2. Die verantwortliche Person muss dem Betroffenen zumindest über ihre Identität, den Zweck, zu dem sie die Verarbeitung auszuführen beabsichtigt, die Adressaten, an die sie die personenbezogenen Daten weiterzuleiten gedenkt, und die Art, auf die der Betroffene seine in dem vorliegenden Dokument beschriebenen Rechte ausüben kann, sowie alle weiteren Informationen, die die loyale Verarbeitung dieser personenbezogenen Daten gewährleistet, informieren.

3. Wenn die personenbezogenen Daten direkt von dem Betroffenen geliefert wurden, muss die Information zum Zeitpunkt der Datenerhebung gegeben werden, falls sie nicht schon vorher erteilt wurde.

4. Falls die personenbezogenen Daten nicht direkt vom Betroffenen stammen, muss die Information innerhalb eines angemessenen Zeitraums erbracht werden, obwohl sie auch durch alternative Maßnahmen ersetzt werden kann, falls die Erfüllung dieser Vorgabe unmöglich ist oder von der verantwortlichen Person einen unverhältnismäßigen Aufwand verlangt.

5. Alle Informationen, die dem Betroffenen gegeben werden, müssen verständlich und in einer eindeutigen und einfachen Sprache abgefasst sein, was insbesondere für solche Verarbeitungen gilt, die sich speziell an Minderjährige richten.

6. Wenn die personenbezogenen Daten online über elektronische Kommunikationsnetze erhoben werden, können die in diesem Artikel enthaltenen Verpflichtungen erfüllt werden, indem die Datenschutzpolitik leicht zugänglich und erkennbar veröffentlicht wird, wobei alle oben aufgeführten Punkte eingehalten werden müssen.

11. Verantwortlichkeitsprinzip

Die verantwortliche Person muss:

a) Die notwendigen Maßnahmen zur Erfüllung der in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung aufgeführten Grundsätze und Verpflichtungen ergreifen; und

b) die erforderlichen Nachweise über die Erfüllung der o.g. Vorgaben erbringen, und zwar sowohl gegenüber dem Betroffenen als auch gemäß Artikel 23 gegenüber den zuständigen Aufsichtsbehörden.

Teil III: Rechtfertigung der Verarbeitung

12 Allgemeines Rechtfertigungsprinzip

1. Als allgemeine Regel gilt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn einer der folgenden Punkte erfüllt wird:

a) nach Erhalt des freien, eindeutigen und informierten Einverständnisses des Betroffenen;

b) wenn ein legitimes Interesse der verantwortlichen Person die Verarbeitung rechtfertigt, vorausgesetzt, dass die legitimen Interessen, Rechte oder Freiheiten des Betroffenen keinen Vorrang haben;

c) wenn die Verarbeitung für die Aufrechterhaltung oder Erfüllung eines Rechtsverhältnisses zwischen der verantwortlichen Person und dem Betroffenen erforderlich ist;

d) wenn die Verarbeitung für die Erfüllung einer Verpflichtung, die der verantwortlichen Person von der anzuwendenden nationalen Gesetzgebung auferlegt wird, notwendig ist oder wenn sie von einer öffentlichen Behörde, die diese für die legitime Erfüllung ihrer Zuständigkeiten benötigt, ausgeführt wird;

e) wenn außergewöhnliche Umstände auftreten, die das Leben, die Gesundheit oder die Sicherheit des Betroffenen oder einer anderen Person gefährden.

2. Die verantwortliche Person muss den Betroffenen einfache, schnelle und wirksame Verfahren bereitstellen, damit diese ihr Einverständnis jederzeit zurücknehmen können. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für die Betroffenen noch Einkünfte der verantwortlichen Person verursachen.

13. Sensitive Daten

1. Als sensitiv werden folgende personenbezogenen Daten betrachtet:

a) Solche, die die Intimsphäre des Interessierten betreffen; oder

b) wenn deren ungerechtfertigte Verwendung

i. eine gesetzwidrige oder willkürliche Diskriminierung verursacht; oder

ii. ein schwerwiegendes Risiko für den Betroffenen darstellt.

2. Insbesondere werden solche personenbezogenen Daten als sensibel eingestuft, die Aufschluss über Aspekte wie die rassische oder ethnische Herkunft, politische Einstellungen, religiöse oder philosophische Überzeugungen geben, sowie Daten, die sich auf die Gesundheit oder die Sexualität beziehen. Falls die Umstände, auf die der vorhergehende Artikel sich bezieht, auftreten, kann die anzuwendende nationale Gesetzgebung weitere Kategorien für sensitive Daten vorsehen.

3. In der jeweiligen nationalen Gesetzgebung müssen die notwendigen Garantien zum Schutz der Rechte der Betroffenen festgeschrieben werden. Diese müssen zusätzliche Bedingungen für die Verarbeitung sensibler personenbezogener Daten enthalten.

14. Datenverarbeitung im Auftrag

Die verantwortliche Person kann die Verarbeitung von personenbezogenen Daten von verschiedenen Auftragnehmern durchführen lassen. In diesem Fall verpflichtet sie sich zur:

a) Kontrolle, dass jeder Auftragnehmer sicherstellt, dass zumindest das in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung vorgeschriebene Schutzniveau eingehalten wird; und

b) Verbindlichmachung der Rechtsbeziehung mittels eines Vertrags oder eines anderen Rechtsakts, der das Vorhandensein, die Reichweite und den Inhalt des Rechtsverhältnisses nachweist und den Auftragnehmer zur Einhaltung dieser Garantien und zur Gewährleistung, dass die personenbezogenen Daten gemäß der Anweisungen der verantwortlichen Person verarbeitet werden, verpflichtet.

15. Internationaler Datenverkehr

1. Als allgemeine Regel gilt, dass personenbezogene Daten grenzüberschreitend übermittelt werden können, wenn der Staat, in den diese Daten übertragen werden, zumindest das in dem vorliegenden Dokument vorgesehene Schutzniveau bietet.

2. Übermittlungen personenbezogener Daten in Staaten, die das in dem vorliegenden Dokument vorgesehene Schutzniveau nicht bieten, sind möglich, wenn derjenige, der die Daten zu übertragen beabsichtigt, garantiert, dass der Empfänger dieses Schutzniveau sicherstellt. Diese Garantie kann sich beispielsweise aus geeigneten vertraglichen Klauseln ableiten. Insbesondere, wenn die Datenübermittlung im Rahmen multinationaler Organisationen oder Unternehmensgruppen erfolgt, kann diese Garantie durch interne Datenschutzbestimmungen, deren Einhaltung rechtsverbindlich ist, geleistet werden.

3. Wenn die Übermittlung im Rahmen einer Vertragsbeziehung zugunsten des Betroffenen, zum Schutz eines lebenswichtigen Interesses des Betroffenen bzw. einer anderen Person oder zur Erfüllung einer gesetzlichen Verpflichtung zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, kann die für den Datenexporteur geltende nationale Gesetzgebung die Übermittlung der personenbezogenen Daten in Staaten zulassen, die das im vorliegenden Dokument vorgesehene Schutzniveau nicht bieten.

4. Die anzuwendende nationale Gesetzgebung kann die in Artikel 23 genannten Aufsichtsbehörden, die im Absatz 23 vorgesehen sind, zur vorherigen Genehmigung aller oder einiger grenzüberschreitender Übermittlungen von personenbezogenen Daten ermächtigen, die von ihrem Zuständigkeitsbereich aus erfolgen. Auf jeden Fall muss derjenige, der die personenbezogenen Daten ins Ausland übermitteln will, nachweisen, dass die Übermittlung die im vorliegenden Dokument

vorgesehenen Garantien erfüllt, insbesondere wenn dies von den Aufsichtsbehörden in Ausübung ihrer im Artikel 23.2 vorgesehenen Zuständigkeiten gefordert wird.

Teil IV: Die Rechte des Betroffenen

16. Recht auf Einsicht

1. Der Betroffene hat das Recht, bei der verantwortlichen Person Informationen über die konkreten zu verarbeitenden personenbezogenen Daten sowie über die Herkunft dieser Daten, die Zwecke ihrer Verarbeitung und die Empfänger bzw. Empfängerkategorien zu verlangen, an die diese Daten weitergeleitet werden bzw. werden sollen.

2. Alle Informationen, die dem Betroffenen zugänglich gemacht werden, müssen in einer verständlichen, klaren und einfachen Sprache gehalten sein.

3. Die anzuwendende nationale Gesetzgebung kann die wiederholte Ausübung dieser Rechte, die die verantwortliche Person dazu veranlassen würde, in kurzen Zeitabständen eine Vielzahl von Anträgen zu beantworten, einschränken, außer in den Fällen, in denen der Betroffene in seinem Antrag ein berechtigtes Interesse nachweist.

17. Recht auf Berichtigung und Löschung

1. Der Betroffene hat das Recht, bei der verantwortlichen Person die Berichtigung oder Löschung unvollständiger, ungenauer, unnötiger oder übermäßiger personenbezogener Daten zu beantragen.

2. Wenn dieser Fall eintritt, muss die verantwortliche Person die personenbezogenen Daten antragsgemäß berichtigen oder löschen. Er muss dies außerdem den Dritten, an die er die personenbezogenen Daten weitergeleitet hat, mitteilen, falls er diese kennt.

3. Die Löschung erfolgt nicht, wenn die personenbezogenen Daten entsprechend einer der verantwortlichen Person von der nationalen Gesetzgebung auferlegten Verpflichtung oder infolge der Vertragsbeziehungen zwischen der verantwortlichen Person und dem Betroffenen aufbewahrt werden müssen.

18. Widerspruchsrecht

1. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten widersprechen, wenn er einen berechtigten Grund aufgrund seiner konkreten persönlichen Situation vorbringt.

2. Dieses Widerspruchsrecht kann nicht ausgeübt werden, wenn die Verarbeitung der personenbezogenen Daten der verantwortlichen Person von der nationalen Gesetzgebung vorgeschrieben ist.

3. Jeder Betroffene kann gleichfalls solchen Entscheidungen widersprechen, die allein auf der automatischen Verarbeitung der personenbezogenen Daten beruhende Rechtsfolgen nach sich ziehen, es sei denn die Entscheidung wurde von dem Betroffenen ausdrücklich beantragt oder sie ist für den Abschluss, die Aufrechterhaltung oder Erfüllung einer Rechtsbeziehung zwischen der verantwortlichen Person und dem Betroffenen erforderlich. In diesem letzten Fall muss der Betroffene zur Verteidigung seines Rechts oder Interesses die Möglichkeit zur Geltendmachung seiner Sichtweise haben.

