Dokumente
zu Datenschutz
und Informationsfreiheit
2011

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 2012

Inhaltsverzeichnis

Seite

Vorwort 7

A. Dokumente zum Datenschutz 9

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 9

1. Entschließungen der 81. Konferenz am 16./17. März 2011 in Würzburg 9

– Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen 9

– Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze 10

– Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten! 12

– Beschäftigtendatenschutz stärken statt abbauen 13

– Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten 15

– Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene 15

2. Entschließung zwischen der 81. und 82. Konferenz (vom 27. Juli 2011) 16

– Funkzellenabfrage muss eingeschränkt werden! 16

3. Entschließungen der 82. Konferenz am 28./29. September 2011 in München 18

– Datenschutz bei sozialen Netzwerken jetzt verwirklichen! 18

– Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick 19

– Datenschutz als Bildungsaufgabe 20

– Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing 22

– Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen! 23

– Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten! 25

– Anonymes elektronisches Bezahlen muss möglich bleiben! 26

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich 27

1. Umlaufbeschluss (vom 8. April 2011) 27

– Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert 27

2. Beschlüsse der Sitzung am 4./5. Mai 2011 in Düsseldorf 28

– Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze 28

– Datenschutzgerechte Smartphone-Nutzung ermöglichen! 30

– Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen 31

3. Beschlüsse der Sitzung am 22./23. November 2011 in Düsseldorf 33

– Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen! 33

– Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen 34

4. Umlaufbeschluss (vom 8. Dezember 2011) 35

– Datenschutz in sozialen Netzwerken 35

III. Europäische Konferenz der Datenschutzbeauftragten 39

Brüssel, 5. April 2011 39

Entschließung über die Notwendigkeit eines umfassenden Rahmens für den Datenschutz 39

IV. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe 42

– Stellungnahme 10/2011 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (WP 181) 42

– Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung („Smart Metering“) (WP 183) 54

– Arbeitsdokument 1/2011 über die EU-Regeln für Verstöße gegen die Datenschutzvorschriften mit Empfehlungen für zukünftige Politikentwicklungen (WP 184) 74

– Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (WP 185) 89

V. Internationale Konferenz der Datenschutzbeauftragten 115

33. Konferenz vom 1.–3. November 2011 in Mexiko-Stadt 115

Entschließung über die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6) 115

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation 117

49. Sitzung am 4./5. April 2011 in Montreal 117

– Datenaufzeichnung in Fahrzeugen (Event Data Recording – EDR): Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller 117

50. Sitzung am 12./13. September 2011 in Berlin 124

– Privacy by Design und Smart Metering: Minimierung personenbezogener Informationen zur Wahrung der Privatsphäre 124

– Datenschutz und elektronisches Micropayment im Internet 134

B. Dokumente zur Informationsfreiheit 137

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) 137

1. Entschließungen der 22. Konferenz am 23. Mai 2011 in Bremen 137

– Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger! 137

– Informationsfreiheit – Lücken schließen! 138

2. Entschließung der 23. Konferenz am 28. November 2011 in Berlin 139

– Informationsfreiheit ins Grundgesetz und in die Landesverfassungen 139

II. Live-Übertragung der Sitzungen der Bezirksverordnetenversammlung (BVV) via Internet 140

Vorwort

Die Datenschutzbehörden in Deutschland haben sich 2011 in gemeinsamen Entschließungen vor allem zu drei Schwerpunktthemen geäußert: Krankenhausinformationssysteme, Cloud Computing und soziale Netzwerke. Daneben sind Stellungnahmen zu einer Vielzahl anderer Themen entstanden, die kaum weniger wichtig sind. Durch alle diese Papiere zieht sich die Kernaussage, dass Datenschutz keine technische Entwicklung verhindert, sondern sich dafür einsetzt, dass von vornherein bestimmte Voraussetzungen zur Gewährleistung der informationellen Selbstbestimmung eingehalten werden. Dafür hat sich in der internationalen Diskussion der Begriff *privacy by default* (datenschutzgerechte Grundeinstellung) eingebürgert.

Auf europäischer Ebene enthalten die Arbeitspapiere der sog. Art. 29-Gruppe der Datenschutzbehörden seit jeher wichtige Orientierungshilfen. An dieser Stelle können nur ausgewählte Papiere abgedruckt werden, die für Deutschland und Berlin praktisch bedeutsam sind. Allgemein gilt aber schon seit geraumer Zeit, dass auf der europäischen Ebene wesentliche Weichen für den Datenschutz vor Ort gestellt werden.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin-Group) hat erneut zukunftsträchtige Themen (Datenaufzeichnung in Fahrzeugen, elektronische Zahlverfahren und intelligente Stromzähler) behandelt und hierzu Empfehlungen abgegeben.

Der Band wird abgeschlossen durch die Entschließungen der deutschen Informationsfreiheitsbeauftragten und eine rechtliche Einordnung der Online-Berichterstattung (Livestreaming) über Beratungen in Berliner Bezirksverordnetenversammlungen, die auch für das Abgeordnetenhaus von Bedeutung sein kann.

Diese Dokumentensammlung kann auch über unsere Webseite abgerufen werden.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 81. Konferenz am 16./17. März 2011 in Würzburg

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Be-

ratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) – eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

   – mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

– die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/ DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis

  – ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,

  – sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,

  – sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tat-

sächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere

  – zu verbieten, die z.B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.

  – für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

  – zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,

  – zur privaten Nutzung von Telekommunikationsdiensten,

  – zum Thema Whistleblowing,

  – zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,

  – zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,

  – zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[1] – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen

[1] Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

2. Entschließung zwischen der 81. und 82. Konferenz (vom 27. Juli 2011)

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbin-

dungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100 g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100 a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismä-

ßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

3. Entschließungen der 82. Konferenz am 28./29. September 2011 in München

Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öf-

fentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es

gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerin-

nen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,

2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,

3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,

4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und

5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von

Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.

- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.

- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.

- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

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

1. Umlaufbeschluss (vom 8. April 2011)

Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst *nach* der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits *vor* der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.

- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.

- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

2. Beschlüsse der Sitzung am 4./5. Mai 2011 in Düsseldorf

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) – eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

   – mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

   – die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“.

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

– **Transparenz bezüglich der Preisgabe personenbezogener Daten:**
In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

– **Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:**
Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

– **Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:**
Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

– **Anonyme und pseudonyme Nutzungsmöglichkeiten:**
Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport).

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

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 Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu

begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

3. Beschlüsse der Sitzung am 22./23. November 2011 in Düsseldorf

Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen

Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards" erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment") zu erhalten[1].

Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten" (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Daten-screenings umzugehen ist (Treffermanagement). Das

[1] vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!"

Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt. Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25 c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.

- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.

- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

4. Umlaufbeschluss (vom 8. Dezember 2011)

Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerken-

nung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen. Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozia-

len Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugins erhebt. Wenn sie die über ein Plugins mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

III. Europäische Konferenz der Datenschutzbeauftragten

Brüssel, 5. April 2011

Entschließung über die Notwendigkeit eines umfassenden Rahmens für den Datenschutz

Die europäischen Datenschutzbehörden hatten bereits früher auf ihrer Frühlingskonferenz in Edinburgh 2009 eine Erklärung[1] abgegeben, in der sie ihre Absicht bekundeten, sich an der Debatte über die Notwendigkeit hoher Standards für den Datenschutz in allen Lebensbereichen – darunter sich entwickelnde Technologien, Online-Welt und Strafverfolgung – aktiv zu beteiligen und diese Standards zu fördern.