19. Ausübung dieser Rechte

1. Die in den Artikeln 16 bis 18 des vorliegenden Dokuments aufgeführten Rechte können folgendermaßen ausgeübt werden:

a) direkt vom Interessierten, der sich gegenüber der verantwortlichen Person angemessen ausweisen muss.

b) über einen Vertreter, der diese Eigenschaft gegenüber der verantwortlichen Person entsprechend nachweisen muss.

2. Die verantwortliche Person muss Verfahren vorsehen, die es den Betroffenen ermöglichen, die in den Absätzen 16 bis 18 des vorliegenden Dokuments vorgesehenen Rechte einfach, schnell und wirksam auszuüben. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für den Betroffenen noch Einkünfte für die verantwortliche Person verursachen.

3. Wenn die verantwortliche Person der Ansicht ist, dass im Einklang mit der anzuwendenden nationalen Gesetzgebung die Ausübung der in diesem Teil aufgeführten Rechte nicht angebracht ist, muss sie die Betroffenen vollständig über ihre Gründe informieren.

Teil V: Sicherheit

20. Sicherheitsmaßnahmen

1. Sowohl die verantwortliche Person als auch die Auftragnehmer müssen die personenbezogenen Daten, die sie verarbeiten, mit den zu dem jeweiligen Zeitpunkt geeigneten technischen und organisatorischen Mitteln schützen, um ihre Vollständigkeit, Vertraulichkeit und Verfügbarkeit zu gewährleisten. Diese Maßnahmen hängen vom bestehenden Risiko, den möglichen Folgen für die Betrof-

fenen, der Sensitivität der personenbezogenen Daten, dem technischen Zustand und dem Kontext, in dem die Verarbeitung erfolgt, sowie von der jeweiligen nationalen Gesetzgebung ab.

2. Die Betroffenen müssen von denjenigen, die an irgendeinem der Verarbeitungsschritte beteiligt sind, über alle Sicherheitsverstöße, die ihre Vermögens- und Nichtvermögensrechte wesentlich beeinträchtigen könnten, sowie über die ergriffenen Lösungsversuche informiert werden. Diese Information muss früh genug erteilt werden, damit die Betroffenen genügend Zeit haben, zur Verteidigung ihrer Rechte darauf zu reagieren.

21. Datengeheimnis

Die verantwortliche Person und diejenigen, die an irgendeinem der Verarbeitungsschritte der personenbezogenen Daten beteiligt sind, müssen darüber Verschwiegenheit bewahren. Diese Verpflichtung besteht auch dann noch, wenn die Beziehungen mit dem Betroffenen oder der verantwortlichen Person bereits abgeschlossen sind.

Teil VI: Einhaltung und Überwachung

22. Proaktive Maßnahmen

Die Staaten müssen über ihr innerstaatliches Recht Anreize für Maßnahmen schaffen, die eine bessere Einhaltung der Gesetzgebung zum Datenschutz durch diejenigen fördern, die an den unterschiedlichen Verarbeitungsschritten beteiligt sind. Zu diesen Maßnahmen können unter anderem Folgende zählen:

a) Die Einführung von Verfahren zur Vorbeugung und Feststellung von Verstößen, die auf standardisierten Modellen zur Steuerung und/oder für das Management der Informationssicherheit beruhen.

b) Die Ernennung eines oder mehrerer Beauftragter für den Schutz der Privatsphäre oder des Datenschutzes, die für die Wahrnehmung ihrer Aufsichtsfunktionen über ausreichende Qualifikationen, Ressourcen und Kompetenzen verfügen müssen.

c) Die regelmäßige Durchführung von Programmen zur Bewusstseinsbildung, Aus- und Weiterbildung der Mitglieder der Organisation zur Verbesserung ihrer Kenntnisse der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren.

d) Die regelmäßige Durchführung von transparenten Audits durch qualifizierte und vorzugsweise unabhängige Personen, bei denen die Einhaltung der auf

den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren geprüft wird.

e) Die Anpassung der Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, an die auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung, insbesondere wenn es darum geht, Entscheidungen über technische Merkmale, die technische Entwicklung und Implementierung zu treffen.

f) Die Praxisumsetzung von Datenschutz-Folgenabschätzungen vor der Implementierung neuer Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, sowie die Praxisumsetzung neuer Arten der Verarbeitung personenbezogener Daten vor der Einführung wesentlicher Veränderungen der Verarbeitungspraxis.

g) Die Annahme von Verhaltensregeln, deren Einhaltung verpflichtend ist und die es ermöglichen, ihre Wirksamkeit in Bezug auf die Befolgung und den Grad des Schutzes der personenbezogenen Daten zu messen und die wirkungsvolle Maßnahmen im Fall der Nichterfüllung festlegen.

h) Die Einführung von Eventualfallplänen, die Handlungsanweisungen für den Fall festlegen, dass eine Nichtbefolgung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung festgestellt wird, und die zumindest die Verpflichtung enthalten, die Ursache und Reichweite der eingetretenen Vorschriftsverletzung zu bestimmen, ihre negativen Auswirkungen zu beschreiben und die erforderlichen Maßnahmen zu ergreifen, damit das zukünftig nicht noch einmal geschieht.

23. Überwachung

1. In jedem Staat muss es eine oder mehrere Aufsichtsbehörden geben, die im Einklang mit dem innerstaatlichen Recht für die Überwachung der Einhaltung der in dem vorliegenden Dokument festgelegten Grundsätze verantwortlich sind.

2. Diese Aufsichtsbehörden müssen unparteiisch und unabhängig sein und sie müssen über eine angemessene technische Qualifikation, ausreichende Kompetenzen und die geeigneten Ressourcen verfügen, um über die Reklamationen, die die Interessenten an sie richten, entscheiden zu können und um die Untersuchungen und Eingriffe durchführen zu können, die die Befolgung der nationalen Gesetzgebung zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten gewährleisten.

3. Auf jeden Fall und unbeschadet der Einsprüche, die bei den genannten Aufsichtsbehörden eingelegt werden – was auch die gerichtliche Nachprüfung ihrer Entscheidungen einschließt – kann der Betroffene zur Geltendmachung seiner Rechte gemäß den Vorschriften der nationalen Gesetzgebung direkt den Rechtsweg beschreiten.

24. Kooperation und Koordination

1. Die im vorigen Artikel genannten Aufsichtsbehörden müssen bestrebt sein, im Interesse eines einheitlicheren Schutzes der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten sowohl im Inland als auch auf internationaler Ebene miteinander zu kooperieren. Um diese Kooperation zu vereinfachen, müssen die Staaten jederzeit die bei ihnen zuständigen Aufsichtsbehörden benennen können.

2. Diese Behörden bemühen sich insbesondere um die Erfüllung folgender Aufgaben:

a) den Austausch von Studien, Untersuchungsmethoden, Kommunikations- und Regelungsstrategien sowie von allen Informationen, die für eine wirksame Ausübung ihrer Funktionen hilfreich sind, insbesondere nachdem sie von einer anderen Aufsichtsbehörde im Rahmen einer Untersuchung oder Intervention um Unterstützung gebeten worden sind;

b) die Durchführung koordinierter Untersuchungen oder Interventionen – sowohl im Inland als auch auf internationaler Ebene – bei Angelegenheiten, bei denen das Interesse zweier oder mehrerer Aufsichtsbehörden zusammentreffen;

c) die Teilnahme an Verbänden, Arbeitsgruppen oder gemeinsamen Foren sowie Seminaren, Workshops oder Kursen, die dazu beitragen, gemeinsame Standpunkte zu entwickeln oder die technische Qualifizierung des Personals, das diesen Aufsichtsbehörden seine Dienste leistet, zu verbessern;

d) die Aufrechterhaltung einer angemessenen Vertraulichkeit der Informationen, die sie während ihrer Kooperation untereinander ausgetauscht hatten.

3. Die Staaten müssen die Schaffung von Kooperationsvereinbarungen zwischen regionalen, nationalen oder internationalen Aufsichtsbehörden, die zu einer wirksameren Einhaltung dieses Absatzes beitragen, fördern.

25. Haftung

1. Die verantwortliche Person haftet für solche Schäden – sowohl immaterieller als auch materieller Art – die dem Betroffenen durch die Verarbeitung personenbezogener Daten, bei der gegen die Datenschutzvorschriften verstoßen wurde, entstanden sind, es sei denn, sie kann nachweisen, dass der Schaden ihr nicht an-

zulasten ist. Dies gilt unbeschadet des Rechtsanspruchs, den die verantwortliche Person gegenüber den Auftragnehmern, die an den einzelnen Verarbeitungsschritten teilhaben, geltend machen kann.

2. Die Staaten müssen geeignete Maßnahmen fördern, damit die Betroffenen Zugang zu den entsprechenden Gerichts- oder Verwaltungsverfahren haben, die ihnen die Wiedergutmachung der oben erwähnten Schäden ermöglichen.

3. Die in den vorherigen Absätzen vorgesehene Haftung gilt unbeschadet der strafrechtlichen, zivilrechtlichen und verwaltungsrechtlichen Ahndung der Verletzung der Gesetzgebung zum Datenschutz.

4. Das Ergreifen proaktiver Maßnahmen, wie sie im Artikel 22 beschrieben werden, muss bei der Feststellung der Haftung und der Verhängung der in diesem Artikel vorgesehenen Sanktionen berücksichtigt werden.

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

45. Sitzung am 12./13. März 2009 in Sofia

Bericht und Empfehlungen zu Mautsystemen – „Sofia Memorandum“ –

– Übersetzung –

Empfehlungen:

Die Arbeitsgruppe empfiehlt, dass die Hersteller von großangelegten Mautsystemen, die persönliche Daten verarbeiten, die folgenden Empfehlungen zum Schutz der Privatsphäre der Fahrer und der Fahrzeugeigentümer einhalten:

- Die Anonymität der Fahrer kann und sollte durch die Verwendung der sogenannten „Smart-Clients“ oder anonymen Proxies gewahrt werden, die die persönlichen Daten der Fahrer unter deren alleiniger Kontrolle halten und keine Speicherung der Daten außerhalb des Fahrzeugs erfordern.
- Mautsysteme können und sollten so entworfen werden, dass die detaillierten Routendaten gänzlich und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.
- Die Verarbeitung von persönlichen Daten zu anderen Zwecken (z. B. „pay-as-you-drive“-Versicherungen oder verhaltensbasierte Werbung) sollte nur mit der eindeutigen und ausdrücklichen Einwilligung des Betroffenen möglich sein.
- Im Hinblick auf die Durchsetzung sollte das System die Identität der Fahrer oder Fahrzeugbesitzer nicht feststellen, solange nicht der Verdacht besteht, dass der Fahrer eine Zuwiderhandlung begangen hat, die als Verstoß gegen das Mautsystem definiert wird.

Hintergrund:

Großangelegte Mautsysteme, die auf einer „pay as you go“-Basis im fließenden Verkehr angelegt sind, sind keine neue Erfindung. Überlegungen zu elektroni-

schen Mautsystemen kamen in den letzten Jahrzehnten des 20. Jahrhunderts auf[1]. Verschiedene Begriffe werden verwendet, um die Nutzung moderner Informations- und Kommunikationstechnologien für Mautsysteme zu beschreiben; dazu gehören „elektronische Verkehrsgebühr", „Intelligente Verkehrssysteme" (IVS), „elektronische Mauterhebung", „Straßennutzungsgebühr", „Zeit-, Entfernungs-, Ortsgebühren", „entfernungsbasierte Straßennutzungsgebühr", „vehicles miles travelled (VMT) charging" und verschiedene weitere.

Bestehende Mautsysteme können Gebühren auf Autobahnen erheben oder eine Abgabe verlangen, wenn eine bestimmte Zone mit dem Fahrzeug befahren wird. Sie sind jedoch nicht in der Lage, Gebühren mittels eines Algorithmus zu errechnen, der an „Zeit, Strecke und Ort" gebunden ist, was für großangelegte Anwendungen erforderlich wäre. Das erwünschte Resultat eines elektronischen Mautsystems ist die Möglichkeit, nach der *tatsächlichen* Nutzung abrechnen zu können (z. B. je mehr man fährt, desto mehr zahlt man), in Abhängigkeit von der Uhrzeit der Fahrt (z. B. weniger in Zeiten außerhalb des Berufsverkehrs) und in einem variierenden Tarif, der sich anhand der gewählten Straße ermitteln lässt. Der Verkehrsfluss könnte in diesen Systemen dadurch verbessert werden, dass die Fahrer nicht gezwungen wären, an bestimmten Abrechnungsstellen anzuhalten. Prinzipiell wäre dies die gerechteste und ökologisch wünschenswerteste Möglichkeit zu bezahlen – so wie Verbraucher gewöhnlich für ihren Wasser- oder Stromverbrauch zahlen.

Abgesehen von Mautgebühren gibt es zahlreiche andere Dienste, die auf Daten in Bezug auf Zeit, Ort und zurückgelegte Strecke basieren, wie zum Beispiel Parksysteme, „pay-as-you-drive"-Versicherungen, Parkplatzfinder oder -versteigerer, die Rationierung von Straßenraum, Parkplatz-Treue-Programme, Staumelde- und Gebührensysteme, Routenplaner („Sie könnten 12 € pro Woche sparen, wenn Sie jeden Tag 30 Minuten früher losfahren würden") und intelligente Transportsysteme („Wenn Sie heute die A2 nutzen statt der A3, sparen Sie 20%"). Während die elektronische Erhebung und Verarbeitung von Daten in Bezug auf den Ort, die Identifikation einer Person sowie die Reisedaten schon heute für verschiedene Zwecke genutzt werden kann und somit auch mehrere sozioökonomische Probleme hervorruft, bezieht sich dieses Dokument vornehmlich auf datenschutzrechtlich relevante Auswirkungen von (großangelegten) elektronischen Mautsystemen.

Um besser nachvollziehen zu können, worin die datenschutzrechtlichen Auswirkungen bestehen, müssen einige der Grundprinzipien dieser Systeme näher betrachtet werden. Großangelegte Maut-Initiativen, die die Verarbeitung persönlicher Daten implizieren (andere als z. B. bei Vignetten, anonymen Aufklebern

[1] Electronic Road Charging: http://www.parliament.uk/post/pn112.pdf.

und Signalen sowie Gebührensysteme mit Mautstationen, die keinen freien Verkehrsfluss ermöglichen) werden weltweit entwickelt, z. B. in den USA (Oregon und der Puget Sound Region), Australien, Neuseeland, Kanada (auf der Schnellstraße 407), das Toll Collect System in Deutschland[2] und die in den Niederlanden[3] und Norwegen bestehenden Mautpläne. In der EG wird darüber hinaus mit der Richtlinie 2004/52/EG das Ziel verfolgt, das „pay as you go"-Prinzip im freien Verkehrsfluss in den zukünftigen Europäischen Elektronischen Mautdienst (European Electronic Toll Service – EETS) einfließen zu lassen. In seiner letzten Stufe der Entwicklung soll dieses europaübergreifende System die Möglichkeit bieten, Verkehrsgebühren für alle Arten von Straßen einschließlich Viadukten, Tunneln und anderen Objekten zu erheben. Mit dem neuen Abrechnungssystem sollen Fahrer die Gebühren zahlen können, ohne anhalten zu müssen und dadurch Verkehrsstauungen zu verursachen. Gleichzeitig ermöglicht es diese Einrichtung auch, Gebühren für alle kostenpflichtigen Autobahnen in Europa zu erheben.

Der Grund, warum die Debatten über Straßennutzungsgebühren so emotional aufgeladen sind, liegt darin, dass ortsbezogene Daten, Daten zur Identifikation und Abrechnungsdaten zusammengeführt werden. Mit anderen Worten, es wird bekannt, wer zu welcher Zeit wo war, um dafür Gebühren abzurechnen. Um das „pay as you go"-Prinzip im freien Verkehrsfluss umzusetzen (und um über ein interoperatives System zu verfügen), können Mautsysteme eine massive Überwachung der Bewegung von Personen (Fahrzeuginhaber und Fahrer) mit sich bringen. Daher müssen die Auswirkungen auf die Privatsphäre der Betroffenen sorgfältig untersucht werden. Es ist nicht schwierig, sich den enormen Wert einer zentralisierten Datenbank über das Bewegungsverhalten von Fahrern und zahlreiche Szenarios für eine Zweckentfremdung der Daten vorzustellen, bei denen Daten für andere Zwecke genutzt werden als die für die sie ursprünglich erhoben wurden (z. B. Mautgebühren). Zahlreiche Datenschutzbeauftragte haben bereits Stellungnahmen und Empfehlungen zum Schutz der Privatsphäre im Zusammenhang mit Mautsystemen erstellt (z. B. Ontario[4], Niederlande[5], Victoria/Australien[6], Norwegen[7] und Slowenien[8]). Fehlwahrnehmungen hinsichtlich der Auswirkun-

2 Es muss darauf hingewiesen werden, dass das deutsche System nur für Lastkraftwagen gilt: http://www.toll-collect.de.

3 Ministerium für Verkehr, Öffentliche Arbeit und Wassermanagement: Implementierung des Maut-Systems: http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/roadpricing/index.aspx

4 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner Ontario: http://www.ipc.on.ca/images/Resources/407-e.pdf.

5 http://www.curacaoproject.eu/documents/newsletter-issue3.pdf.

6 Eine ausführliche Studie von Mautsystemen und eine vollständige Liste an Quellen wurde durch Victoria Transport Policy Institut vorbereitet: Road Pricing, Congestion Pricing, Value Pricing, Toll Roads and HOT Lanes; http://www.vtpi.org/tdm/tdm35.htm.

7 Road Reform and Privacy: Which Way Forward? Submission by the Privacy Commissioner to the Ministry of Transport in relation to the final report of the Roading Advisory Group: http://www.privacy.org.nz/road-reformand-privacy-which-way-forward/?highlight=impact.

8 http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=568.

gen auf die Privatsphäre werden tatsächlich häufig als eines der größten Hindernisse für die Einführung großangelegter Mautsysteme betrachtet.

Grundsätzlich werden zwei etablierte Technologien für diese Systeme in Erwägung gezogen: short range communications (DSRC[9], das auch als „tag-beacon-System" bezeichnet wird) und globale Satellitennavigationssysteme (GNSS/SN[10]), welche die Position des Fahrzeugs bestimmen und die Daten über leistungsstarke drahtlose Kommunikationsnetzwerke übertragen, wobei das letztgenannte oftmals als satellitengestütztes Mautsystem bezeichnet wird.

Jedes dieser Systeme hat seine Vor- und Nachteile: die DSRC-basierten technischen Lösungen sind z. B. weiter verbreitet und wurden häufiger getestet, aber sie sind nicht auf allen Straßen anwendbar.[11] Die Wahl der Technologie hängt hauptsächlich von der Größe der Implementierung ab und unterscheidet sich in der Umsetzung nach relativ kleinen Gebieten (z. B. Großstädte[12]) und großen Gebieten (z. B. landesweit oder sogar international). Im Hinblick auf großangelegte Implementierungen scheint die DSRC-basierte Technologie an Boden zu verlieren. Wegen der enormen Anzahl an abzudeckenden Straßen sind Lösungen, die beträchtliche Infrastrukturen am Straßenrand erfordern, wie bestehende DSRC-basierte Umsetzungen, nicht so sehr geeignet, wenn auf allen Straßen Gebühren erhoben werden sollen.[13] Diese Sichtweise wird auch in einem neuen Bericht der National Surface Transportation Infrastructure Financing Commission der USA wiedergegeben.[14] Der Vorteil eines Satellitensystems besteht in seiner Flexibilität, wobei solche Systeme auf der anderen Seite noch nicht umfassend in der Praxis getestet wurden.

Die Verwendung elektronischer Mautsysteme ist, – die vielen sozio-ökonomischen Debatten und Probleme außer Acht lassend – oftmals durch zwei gebräuchliche datenschutzrechtliche Fehleinschätzungen gehemmt, die von der allgemeinen Öffentlichkeit und der Presse vertreten werden und denen entschieden entgegengetreten werden muss.

Erstens betont die Arbeitsgruppe, es muss keine Befürchtungen der Art geben, dass GPS-basierte Ansätze bedeuten würden, dass eine allumfassende Datenbank

9 DSRC – Dedicated Short Range Communications.

10 GNSS/CN – Global Navigation Satellite System/Cellular Networks.

11 Privacy-Sensitive Congestion Charging. Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle: http://www.cl.cam.ac.uk/~arb33/papers/BeresfordDaviesHarle-PrivacyAwareCongestion-SPW2006.pdf.

12 Singapore, Melbourne, Trondheim, Toronto sind Beispiele für Systeme in Großstädten.

13 Stefan Eisses, Wiebren de Jonge und Vincent Habers: Privacy And Distance Based Charging For All Vehicles On All Roads.Sh: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf.