Die in der Erklärung zum Ausdruck gebrachte Bereitschaft, eine führende Rolle zu übernehmen, wurde auf der Frühlingskonferenz 2010 in Prag bekräftigt[2]. Insbesondere beharrten die Datenschutzbeauftragten darauf, dass in einer globalen Umwelt für eine wirksame und kohärente Umsetzung der Grundrechte gesorgt werden muss.

Von der Brüsseler Frühlingskonferenz wird der Umstand, dass die Europäische Kommission jetzt mit ihrer Mitteilung 2010 (609) vom 4. November 2010 einen ersten konkreten Schritt hin zu einem Gesamtkonzept für den Datenschutz in der Europäischen Union getan hat, begrüßt und nachdrücklich unterstützt.

Vor dem Hintergrund, dass die Kommission im Laufe des Jahres 2011 einen Vorschlag für einen neuen rechtlichen Rahmen zu unterbreiten beabsichtigt,

– erinnert die Konferenz an die wichtigsten Herausforderungen, die in diesem Rahmen zu meistern sind, darunter

1 *Declaration on leadership and the future of data protection in Europe* (Erklärung zur führenden Rolle und Zukunft des Datenschutzes in Europa), verabschiedet von der Konferenz der europäischen Datenschutzbeauftragten am 23./24. April 2009.

2 *Resolution on future development of data protection and privacy* (Entschließung zur künftigen Entwicklung von Datenschutz und Privatsphäre), verabschiedet von der Konferenz der europäischen Datenschutzbeauftragten am 30. April 2010 in Prag.

- die Konsequenzen der Globalisierung und des grenzüberschreitenden Verkehrs personenbezogener Daten;

- die technologische Entwicklung insbesondere in der Online-Welt;

- die Bedeutung eines wirksamen Schutzes in den Bereichen Polizei und Justiz, auch angesichts der Tendenz, personenbezogene Daten des privaten Sektors in systematischer Weise für Strafverfolgungszwecke wiederzuverwenden.

– betont, dass Artikel 8 Absatz 1 der Charta der Grundrechte und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union ohne Ansehen der Person oder der Verhältnisse Folgendes bestätigen: „*Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten*“.

– stellt allgemeiner fest, dass das neue rechtliche Umfeld des Vertrags von Lissabon und die Charta den Datenschutz ausdrücklich als Grundrecht anerkennen und dieses Recht verbindlich machen und dass der Vertrag von Lissabon die Säulenstruktur abschafft, die Ursache für die Zersplitterung des Datenschutzrahmens auf EU-Ebene war.

– begrüßt den Umstand, dass die Kommission für den neuen Rahmen ein „Gesamtkonzept“ unter Einschluss der Strafverfolgung vorsieht.

– erkennt an, dass zwar für bestimmte Bereiche – darunter die Strafverfolgung, wie in Erklärung 21 im Anhang des Vertrags dargelegt, und andere besondere Bereiche, wie dies bei der Datenschutzrichtlinie für elektronische Kommunikation bereits der Fall war – spezifische ergänzende Vorschriften erforderlich sein könnten, beharrt aber darauf, dass solche bereichsspezifischen ergänzenden Vorschriften das Schutzniveau unter keinen Umständen senken und nur rechtmäßige Einschränkungen zulassen dürfen, die im Einklang mit den allgemeinen Grundsätzen des Datenschutzes stehen.

Die Konferenz beharrt darauf, dass ein umfassendes und kohärentes Konzept benötigt wird, das nicht nur den EU-Rahmen, sondern auch das internationale Umfeld und die Notwendigkeit globaler Standards für den Schutz personenbezogener Daten berücksichtigt. Sie hat deshalb besonderes Interesse:

– an den Arbeiten, die derzeit beim Europarat und bei der OECD geleistet werden, die beide in wertvollen Initiativen ihren derzeitigen Rahmen überprüfen und ermitteln, wo Modernisierungsbedarf besteht.

– an der Initiative des Europarats zur Ermutigung von Nichtparteien des Übereinkommens Nr. 108 und seines Zusatzprotokolls – ob sie nun Mitglied des Rates sind oder nicht –, diesen Instrumenten beizutreten.

– an anderen Initiativen zur Entwicklung internationaler Standards[3], die weltweit anerkannt werden sollen.

Die Konferenz ist der Meinung, dass die Bemühungen um die Modernisierung und Stärkung der verschiedenen rechtlichen Rahmen zu Synergien führen sollten, und ruft die wichtigsten Interessenträger dieser Projekte dazu auf, ihre Aktivitäten zu koordinieren.

Die europäischen Datenschutzbeauftragten sind der Ansicht, dass all diese Entwicklungen enorme Chancen für eine wirkliche Verbesserung des Datenschutzrahmens bieten, um einen wirksamen Schutz für alle Betroffenen unter allen Umständen nicht nur jetzt, sondern auch in einer ferneren Zukunft, zu gewährleisten.

Es ist an der Zeit, ambitioniert zu sein und die Kräfte für einen wirksameren Datenschutz zu bündeln. Die Datenschutzbeauftragten sind bereit, alles ihnen Mögliche dazu beizutragen, dass ein so starkes und umfassendes Datenschutzsystem Wirklichkeit wird.

[3] Siehe insbesondere:
– *International Standards on the Protection of Personal data and privacy* (Internationale Standards zum Schutz von personenbezogenen Daten und Privatsphäre), verabschiedet am 5. November 2009 in Madrid auf der 31. Internationalen Konferenz der Datenschutzbeauftragten;
– *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data* (Entschließung für einen Aufruf zur Veranstaltung einer Regierungskonferenz, auf der ein verbindliches internationales Instrument zur Privatsphäre und zum Schutz personenbezogener Daten entwickelt werden soll), verabschiedet am 29. Oktober 2010 in Jerusalem auf der 32. Internationalen Konferenz der Datenschutzbeauftragten.

IV. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Stellungnahme 10/2011 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (WP 181)

Angenommen am 5. April 2011

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

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

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

hat folgende Stellungnahme angenommen:

1. Einleitung

Am 2. Februar 2011 veröffentlichte die Europäische Kommission ihren Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Die Datenschutzgruppe hat auch zu dem vom der Kommission am 6. November 2007 unterbreiteten vorangegangenen PNR-Vorschlag (Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken) eine Stellungnahme vorgelegt.[1] Die Datenschutzgruppe hat sich außerdem

[1] WP 145 – gemeinsame Stellungnahme mit der Arbeitsgruppe Polizei und Justiz.

bereits in mehreren Stellungnahmen ausführlich zu den verschiedenen zwischen der EU und Drittländern bestehenden PNR-Abkommen sowie zu dem in der Mitteilung der Kommission vom 21. September 2010 dargelegten Konzept der Kommission geäußert.[2] Darüber hinaus hat die Datenschutzgruppe in verschiedenen Schreiben an die Kommissionsmitglieder Barrot und Malmström, Generaldirektor Faull, und den LIBE-Ausschuss des Europäischen Parlaments ihre Bedenken in Bezug auf PNR-Fragen mehrfach wiederholt.

Diese Stellungnahme richtet sich an die an der Erörterung und Erarbeitung des jüngsten Vorschlags Beteiligten, insbesondere die Kommission, die Arbeitsgruppe GENVAL des Rates und das Europäische Parlament.