14 National Surface Transportation Infrastructure Financing Commission: Paying Our Way, a New Framework for Transportation Finance, February 24, 2009 http://www.itif.org/index.php?id=227.

über die Position von Fahrzeugen in einer „Big Brother im Himmel"-Manier aufgebaut würde. Das GPS der USA, das russische GLONASS sowie das zukünftige Satellitensystem Galileo basieren auf passiven Empfängern, die unter Verwendung von Satelliteninformationen den Aufenthaltsort des Fahrzeugs berechnen; diese Empfänger können die Information über den Aufenthaltsort des Fahrzeugs nicht zurück zum Satelliten übermitteln. Daher müssen wir verstehen, wenn die Entscheidung für ein Satellitensystem fallen soll, dass durch Satellitennavigation ein Fahrzeug lediglich die Information über seine Position erhält, während die Ortsangaben an die Kontrollstelle des Mautabrechnungssystems über drahtlose Netzwerke übermittelt werden, so z. B. durch das GSM-Netz. Eine allumfassende Datenbank mit ortsbezogenen Daten und Identifikationsdaten könnte daher nur „vor Ort" in den Kontrollstellen entstehen: Genau davon handelt dieses Dokument.

Zweitens wird häufig der Vergleich zu Mobiltelefonen oder zu Kreditkarten gezogen, wo persönliche Daten nachverfolgt werden oder nachverfolgt werden können. Die Arbeitsgruppe möchte hervorheben, dass vereinfachende Vergleiche dieser Art nicht angemessen sind, vor allem weil Gebührenerfassungsgeräte ununterbrochen in Betrieb sein müssen (zumindest auf kostenpflichtigen Straßen), anders als im Fall von Mobiltelefonen, deren Benutzung völlig freiwillig ist. Die Möglichkeit, das Gerät auf kostenpflichtigen Straßen abzuschalten, würde es einfacher machen, die Gebührenerfassung zu umgehen, und aus diesem Grund werden die Auswirkungen von Mautsystemen auf die Privatsphäre sogar noch relevanter.

Die Verteilung des Abrechnungsprozesses

Der Abrechnungsprozess ist in vier Phasen unterteilt:

1. Bestimmung der Position des Fahrzeugs,
2. Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs,
3. Berechnung des Betrags, der für diesen Bereich fällig wird,
4. Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Ein entscheidender Faktor, wenn man die datenschutzrechtlichen Auswirkungen bestimmen möchte, ist, wie die Phasen des Abrechnungsprozesses zwischen den verschiedenen datenverarbeitenden Stellen verteilt werden. Die vier Phasen des Abrechnungsprozesses können entweder von einer Stelle vorgenommen oder zwischen zwei oder mehreren aufgeteilt werden. Konsequenterweise unterscheiden sich die datenschutzrechtlichen Auswirkungen der verschiedenen Ausfüh-

rungsmodelle. Einige der Modelle werden im Folgenden vorgestellt, zusammen mit den wichtigsten Kriterien, die beachtet werden müssen, wenn man die datenschutzrechtlichen Auswirkungen ermitteln möchte. Die zwei Hauptmodelle für Mautsysteme werden als **Thin-Client-Ansatz** und **Smart-Client-Ansatz** bezeichnet; allerdings gibt es zwischen diesen beiden Systemen noch andere Modelle, so wie der sogenannte Distributed-Role-Ansatz und Proxies. Diese vier Ansätze werden im Folgenden diskutiert.

Der „Thin-Client"-Ansatz

Die im Hinblick auf den Schutz der Privatsphäre am wenigsten favorisierte Variante eines Mautsystems liegt vor, wenn alle Daten über die Reisezeit und die Position der Fahrzeuge an eine einzige Stelle oder Institution, die als Kontrollzentrum agiert, gesendet und dort gespeichert werden. Der sogenannte „Thin-Client" (oder „On-Board-Unit" – OBU) sammelt nur Daten über zurückgelegte Strecken; alle vier Phasen des Abrechnungsprozesses werden durch die Kontrollstelle unter Verwendung einer zentralen Datenbank mit ortsbezogenen Daten, Identifikationsdaten und Abrechnungsdaten verarbeitet.

Die Arbeitsgruppe äußert ihre Bedenken hinsichtlich der Übernahme dieses Ansatzes, denn er bietet offensichtlich den geringsten Schutz für die Privatsphäre der Betroffenen. Im Prinzip ist die Frage, ob man „Thin-Clients" oder „Smart-Clients" bevorzugt, eine Frage von zentralisierter gegenüber dezentralisierter Datenverarbeitung, ein Dilemma, dem der Schutz der Privatsphäre und der Datenschutz oft begegnet.

Die Befürworter einer zentralisierten Datenbank behaupten, wenn die Daten geschützt durch angemessene Maßnahmen zur Datensicherung (z. B. entsprechende Zugangskontrolle, Protokollierung der Verarbeitung persönlicher Daten usw.) zentral gespeichert werden, könne ein höheres Sicherheitslevel gewährleistet werden, als es eine Einzelperson tun könne. Ein Gegenargument ist allerdings, dass dort, wo die Daten unter der Kontrolle eines Einzelnen sind, nur dessen Daten gefährdet sind (z. B. wenn das Fahrzeug oder das im Fahrzeug installierte Gebührenerfassungsgerät gestohlen wurden), wohingegen in dem zentralisierten Verarbeitungssystem persönliche Daten potentiell aller Betroffenen gefährdet sind (trotz eines möglicherweise höheren Grades an Sicherheit). Aus diesem Grund sind aus der Perspektive des Schutzes der Privatsphäre Lösungen zu befürworten, wo persönliche Daten nicht zentralisiert gespeichert werden, sondern im Besitz und unter der Kontrolle des Nutzers bleiben. Darüber hinaus begegnen Datenschützer regelmäßig dem Problem der zweckfremden Nutzung (dem sog. „function creep"-Phänomen) – dabei werden Daten, die ursprünglich für einen bestimmten Zweck erhoben wurden (der völlig legitim und gesetzeskonform sein kann), später für einen völlig anderen Zweck genutzt, ein Zugriff auf die Daten ist vorher unvorhergesehenen Dritten möglich, usw.

Der „Distributed-Role"-Ansatz

Manche Modelle schlagen den sogenannten Distributed-Role-Ansatz vor, der vermutlich einen besseren Schutz der Privatsphäre und der persönlichen Daten bietet. Der Distributed-Role-Ansatz stellt eine Lösung dar, die auf dem Prinzip basiert, die Daten zwischen zwei Stellen oder Parteien zu verteilen, wobei eine Partei die ortsbezogenen Daten und die Abrechnungsdaten hat und die andere nur die Identifikationsdaten der Fahrer.

Die erste Stelle oder Partei verfügt über die Identifikationsnummer des Geräts, das sich im Fahrzeug befindet, und empfängt Informationen über die Strecke, die das Fahrzeug zurücklegt (Fahrtdauer und Position), weiß aber nicht, wer der Inhaber des Geräts ist. Basierend auf diesen Informationen berechnet diese Partei die fälligen Gebühren. Die Ergebnisse dieser aggregierten Berechnungen (nur die Gebührensumme in einer bestimmten Periode, ohne Informationen über Fahrtzeit und Position) werden zusammen mit der Identifikationsnummer des Geräts an eine andere Partei übermittelt, die den Besitzer des Gerätes identifizieren kann, von dem dann die Gebühr erhoben wird; jedoch sammelt diese zweite Partei keine Informationen über die Reise des Fahrzeugs. Die Befürworter dieses Ansatzes berufen sich häufig darauf, dass durch die Verteilung der Rollen insgesamt keine Verarbeitung personenbezogener Daten stattfindet. Die Arbeitsgruppe stellt eine solche Begründung allerdings in Frage, denn eine große Menge an personenbezogenen Daten wird immer noch von den verschiedenen Parteien verarbeitet.

Diese Lösung schützt die Privatsphäre eines Betroffenen nur scheinbar, auch wenn eine Partei nur die Information über die Position des Fahrzeuges und die Reisedauer sammelt und die Identität des Fahrers nicht kennt und umgekehrt. Innerhalb dieses Ansatzes werden immer noch von einer Stelle große Mengen an Daten gesammelt und verarbeitet; nur die Identifikationsdaten werden einer anderen Stelle oder Partei anvertraut. Die Arbeitsgruppe verweist auf die Stellungnahme der Artikel 29-Datenschutzgruppe, wonach Daten, die auf eine identifizierte oder identifizierbare natürliche Person beziehbar sind, wie personenbezogene Daten behandelt werden müssen und dass die Identifizierbarkeit eines Betroffenen nicht nur durch die Mittel und Ressourcen einer datenverarbeitenden Stelle (in diesem Fall die erste Partei) zu bestimmen ist, sondern in einem generelleren Sinn. Die datenverarbeitende Stelle sollte voraussehen, dass „die Mittel, die wahrscheinlich und vernünftigerweise genutzt werden", um eine Person zu identifizieren, verfügbar sein werden, wie z. B. durch die angerufenen Gerichte (anders würde das Erheben der Daten keinen Sinn machen) und daher sollten diese Information als personenbezogene Daten behandelt werden. Unabhängig davon, ob die erste Partei einen Betroffenen, auf den sich die Orts- und Zeitangaben beziehen, selbst zu identifizieren vermag oder nicht, verarbeitet diese Partei unzweifelhaft personenbezogene Daten. Um dies zu untermauern: Es ist offensichtlich, dass in Fällen, in denen die Straßennutzungsgebühr nicht gezahlt wurde

oder die Person sich geweigert hat, die Gebühr zu zahlen, der Gläubiger einen schnellen und einfachen Weg finden muss, die Kalkulation der Gebühr zu reproduzieren, was es erforderlich macht, die Daten über die Fahrtzeit und Position einer identifizierbaren Person zu verarbeiten. Darüber hinaus ist eine Zweckentfremdung („function creep") der Daten erneut sehr wahrscheinlich, denn große Mengen von Daten werden zentral gespeichert.