2. Notwendigkeit und Verhältnismäßigkeit

Dem Vorschlag von 2011 ist eine Folgenabschätzung beigefügt, in der die Beweggründe für den Vorschlag und sein Inhalt näher erläutert werden. Die Datenschutzgruppe ist der Auffassung, dass der Kampf gegen Terrorismus und organisierte Kriminalität notwendig und legitim ist und personenbezogene Daten, insbesondere bestimmte Fluggastdaten, zur Abschätzung der Risiken sowie Verhütung und Bekämpfung von Terrorismus und organisierter Kriminalität von Wert sein können. Allerdings muss im Falle eines EU-PNR-Systems die Einschränkung von Grundrechten und -freiheiten sorgfältig begründet und ihre Notwendigkeit eindeutig nachgewiesen werden, um ein ausgewogenes Verhältnis zwischen dem gebotenen Schutz der öffentlichen Sicherheit und der Einschränkung der Privatsphäre wahren zu können.

Die Datenschutzgruppe hat die Notwendigkeit und Verhältnismäßigkeit von PNR-Systemen stets in Frage gestellt und bezweifelt sie auch in Bezug auf den Vorschlag von 2011. Wir begrüßen zwar die in der Folgenabschätzung enthaltenen zusätzlichen Einzelheiten, meinen aber dennoch, dass sie keine angemessene Beurteilung der Verwendung von PNR-Daten darstellt und die Notwendigkeit der vorgeschlagenen Maßnahmen nicht belegt. Aus dem Vorschlag sollte eindeutig hervorgehen, ob er auf die Bekämpfung schwerer (grenzüberschreitender) Kriminalität, zu der auch Terrorismus zählt, oder nur auf die Bekämpfung von Terrorismus und terroristischen Straftaten abzielt.

In Kapitel 3.2 der Folgenabschätzung „Respect of fundamental rights" (*Achtung der Grundrechte*) heißt es lediglich, dass die Checkliste für Grundrechte verwendet wurde, es fehlen jedoch weitere Informationen über diese Einschätzung zur

[2] Stellungnahmen WP 103 (Kanada); WP 138 (USA); WP 151 (USA – Information von Fluggästen) und WP 178 (sektorübergreifendes Konzept der Kommission).

Begründung der daraus gezogenen Schlüsse. Darüber hinaus stützt sich dieses Kapitel in Bezug auf Eingriffe in die Privatsphäre gemäß Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union auf einen Zirkelschluss. Die rechtliche Voraussetzung für einen Eingriff in diese Rechte ist, dass er „für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer" sowie „in einer demokratischen Gesellschaft notwendig" ist und nur „unter Wahrung des Grundsatzes der Verhältnismäßigkeit" vorgenommen werden darf. Die Tatsache, dass der Vorschlag auf die Verhütung von Terrorismus und schwerer Kriminalität abzielt, bedeutet nicht unbedingt, dass er diese Anforderungen erfüllt. Der Nachweis der Notwendigkeit und Verhältnismäßigkeit steht jedenfalls noch aus. In dem von der Kommission selbst gegebenen Überblick über Informationsmanagementsysteme[3] heißt es:

> „Notwendigkeit
> Die Beeinträchtigung des Rechtes einer Person auf ihre Privatsphäre durch eine staatliche Behörde kann im Interesse der nationalen oder öffentlichen Sicherheit oder der Kriminalitätsvorbeugung notwendig sein. Der Europäische Gerichtshof für Menschenrechte hat drei Bedingungen herausgearbeitet, unter denen solche Beeinträchtigungen gerechtfertigt sein können: Der Eingriff muss rechtmäßig sein, mit ihm muss ein legitimes Ziel verfolgt werden, und er muss in einer demokratischen Gesellschaft notwendig sein. Ein Eingriff in das Recht auf Privatsphäre gilt dann als notwendig, wenn er einem zwingenden gesellschaftlichen Erfordernis entspricht, wenn er im Vergleich zu dem verfolgten Ziel verhältnismäßig ist und wenn die staatlichen Behörde den Eingriff ‚ausreichend begründet'. Bei allen künftigen Vorschlägen in diesem Bereich wird die Kommission die erwarteten Auswirkungen auf die Rechte des Einzelnen auf Privatsphäre und auf den Schutz der personenbezogenen Daten abschätzen und darlegen, warum die Maßnahme notwendig und die vorgeschlagene Lösung im Vergleich zum legitimen Ziel der Aufrechterhaltung der inneren Sicherheit in der Europäischen Union, zur Verhütung von Straftaten und für die Migrationssteuerung verhältnismäßig ist."

Die Datenschutzgruppe ist nicht der Auffassung, dass die Kommission die vorstehenden Zusagen im Hinblick auf den EU-PNR-Vorschlag erfüllt hat. Verschiedene weitere Aspekte der Argumentation zu Notwendigkeit und Verhältnismäßigkeit werden nachstehend erörtert.

[3] Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht, KOM(2010)385 endgültig.

2.1. Mehr Sicherheit

Laut dem Vorschlag und der Folgenabschätzung würde ein EU-PNR-System die Sicherheit gewährleisten und Sicherheitslücken aufgrund der Abschaffung der Kontrollen an den Binnengrenzen im Rahmen des Schengener Übereinkommens schließen. Dies wäre bei angemessener Begründung ein legitimes Ziel, allerdings liegen der Datenschutzgruppe noch keine ausreichenden Nachweise dafür vor, dass durch die Verarbeitung von PNR-Daten in allen Mitgliedstaaten Sicherheitslücken vermieden werden, die durch die Verarbeitung dieser Daten in nur einigen Mitgliedstaaten entstehen.

Es gibt bereits auf EU-Ebene Systeme und Instrumente als Ausgleich für die Abschaffung der Grenzkontrollen im Schengen-Raum, die sich auf den sogenannten Schengen-Besitzstand stützen. Wenn also noch Sicherheitslücken bestehen, dann sollte der erste Schritt eine Untersuchung des reibungslosen Funktionierens der bestehenden Systeme sein.

2.2. Bestehende Systeme, Instrumente und Zusammenarbeit

In dem Überblick der Kommission über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht wird weder die Wirksamkeit der verschiedenen bestehenden Systeme beurteilt noch geprüft, ob sie in ihrer Gesamtheit geeignete Instrumente zur Bekämpfung von Terrorismus und organisierter Kriminalität darstellen und wo – falls dem nicht so ist – mögliche Sicherheitslücken bestehen. Die Datenschutzgruppe ist der Auffassung, dass eine solche Beurteilung erforderlich ist, bevor weitere, ähnliche Maßnahmen wie ein EU-PNR-System eingeführt werden. Der PNR-Vorschlag führt zu einander überschneidenden Verpflichtungen für Fluggesellschaften, zur Sammlung von bereits in anderen Systemen verfügbaren Daten und birgt ernsthaft die Gefahr einer schleichenden Zweckentfremdung (function creep). So verpflichtet die API-Richtlinie etwa Fluggesellschaften, Angaben über die beförderten Personen im Voraus zu übermitteln, wobei die Daten nicht nur bei Grenzkontrollen, sondern auch für die Strafverfolgung verwendet werden dürfen. Obwohl die Datenschutzgruppe dieses Thema mehrfach gegenüber der Kommission angesprochen hat, liegt ihr noch keine sachgerechte Bewertung der Wirksamkeit der API-Richtlinie und ihrer nationalen Umsetzungsmaßnahmen vor und sie bezweifelt, dass die API-Richtlinie nach der Einführung eines EU-weiten PNR-Systems überhaupt noch notwendig ist.

Die Datenschutzgruppe fragt sich, ob nicht alle in der EU bereits bestehenden Formen der polizeilichen und justiziellen Zusammenarbeit zur Verhütung und Verfolgung von Straftaten, die auch die Bekämpfung von Terrorismus und schwe-

rer Kriminalität einschließen, für den vom PNR-Vorschlag vorgesehenen Zweck ausreichen. Dies wird in der Folgenabschätzung nicht untersucht.

Die Datenschutzgruppe erkennt an, dass einige Mitgliedstaaten, die nicht dem Schengen-Raum angehören, einige der bestehenden Instrumente und Systeme nicht nutzen können, was sich möglicherweise auf die Prüfung der Notwendigkeit für diese Staaten auswirkt. Allerdings können diese Mitgliedstaaten die API-Richtlinie anwenden und tun dies auch. Deshalb sollte geprüft werden, ob nicht durch eine bessere Nutzung bestehender Systeme und eine verstärkte Zusammenarbeit zwischen diesen und anderen Mitgliedstaaten die benötigten Informationen für die jeweiligen Zwecke beschafft werden können. Dass PNR-Daten, wie in der Folgenabschätzung erwähnt wird, zur polizeilichen Erkenntnisgewinnung verwendet werden sollen, erhöht ebenfalls die Anforderungen an die Datenschutzgarantien.

2.3. Verhältnismäßigkeit

Nach dem Vorschlag sollen personenbezogene Daten über alle Fluggäste, die in die EU einreisen und aus der EU ausreisen, unabhängig davon, ob sie verdächtig sind, in großer Menge gesammelt werden. Die Sammlung und Verarbeitung von PNR-Daten zur Bekämpfung von Terrorismus und schwerer Kriminalität darf keine massenhafte Verfolgungund Überwachung aller Reisenden ermöglichen. Nach Auffassung der Datenschutzgruppe ist die Sammlung und Speicherung sämtlicher Daten über alle Fluggäste für alle Flüge unverhältnismäßig und steht daher nicht im Einklang mit Artikel 8 der Charta der Grundrechte. Wie bereits ausgeführt, enthält die Folgenabschätzung diesbezüglich keine überzeugenden Anhaltspunkte. Vorschläge auf EU-Ebene sollten spezifisch und gezielt an ein bestimmtes Problem herangehen und in diesem Zusammenhang sollte sich jeder Vorschlag schwerpunktmäßig mit den durch Terrorismus und schwere Kriminalität bedingten Risiken befassen.

Die Datenschutzgruppe hegt ernste Zweifel an der Verhältnismäßigkeit des systematischen Abgleichs aller Fluggäste mit bestimmten im Voraus festgelegten Kriterien und nicht näher bezeichneten „relevanten … Datenbanken“. Es ist nicht klar, wie diese im Voraus festgelegten Kriterien und relevanten Datenbanken bestimmt werden sollen, ob PNR-Daten zur Erstellung oder Aktualisierung der Kriterien verwendet und in welchem Umfang alle Treffer zusätzlich untersucht werden. Die Datenschutzgruppe möchte auch daran erinnern, dass in einigen Mitgliedstaaten ähnliche Methoden der Polizeiarbeit nur dann verfassungskonform sind und von der Polizei eingesetzt werden dürfen, wenn eine gerichtliche Genehmigung dafür vorliegt und bestimmte Umstände, wie etwa eine konkrete Bedrohung, gegeben sind. Das vorgeschlagenen PNR-System würde diese Ausnah-

mefällen vorbehaltene Methode zu einem gewöhnlichen Instrument der Polizeiarbeit machen.

Maßnahmen, die den Schutz der Rechte und Freiheiten von Reisenden nicht gewährleisten können, sind nur dann verhältnismäßig, wenn sie befristet für eine konkrete Bedrohung eingeführt werden, was für diesen Vorschlag nicht zutrifft. Der Eingriff in die Privatsphäre von Reisenden muss in einem angemessenen Verhältnis zu dem dadurch erzielten Nutzen für die Bekämpfung von Terrorismus und schwerer Kriminalität stehen. Der Datenschutzgruppe sind bislang keine Statistiken über das Verhältnis zwischen der Zahl unschuldiger Reisender, deren PNR-Daten erfasst wurden, und der Zahl der mithilfe dieser PNR-Daten erzielten Erfolge der Strafverfolgung bekannt.

Insgesamt ist die Datenschutzgruppe nach wie vor der Auffassung, dass die Notwendigkeit des Systems nicht erwiesen ist und die vorgeschlagenen Maßnahmen nicht dem Grundsatz der Verhältnismäßigkeit entsprechen. Sie hält es aber dennoch für konstruktiv, im Folgenden auch zu anderen Aspekten der vorgeschlagenen Richtlinie Stellung zu nehmen.

3. Zwecke

In der vorgeschlagenen Richtlinie sind zwei allgemeine Zwecke der Verarbeitung mit vier spezifischen Aktivitäten angegeben. PNR-Daten können nur zu folgenden Zwecken verarbeitet werden:

– Verhütung, Aufdeckung, Aufklärung und strafrechtliche Verfolgung von terroristischen Straftaten und schwerer Kriminalität durch Überprüfung von Fluggästen vor ihrer Ankunft bzw. ihrem Abflug durch Abgleich mit relevanten Datenbanken (Zweck 1, Aktivität 1) und durch Beantwortung von Anfragen zuständiger Behörden in besonderen Fällen (Zweck 1, Aktivität 2);

– Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer grenzüberschreitender Kriminalität durch Überprüfung von Fluggästen vor ihrer Ankunft bzw. ihrem Abflug anhand bestimmter Kriterien (Zweck 2, Aktivität 3) und durch Auswertung von PNR-Daten zwecks Aktualisierung oder Aufstellung neuer Kriterien (Zweck 2, Aktivität 4).

Es ist nicht klar, was diese Zwecke in der Praxis bedeuten. Mit Aktivität 1 (Zweck 1) scheint ein Abgleich mit Beobachtungslisten, der SIS-Datenbank oder anderen Datenbanken auf EU-Ebene und nationaler Ebene gemeint zu sein. Mit Aktivität 2 (Zweck 1) scheint der individuelle Austausch von Informationen aufgrund einer konkreten Anfrage gemeint zu sein. Mit Aktivität 3 (Zweck 2) scheint

ein Abgleich von PNR-Daten mit Profilen für bestimmte Straftaten und mit Aktivität 4 (Zweck 2) die Verwendung von PNR-Daten zur Entwicklung dieser Profile gemeint zu sein.

Ein Grundprinzip des Datenschutzes besteht darin, dass die Ziele und Aktivitäten klar definiert sein müssen. Die „relevanten … Datenbanken" sollten ebenfalls genauer definiert werden, möglicherweise indem sie in die Liste der zuständigen Behörden aufgenommen werden, die jeder Mitgliedstaat an die Kommission zu übermitteln hätte. In jedem Fall sollten die verwendeten Datenbanken diejenigen sein, die für dieselben Zwecke, nämlich die Verhütung, Aufdeckung, Aufklärung und strafrechtliche Verfolgung von terroristischen Straftaten und schwerer Kriminalität, eingerichtet worden sind. Ferner müssen in den Umsetzungsmaßnahmen die Nutzungsbeschränkungen dieser Datenbanken eindeutig festgelegt sein. Die Datenschutzgruppe erinnert außerdem daran, wie wichtig es ist, dass alle von den Mitgliedstaaten zur Auswertung von Daten verwendeten Prüfkriterien spezifisch, notwendig und gerechtfertigt sind und regelmäßig überprüft werden.