Der „Smart-Client"-Ansatz

Um den Schutz der Privatsphäre der Betroffenen sicherzustellen, wäre sicherlich ein System am meisten geeignet, in dem die Daten, die zum Zweck der Mauterhebung erforderlich sind, ausschließlich unter der Kontrolle der Nutzer stehen. In diesem Fall würde die Berechnung der Gebühr durch das Gerät (das sogenannte *intelligent device*) erfolgen, wobei die Kontrollstelle nur die Summe der anfallenden Gebühren empfangen würde. Dies bedeutet, dass alle vier Abrechnungsphasen innerhalb dieses Gerätes erfolgen würden: Bestimmung der Position des Fahrzeugs; Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs; Berechnung des Betrags, der für diesen Bereich fällig wird und Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Die Anonymität des Fahrers würde auf diesem Weg gewahrt, weil alle Daten über Position und Fahrtzeit unter der alleinigen Kontrolle des Nutzers stünden. Die Nutzer sollten sich nur selbst identifizieren, wenn gewisse Unregelmäßigkeiten auftreten, die eine Identifizierung erforderlich machen: z. B. wenn der Nutzer eine richtig berechnete Mautgebühr nicht gezahlt hat, das Fahrzeug gestohlen wurde oder wenn das Gebührenerfassungssystem des Nutzers kaputt ist oder nicht richtig funktioniert (während des Befahrens einer kostenpflichtigen Straße). Die Kontrollstelle muss nur Gewissheit darüber haben, dass das Gerät im Fahrzeug, das die Gebühren berechnet, auf kostenpflichtigen Straßen richtig arbeitet.

In einem solchen System hat die Kontrollstelle keine Daten über die Position des Fahrzeugs; sie kontrolliert nur, ob das Gerät richtig funktioniert. Dieses System erfordert natürlich einige operative Maßnahmen, wie den Schutz der Einrichtungen vor Betrug (dies umfasst die Blockierung, Verfälschung, Abschirmung, Modifikation, absichtliches Herbeiführen einer Fehlfunktion etc.). Ein sehr wichtiger Aspekt sowohl des Thin- als auch des Smart-Clients ist, dass sie nicht durch den Benutzer abgeschaltet werden können, sofern sich das Fahrzeug auf einer kostenpflichtigen Straße befindet, denn das wäre eine Umgehung der Zahlungspflicht. Der Smart-Client-Ansatz ist nicht ohne Herausforderungen, es ist zum Beispiel notwendig, passende Zertifizierungsstandards anzubieten, eine richtige Installation und die Wartung der Geräte zu gewährleisten und außerdem einige andere technische Aspekte zu beachten (z. B. Energieversorgung, Funktionskontrolle, Speicherkapazitäten) und – wahrscheinlich der wichtigste Aspekt – die Kosten.

Während der Smart-Client-Ansatz kostenintensiver erscheint als der sogenannte Thin-Client-Ansatz, hat der Smart-Client-Ansatz auch gewisse ökonomische Vorteile: Das „intelligente" Gerät ist nicht anfällig für Kommunikationsstörungen (z. B. in Regionen, in denen kein GSM-Signal verfügbar ist) oder wenn die Kontrollstelle temporär nicht betriebsbereit ist, weil der Smart-Client die Gebühr selbst errechnen kann. Auf der anderen Seite kann das Gerät, das permanent Daten an die Kontrollstelle sendet und von der Kalkulation der Kontrollstelle abhängig ist (der Thin-Client) in Gebieten, in denen keine GSM-Abdeckung vorliegt oder wenn die Kontrollstelle nicht arbeitet, die Gebühr nicht allein errechnen. Es ist auch hervorzuheben, dass das „intelligente" Gerät auch Operationen im Thin-Client-Modus unterstützen kann (metaphorisch gesprochen kann der „dumme" Client nicht „intelligent" werden, während das Umgekehrte möglich ist), was eine bedeutende Voraussetzung für die Interoperabilität der Systeme ist (z. B. innerhalb des zukünftigen europäischen elektronischen Mautservices) oder mit anderen zuvor bestehenden städtischen Gebührensystemen oder City-Maut Systemen. Die Geräte in den Fahrzeugen müssen wissen, wie sie auf unterschiedliche Systeme reagieren sollen: Nachdem die Zone eines anderen Betreibers erreicht wurde, wird das Gerät Anweisungen erhalten, wie es zu arbeiten hat. Internationale Standardisierungsorganisationen (ISO und CEN) entwickeln passende technische Standards, während die Industrie bereits funktionierende Lösungen getestet hat. Während ökonomische Faktoren für die Einführung eines bestimmten Systems entscheidend sind, beeinflussen sie die datenschutzrechtlichen Implikationen nicht. Der vermeintliche Nachteil für einen Smart-Client könnte durch Massenproduktionen oder Anreize (z. B. durch die Kombination eines Freisprechmobiltelefons oder eines Satellitennavigationssystems mit dem Gerät) minimiert werden.

Der Smart-Client könnte auch eine anonyme Nutzung erleichtern, wenn Pre-Paid-Lösungen wie beim Mobiltelefon angeboten würden. Ein Fahrer sollte die Möglichkeit haben, ein Gebührenguthaben zu kaufen, das mit der On-Board-Einheit verwendet werden könnte, die dann die Kontrollstelle informieren könnte, dass die Gebühren für den Straßenabschnitt bereits vorab gezahlt wurden.

Proxies

Es sind auch weitere gemischte Ansätze bekannt und schon jetzt auf dem Markt erhältlich. Die Abrechnungsstelle kann zum Beispiel ausschließlich als technisches Zentrum agieren, als eine Art Zwischenstelle oder Proxy, der ausgewählt wird, um Berechnungen vorzunehmen. Diese Proxies (gewöhnlich als anonyme weiterleitende Proxies oder anonyme „loop-back"-Proxies bezeichnet) können im Fahrzeug oder außerhalb installiert werden und die Funktion haben, die Daten an Bord des Fahrzeugs oder an einer anderen Stelle zu speichern. Die datenschutzrechtlichen Auswirkungen eines solchen Ansatzes zu bewerten ist im Prin-

zip eine Frage des Vertrauens (z. B. ob dem Gerät vertraut werden kann und ob Dritte wirklich nicht in der Lage sind, auf die Daten zuzugreifen).

Die Arbeitsgruppe befürwortet generell solche Proxy-Ansätze, sofern deren Schutz der Privatsphäre unabhängig überprüft werden kann und sie den Grad an Schutz der Privatsphäre garantieren, der bei einem reinen Smart-Client-Ansatz erreicht wird.

Durchsetzung

Die Durchsetzung ist ein anderes entscheidendes Element, das in einer datenschutzfreundlichen Art und Weise gestaltet werden muss, wenn man anstrebt, die Anonymität der Fahrer in elektronischen pay-as-you-go-Mautsystemen zu wahren.

Der Bereich, in dem ein möglicher Missbrauch der persönlichen Daten stattfinden könnte und der besondere Aufmerksamkeit erfordert, ist die Überwachung und das Aufspüren von Zuwiderhandelnden. Die Identität der Fahrer muss nicht festgestellt werden, bis der Fahrer etwas getan hat, das als Verletzung der Nutzungsbedingungen des Mautsystems definiert ist oder als sonstiges Vergehen. Der Grundsatz der Verhältnismäßigkeit sollte in vollem Umfang beachtet werden, z. B. muss zunächst festgestellt werden, dass sich das Gebührensystem in dem Fahrzeug befindet und ob es fehlerfrei funktioniert. Wenn die Kontrolleinheit keine Verletzung hinsichtlich des Vorhandenseins oder der ordentlichen Funktionsweise des Gebührenerhebungsgeräts feststellt, sollte sie keine weiteren Schritte zur Ermittlung der Identität des Geräts oder des Fahrers einleiten. Nur wenn die Aufsichtsstelle feststellt, dass ein Gerät nicht vorhanden ist, dass das Gerät nicht ordentlich funktioniert oder dass die Einstellungen missbräuchlich verändert worden sein könnten, sollte eine autorisierte Stelle – im Einklang mit dem Verhältnismäßigkeitsgrundsatz – mit der Identifizierung des Fahrers fortfahren. Laut Berichten von Expertengruppen stellt die Erfassung des Nummernschilds und somit die Identifizierung des einzelnen Fahrers oder Fahrzeuginhabers eine zufriedenstellende Kontrollmöglichkeit in dieser Hinsicht dar.

Das oben Gesagte bedenkend sollten die persönlichen Daten der Fahrer, die dem System nicht zuwidergehandelt haben, auf keine Art und Weise, außer durch den Fahrer selbst, verarbeitet werden. Diesem Ansatz folgend würde die Kontrollstelle lediglich überprüfen, ob das Gerät im Fahrzeug richtig funktioniert, und nur eine autorisierte Person (für den Zweck, für den dieser Person die Berechtigung zum Zugriff auf personenbezogene Daten erteilt wurde) darf die Identität der Betroffenen erfragen oder Informationen über die Position des Fahrzeugs erhalten. Dies darf nur unter bestimmten Umständen erlaubt sein, die im Vorhinein bestimmt und aufgelistet sein müssen (z. B. wenn an dem elektronischen Mautgerät in dem Fahrzeug unerlaubte Änderungen vorgenommen wurden, wenn das Gerät auf kostenpflichtigen Straßen nicht funktioniert oder wenn das Auto gestohlen

wurde). Jeder Zugriff zum Zweck der Durchsetzung auf Informationen über die Position des Fahrzeugs, die Reisezeit und Gebühren muss entsprechend dokumentiert werden, so dass eine vollständige Nachüberprüfung möglich ist. Es wäre unzulässig, einen nicht autorisierten und nicht registrierten Zugang zu den Daten in dem Gerät zu erlauben.

Die Frage der optionalen oder zwangsweisen Verwendung

Wenn die Nutzung der On-Board-Einheit optional wäre, könnten die Fahrer entweder die On-Board-Einheit oder eine andere Methode wählen, die Gebühren zu erheben und abzurechnen (z. B. Anmeldung und Zahlung an einer automatischen Station). Hervorgehoben werden muss, dass der Nutzer weder in dem optionalen noch in dem freiwilligen Schema das Gerät abschalten kann, während er auf einer kostenpflichtigen Straße fährt. Die Frage nach einer optionalen oder freiwilligen Nutzung des Mautgeräts und den Auswirkungen auf die Privatsphäre ist zu einem großen Maß eng mit der Frage der Überwachung verbunden. Im Prinzip ist die optionale Verwendung benutzerfreundlicher, weil die Betroffenen ihre vorherige Einstimmung in die Verarbeitung ihrer persönlichen Daten erteilen können; allerdings sind auch die Durchsetzungsprobleme eng mit dieser Frage verbunden und sollten insofern auch bewertet werden.