3.1. Begriffsbestimmungen

In dem Vorschlag werden „terroristische Straftaten" als Straftaten im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates definiert. „Schwere Kriminalität" und „schwere grenzüberschreitende Kriminalität" werden als die in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates aufgeführten strafbaren Handlungen definiert. Die Datenschutzgruppe unterstreicht, wie wichtig konkrete Definitionen in diesem Bereich sind. Allerdings ist die Definition von schwerer Kriminalität sehr weit gefasst und wir bezweifeln die Notwendigkeit und Verhältnismäßigkeit der Verwendung von PNR-Daten bei einigen dieser Straftaten.

In diesem Zusammenhang können die Mitgliedstaaten nach Erwägungsgrund 12 des Vorschlags nicht ganz so schwerwiegende Straftaten ausschließen, bei denen eine Verarbeitung von PNR-Daten nicht verhältnismäßig wäre, wobei die Wahl jedoch den einzelnen Mitgliedstaaten überlassen bleibt. Dies wird wahrscheinlich dazu führen, dass Straftaten in manchen Mitgliedstaaten einbezogen werden, in anderen hingegen nicht. Es ist nicht klar, wer über die Verhältnismäßigkeit entscheidet und ob diese Entscheidung der Kommission mitzuteilen ist, die beispielsweise für eine einheitliche und korrekte Anwendung des Grundsatzes der Verhältnismäßigkeit sorgen könnte.

Die Bedenken der Datenschutzgruppe im Hinblick auf die möglicherweise zu breit gefasste Definition schwerer Kriminalität betreffen auch die Bestimmungen der vorgeschlagenen Richtlinie zur Weitergabe von Daten an andere Behörden innerhalb und außerhalb der EU.

4. Speicherung

Die vorgeschlagenen Speicherungsfristen liegen deutlich unter denen des vorangegangenen Vorschlags und der verschiedenen PNR-Abkommen auf EU-Ebene. Die Datenschutzgruppe hält jedoch den Vorschlag, Daten, selbst wenn sie unkenntlich gemacht wurden, fünf Jahre lang zu speichern, nach wie vor für unverhältnismäßig. An PNR-Systemen wird schon immer bemängelt, dass sämtliche Daten über alle Reisenden gleich lange gespeichert werden und dass diese Speicherungsfrist an sich unverhältnismäßig ist. Der Datenschutzgruppe liegt bislang keine ausreichende Begründung dafür vor, dass die Daten über alle Reisenden gespeichert werden müssen und dass die Speicherungsfrist fünf Jahre betragen muss.

4.1. Unkenntlichmachung von Daten

Wenngleich der Vorschlag vorsieht, dass die Daten nach 30 Tagen unkenntlich gemacht werden und grundsätzlich nur bestimmten, mit der Erstellung von Profilen und Mustern zum Reiseverhalten befassten Mitarbeitern der PNR-Zentralstelle zugänglich sind, wäre dennoch der vollständige Zugriff auf alle Daten während der gesamten Speicherungsfrist möglich. Selbst wenn mit der Unkenntlichmachung von Daten versucht wird, wichtigen Grundsätzen des Datenschutzes (Datenminimierung und Zugriffskontrolle) Rechnung zu tragen, bezweifelt die Datenschutzgruppe nach wie vor, dass sämtliche Daten über alle Reisenden benötigt werden, und ist der Ansicht, dass die Daten von nicht verdächtigten Reisenden gelöscht werden sollten.

Sollte der Gesetzgeber beschließen, die Daten für einen begrenzten Zeitraum zu speichern, dann sollten die Daten so geschützt sein, dass die zur Identifizierung geeigneten Angaben nicht erkennbar sind. Die betreffenden Schutzmaßnahmen sollten spätestens bei der Ankunft des Fluges erfolgen. Für den Zugriff auf die geschützten Daten zwecks Abruf der zur Identifizierung notwendigen Angaben für konkrete strafrechtliche Ermittlungen sollte in jedem Fall ein richterlicher Beschluss erforderlich sein.

Die Datenschutzgruppe möchte außerdem besonders die Notwendigkeit einer exakten, eindeutigen und unmissverständlichen Sprachregelung betonen. In dem Vorschlag ist sowohl von Unkenntlichmachung als auch von Anonymisierung die Rede. Die beiden Begriffe haben nicht dieselbe Bedeutung, wobei klar ist, dass Unkenntlichmachung und nicht Anonymisierung gemeint ist, da die zur Identifizierung einer Person erforderlichen Daten nach wie vor leicht abgerufen werden können. Der Vorschlag darf weder absichtlich noch aus anderen Gründen missverständlich oder irreführend sein und keine unhaltbaren Versprechungen machen.

5. Individuelle Datenschutzrechte

Der Vorschlag enthält Bestimmungen, die speziell den Datenschutz betreffen. Die Datenschutzgruppe hält es für notwendig, dass jeder auf EU-Ebene unterbreitete Vorschlag, der sich auf die Rechte und Freiheiten von Personen auswirkt, Bestimmungen über die Rechte des Einzelnen auf Auskunft, Berichtigung, Schadenersatz und Rechtsbehelfe enthält. Allerdings entsprechen die in diesem Vorschlag verankerte Rechten nicht denen der Richtlinie 95/46/EG, sondern denen des Rahmenbeschlusses 2008/977/JI und sind somit stärker eingeschränkt. Es ist nicht klar, ob die Rechte nur für Daten, die an eine andere Behörde übermittelt werden, oder auch für die von der nationalen Behörde gespeicherten Daten gelten. In einigen Mitgliedstaaten, die derzeit PNR-Daten nutzen, stehen Personen Rechte auf Auskunft und Berichtigung sowie Rechtsbehelfe nach den nationalen Umsetzungsmaßnahmen zur Richtlinie 95/46/EG zu. Diese Rechte würden im Falle einer Inkraftsetzung der vorgeschlagenen PNR-Richtlinie eingeschränkt.

Ferner besteht die Gefahr der Diskriminierung aufgrund der Profilerstellung, da dieses System die Fluggäste als Gruppe ins Visier nimmt. Die Fluggäste werden nicht über die Kriterien unterrichtet, anhand derer sie überprüft werden, was die von der Profilerstellung unmittelbar Betroffenen in der Ausübung ihrer Rechte einschränkt.

Die Datenschutzgruppe erinnert daran, wie wichtig es ist, dass auf EU-Ebene unterbreitete Vorschläge, die sich auf die Rechte und Freiheiten von Personen auswirken, geeignete Datenschutzmaßnahmen und -garantien wie etwa Vorschriften zur Vertraulichkeit und Sicherheit der Verarbeitung, Verpflichtungen zur Unterrichtung von Personen, das Verbot der Übermittlung von Daten an private Nutzer sowie Bestimmungen enthalten, wonach Entscheidungen nicht allein aufgrund einer automatisierten Verarbeitung getroffen werden dürfen. Die Datenschutzgruppe betont außerdem die Bedeutung der Einbeziehung von nationalen Aufsichtsbehörden, die auf Ebene der Mitgliedstaaten für die Umsetzung von EU-Rechtsvorschriften zuständig sind.