Ein Beispiel aus der deutschen Erfahrung mit Lastkraftwagen (Toll Collect System) zeigt, dass 90 % der LKW-Fahrer sich für die Installation eines Satellitensystems entschieden haben; weniger als 10 % bevorzugen andere Systeme. Die Zuverlässigkeit und Genauigkeit des installierten Systems liegt bei 99,75 %, was bedeutet, dass gewissermaßen alle Probleme in Bezug auf die Durchsetzung und Unregelmäßigkeiten bei denen auftreten, die kein Gerät installiert haben und sich bei Mautstationen anmelden und dort manuell bezahlen. Wenn man diese Erfahrungen mit LKW auf ein Mautsystem für private Fahrzeuge überträgt (insbesondere wenn dies schlussendlich auf allen Straßen eingesetzt werden soll), scheint eine optionale Verwendung wenig realistisch. Ein optionales Mautsystem im freien Verkehr würde die Installation sehr komplexer und teurer Kontrollsysteme auf allen kostenpflichtigen Straßen erfordern (Videoüberwachung, Identifizierung der Nummernschilder etc.), was im Ergebnis zu einem höheren Grad an Überwachung und einem größeren Eingriff in die Privatsphäre führen würde als ein verbindliches System. Die Entscheidung, ob man eine optionale Verwendung erlaubt oder eine verbindliche Nutzung durchsetzt, hängt wesentlich von der Größe der Implementierung und den für die Durchsetzung verfügbaren Ressourcen ab und kann daher im kleinräumigen und großräumigen Ansatz (national oder sogar international) unterschiedlich sein.[15]

[15] In den Niederlanden werden zum Beispiel alle registrierten Fahrzeuge im Land von dem Mautsystem erfasst. Es gibt allerdings Ausnahmen innerhalb dieser Gruppe: Motorräder und bestimmte Fahrzeuge wie Rettungswagen. Ausgenommene Fahrzeuge werden nicht mit einem On-Board-Gerät ausgestattet.

Die Rechte der Betroffenen

Eine besondere Aufmerksamkeit sollte der Frage von umstrittenen Gebühren gewidmet werden. Wenn man sicherstellen will, dass personenbezogene Daten unter der alleinigen Kontrolle des Nutzers verbleiben, sollte ein Zugriff zu den Daten nur ermöglicht werden, wenn der Nutzer es ausdrücklich verlangt. Mautsysteme können und sollten so gestaltet sein, dass die detaillierten Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden und jede Frist, innerhalb derer die Gebühr angefochten werden kann, abgelaufen ist (wie es z. B. im Londoner City-Maut System geschieht).

Ein Fernzugriff auf die Rohdaten durch die Kontrollstelle oder durch Dritte zu anderen als Durchsetzungszwecken, unabhängig davon, ob die Daten in dem Gerät gespeichert sind oder nicht, sollte nur mit Einwilligung des Betroffenen erfolgen. Ebenso sollte die Verarbeitung zu anderen Zwecken (z. B. „pay-as-you-go"-Kfz-Versicherung oder verhaltensbasierte Werbung) nur möglich sein, wenn der Fahrzeughalter seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Ergebnis

Die Arbeitsgruppe ist der Ansicht, dass die zentralisierte Verarbeitung persönlicher Daten für Mautsysteme im freien Verkehrsfluss nicht erforderlich und daher gemäß dem Verhältnismäßigkeitsgrundsatz nicht gerechtfertigt ist, angesichts der nachweisbaren Existenz technischer Lösungen, die eine zentralisierte Verarbeitung der Daten nicht erfordern. Ein starker Schutz der Privatsphäre kann und sollte von Beginn an so gestaltet sein, dass Informationen, die an die Kontrollstelle übermittelt werden, sich lediglich auf die Höhe der Gebühren beziehen und nicht auf Ort und den Zeitpunkt der Reise. Wie es in dem Bericht der National Surface Transportation Infrastructure Financing Commission der USA dargestellt wurde, würde ein solches System einen wesentlich höheren Grad an Privatsphäre bieten als andere Informationssysteme in unserer Gesellschaft, wie z. B. Kreditkarten und Mobiltelefonsysteme, bei denen der Anbieter nicht weiß, wie viel eine Person schuldet, aber wo Personen einkaufen und welche Nummern sie angerufen haben (mehr oder weniger präzise sogar den Ort). Mautsysteme können und sollten so gestaltet sein, dass detaillierte Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, sobald die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.

Die Anonymität des Fahrers sollte innerhalb des Systems durchgängig gewährleistet bleiben. Im Hinblick auf die Durchsetzung sollte das System die Identität des Fahrers nicht feststellen, es sei denn, der Fahrer hat etwas getan, das als Ver-

letzung der Nutzungsbedingungen des Mautsystems definiert ist. Die Verarbeitung der Daten zu anderen Zwecken (z. B. „pay-as-you-go"-Kfz-Versicherung oder verhaltensbasierte Werbung) sollte nur möglich sein, soweit der Betroffene seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Im Prinzip ist die Frage nach der Privatsphäre in elektronischen Mautsystemen relativ einfach: Wesen und Zweck jedes groß angelegten Mautsystems erfordern die Verarbeitung persönlicher Daten, setzen aber nicht eine zentralisierte Verarbeitung der personenbezogenen Daten (solange keine Zuwiderhandlung begangen wurde), die unverhältnismäßige Verarbeitung der Daten, den Zugang zu persönlichen Daten oder eine allgegenwärtige Überwachung voraus. Die fundamentalen Grundsätze des Schutzes persönlicher Daten streben danach, die Anonymität zu bewahren; die Technologie kann und sollte in einer Weise eingesetzt werden, die es ermöglicht, die Anonymität der Fahrer zu erhalten. Jede Abweichung von diesem Grundsatz würde einen zusätzlichen Eingriff in die bereits erodierte Privatsphäre in der Informationsgesellschaft bedeuten.

Empfehlung zum Datenschutz und Elektronik-Abfall („E-Waste“)

– Übersetzung –

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation,

Berücksichtigend, dass die zunehmende und umfassende Nutzung elektronischer Geräte und Anlagen sowohl für private als auch für öffentliche Zwecke die Notwendigkeit mit sich bringt, solche Einrichtungen auch angemessen zu entsorgen und/oder zu recyceln;

Berücksichtigend, dass solche elektronischen Geräte und Anlagen Einrichtungen zur Kommunikation enthalten und in Anbetracht der zunehmenden technischen Konvergenz und des Vorhandenseins von Mehrzweckgeräten[1];

Berücksichtigend, dass die Europäische Union seit langem eine umweltfreundliche Politik verfolgt, die die Verminderung der Ausbeutung natürlicher Rohstoffe sowie Maßnahmen zur Verminderung der Verschmutzung umfasst; und berücksichtigend, dass solche Ziele auch seit langem in verschiedenen Nicht-EU-Staaten verfolgt werden;

Berücksichtigend, dass die angesprochenen Strategien angemessene Recycling- und Abfallbeseitigungsmaßnahmen in Bezug auf Elektro- und Elektronikabfall (E-Waste) vorsehen, wie sie mit der EG der Richtlinie 2002/96/EG[2] auf den Weg gebracht wurden;

Berücksichtigend, dass es einschlägigen regulatorischen Instrumenten bisher weder auf nationaler noch auf überstaatlicher Ebene gelungen ist, den Risiken, die mit dem Recycling oder der Beseitigung von Elektro- und Elektronik-Geräten insoweit einhergehen, dass solche Geräte persönliche Daten über den Nutzer des Geräts oder Dritte enthalten können, hinreichend Rechnung zu tragen;

Berücksichtigend, dass es notwendig ist, die Aufmerksamkeit aller Interessenvertreter – sei es im öffentlichen oder im privaten Bereich – inklusive solcher staatlichen Stellen und Firmen, die die E-Waste recyceln oder verwerten, auf dieses Thema zu lenken, insbesondere insoweit, als dass diese Stellen, vor allem dieje-

[1] Abgesehen von und über solche Geräte und Ausstattungen hinaus, die ursprünglich für Kommunikationszwecke bestimmt waren, gibt es eine zunehmende Anzahl an Geräten, die als Datenübertragungsendgerät eingesetzt werden können, wenn sie an ein elektronisches Kommunikationsnetzwerk angeschlossen sind.

[2] Richtlinie 2002/96/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 über Elektro- und Elektronik-Altgeräte.

nigen, die sich selbst Kommunikationsgeräte und -Ausstattungen zunutze machen, als datenverarbeitende Stellen verpflichtet sind, angemessene Maßnahmen zu ergreifen, um die Sicherheit persönlicher Daten zu gewährleisten, wobei diese Maßnahmen zum Zeitpunkt des Recycelns und/oder des Beseitigens derjenigen Geräte und Ausstattungen, die zur Verarbeitung persönlicher Daten eingesetzt wurden, durchgeführt werden müssen;

Unter Bezugnahme auf generelle bestehende Leitlinien, wie sie von manchen nationalen Datenschutzbehörden in Verbindung mit der angemessenen Vernichtung und/oder Löschung von persönlichen Daten aufgestellt wurden[3];

EMPFIEHLT

1. Dass die nationalen Regulierungsbehörden, in Zusammenarbeit mit den nationalen Datenschutzbehörden und allen relevanten Interessenvertretern aus der Industrie, angemessene Maßnahmen auf den Weg bringen, die den unberechtigten Zugang zu persönlichen Daten, die in zu recycelnden und/oder zu verwertenden Geräten gespeichert sind, verhindern oder begrenzen. Darüber hinaus muss sichergestellt werden, dass die entsprechenden Maßnahmen auch von den datenverarbeitenden Stellen umgesetzt werden. Solche Maßnahmen könnten zum Inhalt haben, dass Informationstechnik und/oder andere Werkzeuge und/oder Vorkehrungen – soweit als möglich als Freeware (kostenlose und lizenzfreie Software) – bereitgestellt werden, um die Speicherung personenbezogener Daten in den entsprechenden Geräten zu begrenzen oder zu verhindern, da es sich als schwierig erweisen wird, solche Daten zu entfernen, ohne das betreffende Gerät und/oder Equipment zu zerstören[4];

2. Dass die Maßnahmen zum Schutz personenbezogener Daten, die von den datenverarbeitenden Stellen zu ergreifen sind, den unterschiedlichen Risiken Beachtung schenken, die mit Recyclingprozessen im Gegensatz zu Abfallbeseitigungsmaßnahmen von Elektronik-Abfall einhergehen;

---

[3] Vgl. z. B.: Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe „Sicheres Löschen magnetischer Datenträger". Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes, Stand: 7.10.2004 (http://www.datenschutz.mvnet.de/dschutz/informat/magloe/magloe.html); Orientierungshilfe „Datensicherheit bei USB-Geräten", Stand: November 2003 (http://www.datenschutz.mvnet.de/dschutz/informat/usb/oh_dsusb.html); Hellenic Republic Data Protection Authority, Directive 1/2005, Athens 17-10-2005, Ref. Num. 3845; Entscheidung der Italienischen Datenschutzbehörde vom 9. Dezember 2008, abrufbar unter: http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482; siehe auch: Pressemitteilungen des Berliner Beauftragten für den Datenschutz und die Informationsfreiheit vom 24. Januar 2007 (http://www.datenschutz-berlin.de/content/nachrichten/pressemitteilungen/pressemitteilungen-im-jahr-2007) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 23. Dezember 2008 (http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_37_08_KeinePersoenlichenDatenAufAusrangiertenPCsVergessen.html?nn=409394).

[4] In dieser Hinsicht kann auf herausnehmbare Speicherkarten verwiesen werden, wie sie in Mobiltelefonen eingesetzt werden.

3. Dass mit der Einführung von Maßnahmen zum Schutz persönlicher Daten in Verbindung mit dem Recycling von Elektronik-Abfall insbesondere sichergestellt werden muss, dass die personenbezogenen Daten von magnetischen und elektronischen Medien unter Einhaltung des gegenwärtigen Stands der Technik, wie zum Beispiel durch mehrfaches Überschreiben oder Entmagnetisierung (degaussing), gelöscht werden;

4. Dass bei der Einführung von Maßnahmen zum Schutz personenbezogener Daten in Verbindung mit dem Recycling von Elektronik-Abfall die Zweckmäßigkeit der Implementierung effektiver Mechanismen zur Zerstörung magnetischer und elektronischer Medien berücksichtigt werden soll, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern;

5. Dass die zuständigen nationalen und supranationalen Stellen angemessene Aufklärungsmaßnahmen ergreifen, um die datenverarbeitenden Stellen und die Nutzer über die einschlägigen Risiken und Anforderungen zu informieren.

46. Sitzung am 7./8. September 2009 in Berlin

DAS ERBE VON EMAILS: WAS GESCHIEHT, WENN EIN NUTZER IN EINE ANDERE DOMÄNE WECHSELT?

Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft

– Übersetzung –

Einleitung

Für viele Menschen sind Emails das primäre Kommunikationsmittel geworden, das traditionelle Briefe sowohl für private als auch für geschäftliche Zwecke ersetzt. Bei einem Email-Account, der eine Person identifizieren und für private Kommunikation genutzt werden kann, handelt es sich nach allgemeiner Auffassung der Datenschutzbehörden um personenbezogene Daten.

Eine Person kann einen oder mehrere Email-Accounts haben, die über einen kostenlosen oder kostenpflichtigen Dienst angeboten werden; einem Angestellten kann es auch von seinem Arbeitgeber gestattet sein, eine geschäftliche Email-Adresse für private Zwecke zu nutzen. Email-Accounts, die scheinbar umsonst zu haben sind, können mit anderen Informationsdiensten, wie Breitbanddiensten und Kabelfernsehen gebündelt sein.

Was also geschieht, wenn eine Person ihren Email-Anbieter wechseln muss?

Die Analogie in der realen Welt besteht darin, aus einem Haus in ein anderes umzuziehen. Gewöhnlicherweise schicken Personen, die umziehen, Briefe an alle ihre geschäftlichen und privaten Kontakte, um diese über den Umzug zu informieren. Darüber hinaus wird die Person in der Regel mit dem Post-Zusteller vereinbaren, dass alle Briefe an die neue Adresse weitergeleitet werden – heutzutage keine einfache Angelegenheit, da viele Postzustellungsunternehmen eingebunden sein können. Die Lösung kann darin bestehen, den neuen Bewohnern für die verbleibende Post Etiketten mit der neuen Anschrift zu geben.

Wenn wir diese Analogie aus der echten Welt in die virtuelle Welt übertragen, müssen wir alle Dienste der Informationsgesellschaft in Betracht ziehen, die es mit sich bringen, eine Person anhand des Namens zu identifizieren. Dies kann die zunehmend beliebten sozialen Netzwerke umfassen und auch Accounts bei virtuellen Marktplätzen, die eine Email-Adresse zu Zwecken der Validierung nutzen und an die elektronische Güter und Belege etc. gesendet werden können. Das-

selbe Problem könnte sich auch im Fall des Verschickens von SMS im Zusammenhang mit Mobiltelefonen ergeben.

Wechsel einer Email-Adresse oder eines Accounts bei Diensten der Informationsgesellschaft

Wenn eine Email-Adresse oder ein virtueller Account geschlossen wird, besteht die Möglichkeit, dass ein neuer Nutzer den Benutzernamen wieder benutzen und dessen „Vergangenheit erben" könnte. Diese Möglichkeit ist im Fall von kostenlosen „email-for-life"-Diensten (sowie bei gmail oder hotmail) ziemlich abwegig, da solche Anbieter kaum abgelaufene Accounts neu verteilen würden.

Außer wenn der Nutzer für eine Domain gezahlt hat, wird der Domain-Name aller Wahrscheinlichkeit nach mit dem Service-Provider verbunden und nicht von einem auf den anderen Anbieter übertragbar sein.

Beispielhaft muss man sich jemanden vorstellen, der einen sehr gebräuchlichen Namen hat, wie „Joe Doe", der in Portugal lebt, gmail benutzt, sich bei einem Kabelfernsehkanal anmeldet und für eine Firma namens Xpto arbeitet; Joe könnte mehrere Email-Accounts haben, wie z. B. **joedoe99@gmail.com**, **joedoe@cabletv.pt**, **joedoe@xpto.pt**. Zusätzlich könnte er eine persönliche Domain für seine Familie gekauft haben oder nutzen wie **doe.pt** und die Email-Adresse **joe@doe.pt** benutzen.

Wenn er seinen gmail-Account aufgeben möchte, kann er ziemlich sicher sein, dass sein Account **joe.doe99@gmail.com** nicht wieder vergeben wird, aber wenn er das Abonnement für das Kabelfernsehen beendet oder seinen Arbeitsplatz wechselt, dann wird er vielleicht entdecken, dass er nicht mehr in der Lage ist, auf seine Emails über die Accounts **joedoe@cabletv.pt** oder **joedoe@xpto.pt** zuzugreifen.

Auf der anderen Seite sollte die Domain **doe.pt** nicht ohne Weiteres auf einen anderen übertragbar sein, vorausgesetzt, seine Familie zahlt weiter dafür.

Wenn dagegen sein früherer Kabelfernsehanbieter einen neuen Kunden hat und sein früherer Arbeitgeber einen neuen Angestellten, der auch Joe Doe heißt, könnten sie entscheiden, seine alte Email-Adresse an diese neue Person zu vergeben. In diesem Fall wird der neue „Inhaber" wohl Email-Nachrichten und persönliche Information „erhalten", die an den ursprünglichen Inhaber gerichtet waren.

In gleicher Weise kann jeder neue Besitzer einer wieder vergebenen Domain, bei der die Bezahlung ausgelaufen ist, Email-Verkehr erhalten, der an den früheren Besitzer gerichtet ist.

Mögliche negative Folgen

Dies kann zahlreiche negative Folgen haben:

- Wenn der Nutzer Abonnements für Email-Newsletter nicht kündigt oder nicht alle Kontakte über den Wechsel seiner Adresse informiert hat, wird der neue Besitzer Informationen erhalten, die für den früheren Besitzer bestimmt sind, was zur Preisgabe personenbezogener Daten führt.

- Wenn ein Beschäftigter seine Arbeitsstelle verlässt, könnte der neue Beschäftigte persönliche Nachrichten erhalten, die für den ehemaligen Beschäftigten bestimmt sind, sowie auch geschäftliche Emails für denjenigen, der den ehemaligen Beschäftigten ersetzt hat.

- Wenn der Vertrag mit einem Internet-Service-Provider beendet wird, könnte sich der neue Kunde versehentlich oder absichtlich als der ehemalige Inhaber der Email-Adresse ausgeben.

Ähnliche Erwägungen sind auf andere Dienste der Informationsgesellschaft anwendbar, wie z. B. Instant Messaging, VoIP/Internettelefonie und soziale Netzwerke, besonders wenn die Email-Adresse zur Authentifizierung genutzt wird. Wenn ein Benutzer einen Dienst beenden möchte, kann der neue Benutzer Nachrichten empfangen, die für den ehemaligen Nutzer bestimmt sind, oder – was schwerwiegender ist – versuchen, als der alte Benutzer aufzutreten.

Während die mobile Rufnummernmitnahme (mobile number portability – MNP), die Möglichkeit des Auftretens dieses Problems im Zusammenhang mit Mobiltelefonen reduzieren kann, mag die Möglichkeit zur Rufnummernmitnahme nicht immer verfügbar sein (z. B. im Fall von mangelndem Bewusstsein, Umzug in ein anderes Land, Tod des Nutzers oder bei manchen Formen von „pay-as-you-go"-Diensten). Dann besteht wieder die Möglichkeit, dass jemand anders eine kürzlich verwendete Rufnummer und das damit verbundene Erbe an SMS-Nachrichten übernimmt.

Dies ist deshalb besonders problematisch, weil SMS in der Regel in besonders vertraulichen Bereichen wie Online-Banking und E-Ticketing verwendet werden.

Der Benutzer könnte dann das Gefühl haben, dass er seine Email-Adresse oder die Nummer seines Mobiltelefons, einen bestimmten Internet-Service-Provider oder Mobilfunkanbieter für immer behalten muss, um seine Privatsphäre und persönliche Sicherheit zu wahren.

Empfehlungen

Die Arbeitsgruppe hat sich schon früher mit Aspekten des Schutzes der Privatsphäre und der Sicherheit im Zusammenhang mit Telekommunikationsdiensten[1], Internetdiensten[2] und sozialen Netzwerken[3] beschäftigt.