Sensible Daten sollen dem Vorschlag zufolge von der PNR-Zentralstelle herausgefiltert und gelöscht werden. In ihren Stellungnahmen zu den verschiedenen PNR-Abkommen der EU mit Drittländern hat die Datenschutzgruppe stets das Verbot der Verarbeitung sensibler Daten in diesem Zusammenhang unterstützt und bekräftigt mit Nachdruck ihre seit langem vertretene Ansicht, dass die Filterung durch die Fluggesellschaften erfolgen sollte, bevor die Daten mittels der Push-Methode an die empfangende Behörde übermittelt werden.

Die Datenschutzgruppe unterstreicht, wie wichtig es ist zu gewährleisten, dass auf EU-Ebene unterbreitete Vorschläge, die sich auf die Rechte und Freiheiten

von Personen auswirken, Überwachungs- und Überprüfungsmaßnahmen wie etwa die Protokollierung der Verarbeitung und von Datenanfragen zur Überprüfung der Rechtmäßigkeit der Verarbeitung, zur Selbstkontrolle und zur Gewährleistung der Unversehrtheit der Daten und der Sicherheit der Datenverarbeitung vorsehen. Ebenso muss aber auch klar sein, wie solche Systeme in der Praxis funktionieren und wie gut die Protokollierung und Dokumentation mit den obengenannten Grundsätzen der Datenminimierung vereinbar ist.

6. Datenelemente

Im Gegensatz zu API-Daten werden PNR-Daten nicht überprüft und sind daher weniger zuverlässig. Die als Anhang zu diesem Vorschlag aufgeführten Datenelemente sind dieselben 19 Elemente wie in den PNR-Abkommen zwischen der EU und den USA bzw. Kanada. Die Datenschutzgruppe bekräftigt ihren Standpunkt, dass kein ausreichender Nachweis dafür vorliegt, welche Felder sich als notwendig erwiesen haben. Daher ist eine solche Liste als unverhältnismäßig zu betrachten. Die Kategorien sind allgemein gehalten und mehrere von ihnen enthalten weitere Datenuntergruppen. Selbst bei einem Verbot der Verarbeitung sensibler personenbezogener Daten, ist in der Liste der Datenelemente das Feld „Allgemeine Hinweise“ vorgesehen, das alle Arten von Informationen wie Menüwünsche, spezielle Serviceanfragen usw. enthalten kann. Der Datenschutzgruppe liegen noch keine ausreichenden Nachweise dafür vor, welche PNR-Datenelemente sich als notwendig erwiesen haben oder erfolgreich für die Strafverfolgung genutzt worden sind. Darüber hinaus sammeln nicht alle Fluggesellschaften PNR-Daten.

7. Zuständige Behörden und Weitergabe von Daten an Dritte

Der Vorschlag sieht vor, dass die Mitgliedstaaten der Kommission innerhalb von zwölf Monaten nach dem Inkrafttreten der Richtlinie die Liste ihrer zuständigen Behörden übermitteln und diese Liste im Amtsblatt veröffentlicht wird. Die Datenschutzgruppe unterstützt der Transparenz dienende Maßnahmen, die eindeutig aufzeigen, wer befugt ist, Daten zu empfangen und zu verarbeiten. Allerdings sind die Rollen (für die Verarbeitung Verantwortliche / Auftragsverarbeiter) der zuständigen Behörden und PNR-Zentralstellen nicht klar.

Die Datenschutzgruppe bekräftigt ihre Bedenken hinsichtlich der weit gefassten Definition von schwerer Kriminalität, insbesondere in Bezug auf die Weitergabe von Daten sowohl innerhalb als auch außerhalb der EU.

8. Überprüfung und Gegenseitigkeit

Dem Vorschlag zufolge soll die Richtlinie innerhalb von vier Jahren nach ihrem Inkrafttreten überprüft werden. Innerhalb von zwei Jahren nach Inkrafttreten der Richtlinie soll im Rahmen einer besonderen Überprüfung die Einbeziehung von Flügen innerhalb der EU in den Anwendungsbereich der Richtlinie untersucht werden. Die Datenschutzgruppe betont, dass bei Überprüfungen von EU-Rechtsvorschriften die Notwendigkeit und Wirksamkeit von Systemen anhand eindeutiger Kriterien beurteilt werden müssen. Sie bekräftigt außerdem die Bedeutung der Einbeziehung der nationalen Datenschutzbehörden in jeden Überprüfungsprozess, zumal andere Rechtsinstrumente auf EU-Ebene wie etwa die PNR-Abkommen der EU mit Drittländern dies vorsehen.

Die Datenschutzgruppe unterstreicht, dass es bei der Erarbeitung von Vorschlägen für EU-Rechtsvorschriften wichtig ist, die Auswirkungen möglicher Gegenseitigkeitsregelungen zu berücksichtigen. Ein europäisches PNR-Modell könnte dazu führen, dass nichtdemokratische Länder oder Länder, die den Schutz von Grundrechten und -freiheiten einschließlich personenbezogener Daten und der Privatsphäre nicht angemessen gewährleisten, im Gegenzug ähnliche Vorschriften erlassen. Es liegt auf der Hand, dass es für den Einzelnen schwerwiegende Folgen haben könnte, falls solche Länder EU-PNR-Daten erhalten.

9. Fazit

Die Datenschutzgruppe ist der Auffassung, dass die Notwendigkeit eines EU-PNR-Systems noch nicht erwiesen ist und die vorgeschlagenen Maßnahmen dem Grundsatz der Verhältnismäßigkeit insbesondere deshalb nicht entsprechen, weil das System die Erfassung und Speicherung sämtlicher Daten über alle Reisenden auf allen Flügen vorsieht. Sie hegt außerdem ernste Zweifel an der Verhältnismäßigkeit eines systematischen Abgleichs aller Fluggäste mit bestimmten im Voraus festgelegten Kriterien.

Die Datenschutzgruppe empfiehlt, zunächst die bestehenden Systeme und Methoden der Zusammenarbeit und ihr Zusammenwirken zu bewerten, um etwaige Sicherheitslücken zu ermitteln. Falls Sicherheitslücken bestehen, sollte dann untersucht werden, wie sie am besten geschlossen werden können, was nicht notwendigerweise mit der Einführung eines völlig neuen Systems verbunden sein muss. Vielmehr könnten die bestehenden Mechanismen weiter genutzt und verbessert werden.

Falls die vorgeschlagene Richtlinie in Kraft tritt, sollte sie geeignete und angemessene Datenschutzmaßnahmen und -garantien enthalten. Die Kommission

sollte außerdem prüfen, ob bestehende Systeme wie die API-Richtlinie aufgehoben werden können, um Maßnahmenüberschneidungen vermeiden.

Die Datenschutzgruppe wird die Entwicklungen weiterhin genau verfolgen und begrüßt jede Gelegenheit, ihre Ansichten gegenüber den verschiedenen an diesem Vorschlag Beteiligten darzulegen und weiterzuentwickeln. Sie wird außerdem weiterhin gegebenenfalls notwendige Stellungnahmen abgeben.

Brüssel, den 5. April 2011

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung („Smart Metering“) (WP 183)

Angenommen am 4. April 2011

Die Gruppe für den Schutz von Personenen bei der Verarbeitung personenbezogener Daten –

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

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

gestützt auf ihre Geschäftsordnung –

hat folgende Stellungnahme angenommen:

Einleitung und Umfang

Die Artikel-29-Datenschutzgruppe verfolgt mit dieser Stellungnahme das Ziel, den rechtlichen Rahmen darzulegen, der auf den Betrieb intelligenter Verbrauchsmessgeräte („Smart Meters“) im Energiesektor zur Anwendung kommt. Diese Stellungnahme soll keinen erschöpfenden Überblick über sämtliche spezifischen Aspekte von Programmen für die intelligente Verbrauchsmessung geben, da dies aufgrund der Uneinheitlichkeit der zu diesem Thema gegenwärtig vertretenen Standpunkte gar nicht möglich wäre. Intelligente Verbrauchsmessgeräte bieten neue Funktionalitäten wie z. B detaillierte Informationen über den Energieverbrauch, die Möglichkeit einer Fernablesung der Verbrauchszähler, die Entwicklung neuer Tarife und Dienstleistungen, die sich nach Energieprofilen richten, sowie die Möglichkeit der Fernabschaltung der Energieversorgung.

Intelligente Stromversorgungsnetze („Smart grids“) bieten noch mehr Entwicklungsspielraum und Möglichkeiten für die Verarbeitung zusätzlicher personenbezogener Daten. Die Arbeitsgruppe möchte zum gegenwärtigen Zeitpunkt ihre Stellungnahme nicht auf die „Smart-Grid“-Funktion ausdehnen, schließt aber nicht aus, dass sie sich eingehender mit intelligenten Stromnetzen befassen wird, sobald sich das Bild weiter konkretisiert hat.

In der EG-Richtlinie über Energieeffizienz und Energiedienstleistungen (2006/32/EG) werden Energieeinsparziele festgelegt, die von den einzelnen Mitgliedstaaten übernommen werden müssen. Um diese Ziele – vorbehaltlich be-

stimmter Ausnahmefälle – zu erreichen, werden die Mitgliedstaaten nach Artikel 13 der Richtlinie verpflichtet, den Verbrauchern Verbrauchsmessgeräte zur Verfügung zu stellen, die ihren Energieverbrauch exakt wiedergeben und Informationen zur tatsächlichen Nutzungszeit liefern. Diese intelligenten Verbrauchsmessgeräte sind Teil der Bestrebungen, die Ziele der Europäischen Union im Hinblick auf den Aufbau einer nachhaltigen Energieversorgung bis zum Jahr 2020 umzusetzen.

Von der Generaldirektion Energie wurde eine Taskforce zu intelligenten Stromversorgungsnetzen („Smart Grids") eingerichtet. Die Sachverständigengruppe 2, die Teil dieser Taskforce ist, ersuchte um Unterstützung durch die Artikel-29-Datenschutzgruppe bei der eingehenderen Analyse der Maßnahmen, die auf nationaler Ebene durchgeführt werden. Hierfür wurde im Jahr 2010 ein Fragebogen an die Datenschutzbehörden versandt. In sechs Fragen wurden Meinungen zur Entwicklung intelligenter Stromversorgungsnetze abgefragt (diese werden großenteils auch in der vorliegenden Stellungnahme angesprochen). In weiteren zwölf Fragen wurden Informationen zum gegenwärtigen Stand der Einführung intelligenter Verbrauchsmesssysteme in den Mitgliedstaaten angefragt. Die Mitgliedstaaten, die die sechs Fragen beantworteten, erklärten in ergänzenden Anmerkungen, dass das Sicherheitsniveau demjenigen anderer breit angelegter Systeme wie Internetbanking vergleichbar sein müsse. Aus den Antworten auf die weiteren zwölf Fragen wurde deutlich, dass die Umsetzung von Programmen, mit denen intelligente Verbrauchsmessungen bei Haushaltskunden der Energieversorger eingeführt werden, in vielen EU-Mitgliedstaaten zu den relevanten und drängenden Problemen gehört. Der intelligenten Verbrauchsmessung kommt insofern besondere Bedeutung zu, als sie das Leben fast aller Bürger beeinflussen kann, da jeder Bürger Strom und Gas bezieht. Ihre Reichweite ist also außerordentlich beträchtlich und beschränkt sich nicht auf Technologiebegeisterte. Das Ziel lautet, dass bis 2020 insgesamt 80 % der Kunden erfasst sein werden[1].

Intelligente Verbrauchsmessgeräte ermöglichen die Erstellung, Übermittlung und Auswertung von Daten über die Verbraucher, und zwar in wesentlich größerem Umfang, als es mit „herkömmlichen" Messgeräten ohne „intelligente" Zusatzfunktionen möglich ist. Demzufolge können auch der Netzbetreiber (auch als Verteilungsnetzbetreiber (VNB) bezeichnet), die Energieversorger und andere Akteure detaillierte Informationen über den Energieverbrauch und die Verbrauchsmuster erstellen und anhand der Nutzungsprofile Entscheidungen über individuelle Energienutzer treffen. Zwar können derartige Entscheidungen häufig in Form von Energieeinsparungen durchaus Vorteile für die Verbraucher mit sich bringen, doch zeichnet sich auch ab, dass durch die in den Privathaus-

[1] Smart meters: controlling your energy bill? *Euractiv.com*, [online] Verfügbar unter: http://www.euractiv.com/en/energy-efficiency/smart-meters-controlling-your-energy-billlinksdossier-257199 [Verfügbar ab 25. März 2011]
Dieser Artikel bezieht sich auf die Meilensteine im Dritten Energiepaket, das im Juni 2009 angenommen wurde.

halten installierten Geräte die Möglichkeit von Eingriffen in die Privatsphäre der Bürger besteht. Außerdem kommt es dadurch zu einer grundsätzlichen Verschiebung in den Beziehungen zu den Energieversorgern, da die Verbraucher in der Vergangenheit lediglich die Lieferanten für die von diesen bezogenen Strom-und Gaslieferungen bezahlt haben. Mit dem Aufkommen intelligenter Verbrauchsmessgeräte gestaltet sich dieser Prozess insofern komplexer, als die betroffenen Personen damit den Versorgern Einblicke in ihre persönlichen Gewohnheiten geben.

Zu den vielfach diskutierten Vorteilen intelligenter Formen des Energieverbrauchszählen die Möglichkeit, dass die Verbraucher ihre Energiekosten durch Änderung ihrer Gewohnheiten deutlich senken können, beispielsweise indem sie ihren Energieverbrauch auf andere Tageszeiten verlegen, in denen günstigere Tarife gelten, sowie durch die Möglichkeit für die Industrie, den Bedarf genauer im Voraus abschätzen zu können, so dass sich kostspielige Energiespeicherkosten verringern lassen. Das Erreichen der Klimaziele stützt sich in gewissem Umfang darauf, dass Verbraucher personenbezogene Daten freigeben, allerdings muss dies so erreicht werden, dass alle an den Programmen zur Einführung intelligenter Verbrauchsmessgeräte und an der Entwicklung der intelligenten Stromversorgungsnetze beteiligten Akteure dafür Sorge tragen, dass die Grundrechte der Bürger geschützt und eingehalten werden. Ohne einen diesbezüglichen Schutz besteht nicht nur die Gefahr, dass die Verarbeitung personenbezogener Daten gegen die einzelstaatlichen Rechtsvorschriften verstößt, mit denen Richtlinie 95/46/EG umgesetzt wird, sondern auch, dass die Verbraucher diese Programme ablehnen, weil sie mit der Erfassung personenbezogener Daten grundsätzlich nicht einverstanden sind. Zu einer solchen Ablehnung kann es selbst dann kommen, wenn gar kein Gesetzesverstoß vorliegt. Kurz gesagt, die Artikel-29-Datenschutzgruppe weist unter datenschutzrechtlichen Aspekten darauf hin, das diese Programme zwar weit reichende, erhebliche potenzielle Vorteile bieten, aber gleichzeitig dazu führen können, dass personenbezogene Daten in zunehmendem Umfang und in einer in dieser Branche noch nie dagewesenen Form verarbeitet werden und personenbezogene Daten einem größeren Empfängerkreis unmittelbar zur Verfügung stehen, als es gegenwärtig der Fall ist.