Die Arbeitsgruppe ist der Auffassung, dass ein Anbieter von Diensten der Informationsgesellschaft (im Folgenden als „ISP" bezeichnet) Dienste anbieten sollte, die es dem Nutzer ermöglichen, jede schädigende Konsequenz, die aus der Kündigung des Vertrages resultieren könnte, zu minimieren, und gibt folgende Empfehlungen:

1. Der ISP sollte eine Übergangsphase von mindestens drei Monaten vorsehen, bevor irgendjemand die Email-Adresse, persönliche Domain oder Telefonnummer eines vormaligen Nutzers übernehmen kann.
2. Der ISP sollte dem Nutzer eine Möglichkeit bieten, dass für die Dauer der Übergangsphase Nachrichten, die an die ausgesetzte Email-Adresse oder Nummer geschickt werden, zusammen mit einer passenden automatisierten Nachricht zurückgesandt werden.
3. Der ISP sollte einen Warnhinweis anbieten, der den Nutzer über das mit dem Ende des Vertrags verbundene Risiko, seine Email-Adresse zu verlieren, informiert sowie über die mögliche Preisgabe von Daten.
4. Der ISP könnte eine Funktion wie einen „wandernden" Ordner anbieten, in dem die Nutzer die Login-Daten speichern könnten, die für Web-Dienste verwendet werden. Wenn der Account geschlossen oder der Vertrag beendet wird, könnte er den Ordner zu einem anderen Dienst mitnehmen. Dies würde erfordern, dass der Nutzer solche Informationen stets aktualisiert.
5. Dienste, die eine SMS-Authentifizierung verwenden (z. B. Online-Banking), sollten die Mobiltelefonnummer anzeigen, an die die Nachricht verschickt wurde. Wenn der Dienst keine Rückmeldung von dem Nutzer erhält, dass die Transaktion fortgeführt werden soll, sollte die betreffende Nummer als gefährdet eingestuft und so lange ausgesetzt werden, bis der Inhaber der Accounts erneut die Nummer des zu verwendenden Mobiltelefons bestätigt.
6. Eine Person, die eine permanente Email-Adresse haben möchte, sollte einen persönlichen Domain-Namen registrieren, der auch als Homepage, Weblog

---

[1] Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz (Berlin 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742.

[2] Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP) (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf?1201702122

[3] Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – Rom Memorandum – (Rom 3/4.03.2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?1234867489

etc. genutzt werden kann. Allerdings erfordert eine persönliche Domain in der Regel eine jährliche Erneuerung, anderenfalls kann sie verloren gehen und an eine andere Person vergeben werden.

7. Arbeitgeber und andere Organisationen, die geschäftliche Email-Adressen verteilen, sollten den Mechanismus festlegen, der eingreift, wenn ein Mitarbeiter geht oder seine Funktion innerhalb des Unternehmens wechselt. Nachrichten an eine solche Adresse sollten zurückgesandt werden, oder es sollte eine automatisierte Nachricht verschickt werden, sodass der Absender weiß, dass die Adresse des Angestellten sich geändert hat oder nicht mehr besteht.

B. Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließung vor der 18. Konferenz (vom 26. Januar 2009)

Keine weitere Einschränkung der Transparenz bei Finanzbehörden

Der Bundesrat hat im Zuge seiner Beratung des Zahlungsdiensteumsetzungsgesetzes (BT-Drs. 16/11613) vorgeschlagen, das Informationsfreiheitsgesetz des Bundes noch weiter einzuschränken: Ausgerechnet gegenüber Bundesbehörden der Finanz-, Wertpapier- und Versicherungsaufsicht soll es künftig kein Recht auf Informationszugang mehr geben. Die Entscheidung liegt jetzt beim Deutschen Bundestag.

Die Informationsfreiheitsbeauftragten in Deutschland lehnen die Schaffung einer solchen pauschalen Ausnahme entschieden ab. Es kann nicht sein, dass gerade bei den Aufsichtsbehörden, deren Tätigkeit durch die aktuelle Finanz- und Bankenkrise in die öffentliche Kritik geraten ist, die Transparenz noch weiter eingeschränkt wird. Das Vertrauen der Öffentlichkeit in die staatlichen Kontrollinstanzen sollte durch mehr Offenheit wiederhergestellt und nicht durch Einschränkung der Informationsfreiheit noch weiter erschüttert werden.

Informationen, die in diesem Bereich tatsächlich geheimhaltungsbedürftig sind, werden bereits heute durch das Informationsfreiheitsgesetz ausreichend geschützt. So müssen solche Informationen nicht offen gelegt werden, deren Bekanntwerden im jeweiligen Einzelfall nachteilige Auswirkungen auf die Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden haben kann; ohnehin sind Betriebs- und Geschäftsgeheimnisse sowie personenbezogene Daten geschützt. Damit besteht schon gegenwärtig im Bereich der Finanzaufsicht nur eine begrenzte Transparenz. Auch die Gerichte entwickeln hier differenzierte und sachgerechte Kriterien für die Anwendung der gesetzlichen Geheimhaltungsgründe. Diese von der Rechtsprechung eingeleitete Gesetzesauslegung nun durch eine Gesetzesänderung korrigieren zu wollen und den Zugang zu Informationen der Finanzaufsichtsbehörden gänzlich auszuschließen, widerspricht Sinn und Zweck des Informationsfreiheitsgesetzes und den berechtigten Auskunftsinteressen der Bürgerinnen und Bürger. Durch die vorgeschlagene Gesetzesänderung würde sogar der Zugang zu Informationen über solche Unterneh-

men ausgeschlossen, die kontinuierlich gegen schwerwiegende Straftatbestände verstoßen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an den Deutschen Bundestag, eine solche Einschränkung des Informationsfreiheitsgesetzes nicht zu beschließen.

2. Entschließungen der 18. Konferenz am 23./24. Juni 2009 in Magdeburg

Informationszugang für Bürgerinnen und Bürger verbessern!

Die Anwendung der Informationsfreiheitsgesetze in Bund und Ländern hat bewiesen: Der freie Zugang von Bürgerinnen und Bürgern zu Informationen öffentlicher Stellen ist auch in Deutschland fester Bestandteil der Demokratie. Seit 1998 haben nun schon elf Länder und der Bund ein allgemeines Informationsfreiheitsgesetz erlassen. Umweltinformationsgesetze und das Verbraucherinformationsgesetz ergänzen und erweitern den freien Zugang zu Informationen in spezifischen Bereichen.

In einer Vielzahl von Fällen haben die Bürgerinnen und Bürger Zugang zu amtlichen Informationen erhalten. Die Erfahrungen zeigen aber auch, dass sie immer wieder auf unnötige Hindernisse stoßen, wenn sie ihre Informationsrechte geltend machen wollen. So ist es für alle Beteiligten, auch für die Behörden, immer wieder schwer zu bestimmen, welches Informationszugangsrecht gilt. Zudem mindern teilweise ausufernde Ablehnungsgründe die Erfolgsaussichten von Zugangsanträgen.

Die Informationsfreiheitsbeauftragten halten es deshalb zugunsten einer größeren Transparenz des Verwaltungshandelns für geboten,

- einen unkomplizierten und umfassenden Zugang zu amtlichen Informationen zu ermöglichen
- Ausnahmen vom Informationszugang auf das unabdingbar notwendige Maß zu beschränken
- den Informationszugang grundsätzlich kostenfrei zu gewähren
- die Verfahren zur Rechtsdurchsetzung des Informationsanspruchs zu beschleunigen

- Veröffentlichungspflichten als zweite Säule des Informationszugangs im Sinne einer aktiven Informationspolitik zu stärken.

Die Konferenz der Informationsfreiheitsbeauftragten Deutschlands sieht darüber hinaus die Notwendigkeit, die Bewertung des Informationsfreiheitsgesetzes des Bundes auf unabhängiger wissenschaftlicher Grundlage anzugehen.

Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern

Beschäftigte, die Missstände und Rechtsverstöße in Behörden oder Unternehmen aufdecken (Whistleblower), sorgen dort für mehr Transparenz. Beispiele wie die Aufdeckung der sog. Gammelfleischskandale, der heimlichen Überwachung von Mitarbeiterinnen und Mitarbeitern, der Ausspähung von Telefonverbindungsdaten und der übermäßigen Erfassung von Gesundheitsdaten belegen das. Nur weil Beschäftigte betriebsinterne Vorgänge offenbarten, gelangten die Rechtsverstöße überhaupt ans Licht.

Das öffentliche Interesse an der Offenlegung von Missständen muss mit den zivil- und arbeitsrechtlichen Loyalitätspflichten der Beschäftigten gegenüber den Arbeitgeberinnen und Arbeitgebern in einen angemessenen Ausgleich gebracht werden. Transparenz kann nur erreicht und gefördert werden, wenn die Hinweisgeberinnen und Hinweisgeber keine Repressalien durch Arbeitgeberinnen und Arbeitgeber und die Kollegenschaft befürchten müssen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Deutschen Bundestag auf, für mehr Informationsfreiheit einzutreten, indem endlich der Schutz von Whistleblowern gesetzlich festgeschrieben wird. Beschäftigte sollen keine arbeitsrechtlichen Konsequenzen befürchten müssen, nur weil sie Rechtsverstöße im Arbeitsumfeld anzeigen. Die Konferenz bedauert, dass ein erster Schritt hierzu, nämlich mit einem neuen § 612a BGB den Informantenschutz für Beschäftigte durch ein Anzeigerecht zu regeln, nicht weiterverfolgt wurde.

Der Gesetzgeber ist auch gehalten, den Transparenzgedanken und die datenschutzrechtlichen Belange der meldenden sowie der gemeldeten Person in ein ausgewogenes Verhältnis zu bringen. Hierfür hält die Konferenz folgende Erwägungen für maßgeblich:

- Zur Wahrung der schutzwürdigen Belange der Beteiligten sind verbindliche Verfahrensregeln in Behörden und Unternehmen unerlässlich.

- Whistleblowern muss die vertrauliche Behandlung des Hinweises zugesagt werden können.

- Auch die Rechte der belasteten Person, z. B. auf Benachrichtigung, Auskunft über sowie Berichtigung und Löschung von Daten, müssen berücksichtigt werden.

- Zum Schutz der Vertraulichkeit können Beschwerden an unabhängige ggf. externe Stellen (Ombudsleute) geschickt werden, die sie nur anonymisiert weitergeben dürfen.

3. Entschließung der 19. Konferenz am 16. Dezember 2009 in Hamburg

Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen!

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder begrüßt die Ankündigung in der Koalitionsvereinbarung der neuen Bundesregierung, die Ansprüche der Verbraucherinnen und Verbraucher auf Information in einem einheitlichen Gesetz zur Regelung der Informationsansprüche der Bürgerinnen und Bürger zusammenzufassen.

Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich insbesondere im Informationsfreiheitsgesetz, im Umweltinformationsgesetz und im Verbraucherinformationsgesetz. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Rechte der Bürgerinnen und Bürger und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei.

Bei der anstehenden Überarbeitung sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Die vielfältigen gesetzlichen Ausnahmetatbestände, wegen derer ein Informationszugang verweigert werden kann, gehören auf den Prüfstand.