Die Artikel-29-Datenschutzgruppe ist sich darüber im Klaren, dass die Umstände je nach Mitgliedstaat erheblich variieren können und das Spektrum von Staaten reicht, in denen nach entsprechender staatlicher Initiative die Einführung weit gehend abgeschlossen ist, bis hin zu Staaten, in denen überhaupt keine entsprechenden Messgeräte installiert sind.

Auch der Grad der Beteiligung der Datenschutzbehörden variiert erheblich. Soweit noch nicht geschehen, möchte die Datenschutzgruppe daher alle Akteure der intelligenten Verbrauchsmesstechnik daran erinnern, wie wichtig die Konsultation der Datenschutzbehörde ist.

Weitere Unterschiede sind in den Strukturen der Märkte der Mitgliedstaaten sowie bei der Zuständigkeit für die Installation der Verbrauchsmessgeräte festzustellen. In einigen Mitgliedstaaten sind im Besitz der öffentlichen Hand befindliche Versorgerbetriebe zuständig. In anderen Ländern stehen die Versorger auf dem Markt miteinander im Wettbewerb. Verteilungsnetzbetreiber nehmen in einigen Ländern eine besonders herausgehobene Stellung ein. In bestimmten Mitgliedstaaten ist der Austausch der Messgeräte bei jedem Kunden vorgeschrieben. Wenn der Messzähler an den VNB eingesandt wird, sind die Energieversorger gegebenenfalls berechtigt, auf die Informationen zuzugreifen, die sie für die Kundenverwaltung und Rechnungsstellung benötigen. Außerdem können sie detailliertere Daten abrufen (beispielsweise zur Beratung über Energieeinsparmöglichkeiten), allerdings nur mit Zustimmung des Energiekunden. Außerdem ist der VNB berechtigt, detaillierte Informationen über den Verbrauch seiner Kunden zu erheben, um sein Netz verwalten und instand halten zu können.

Daneben bestehen vielfältige und komplexe Kommunikationswege mit zusätzlichen Zugangsstellen und Datenwegen, aus denen sich komplizierte Sicherheitsanforderungen ergeben, die umfassende Lösungen erfordern.

Aufgrund der komplexen und uneinheitlichen Gesamtsituation bringt die Aufgabe, Empfehlungen zu formulieren, besondere Herausforderungen mit sich, weshalb Empfehlungen in dieser Phase offenkundig nur in allgemeiner und nicht in spezifischer Form abgegeben werden können. Vernünftig und realistisch ist in dieser Phase daher, eine klare Aufgabenstellung für die Analyse zu formulieren und dabei den Zusammenhang zwischen den rechtlichen Anforderungen in der Datenschutzrichtlinie und dem Kontext der intelligenten Verbrauchsmessung in den Mittelpunkt der Betrachtungen zu stellen. Je nach Erfordernis soll dabei auf die von der Smart Grids Expert Group[2] bereits durchgeführten Forschungsarbeiten eingegangen werden. So decken sich beispielsweise die in dieser Stellungnahme enthaltenen Aussagen zum „eingebauten Datenschutz“ („Privacy by Design“) und zur Sicherheit mit den Empfehlungen der Datenschutzgruppe. Offenkundig ist die massenhafte Einführung intelligenter Verbrauchsmessgeräte bereits in vollem Gange, weshalb die Betroffenen unbedingt verstehen müssen, auf welche Weise intelligente Verbrauchsmessgeräte personenbezogene Daten verarbeiten und welche Fragestellungen sich daraus ergeben, auch wenn der Umfang der vorliegenden Veröffentlichung keinen Anspruch auf Vollständigkeit erhebt.

---

[2] Um den Prozess der EU-weiten Einführung intelligenter Stromversorgungsnetze zu fördern und zu unterstützen, beschloss die Europäische Kommission die Einrichtung einer Taskforce für intelligente Stromversorgungsnetze. Hierfür wurden drei Sachverständigengruppen eingerichtet, die Empfehlungen für die Einführung intelligenter Stromversorgungsnetze erarbeiten sollen. Das Grundlagendokument für diese Stellungnahme ist: Task Force Smart Grids Expert Group 2, *Regulatory Recommendations for Data Safety, Data Handling and Data Protection Report Issued February 16 2011*, [online] Verfügbar unter: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf [eingestellt: 25. März 2011]

In dieser Stellungnahme werden folgende Themenbereiche angesprochen: die Definition personenbezogener Daten im Zusammenhang mit intelligenten Verbrauchsmessverfahren, die Verantwortlichkeit für die Verarbeitung der Daten sowie die Prüfung legitimer Gründe für die Datenverarbeitung. Die Empfehlungen basieren auf dem aktuellen Kenntnisstand, für zukünftige Themen (beispielsweise intelligente Haushaltsgeräte) werden jedoch voraussichtlich noch weitere Arbeiten durchgeführt werden müssen.

Definitionen

Intelligente Verbrauchsmessgeräte und intelligente Stromversorgungsnetze werden auf unterschiedlichste Weise definiert. Um die Fragestellungen und Prioritäten der Artikel-29-Datenschutzgruppe angemessen abdecken zu können, erscheint jedoch die folgende Definition intelligenter Stromversorgungsnetze und intelligenter Verbrauchsmessgeräte zweckmäßig:

Intelligente Verbrauchsmessgeräte werden im Haushalt der Kunden von Energieversorgungsunternehmen installiert und sind für eine Zweiwegekommunikation ausgelegt. Sie informieren die Verbraucher über die verbrauchte Energiemenge, diese Informationen können aber auch zu den Energieversorgern und anderen benannten Akteuren übermittelt werden. Zentrales Merkmal der intelligenten Verbrauchsmessgeräte ist, dass sie die Möglichkeit für eine entsprechende Fernkommunikation zwischen dem Messgerät und befugten Stellen wie Versorgern oder Netzbetreiben und befugten Dritten oder Energiedienstleistungsunternehmen bieten. Durch intelligente Verbrauchsmessgeräte kann die Häufigkeit der Kommunikation zwischen Verbraucher und den anderen Akteuren erhöht und damit auch die Menge der über den Verbraucher vorliegenden Daten gesteigert werden, auf die diese anderen Akteure Zugriff haben. Die Erfassung und Nutzung der Daten deckt ein wesentlich breiteres Spektrum und wesentlich vielfältigere Verwendungszwecke ab, als es bei herkömmlichen Messgeräten ohne intelligente Funktionen der Fall ist, die direkt – allerdings relativ selten – abgelesen werden.

Grundsätzlich zeichnet ein intelligentes Verbrauchsmessgerät Werte auf, welche den Energieverbrauch in einem Gebäude ausdrücken. Dieser aufgezeichnete Wert kann zusammen mit anderen Informationen später auch außerhalb des Gebäudes weiterübermittelt werden. Bei einigen Modellen wird er direkt an einen zentralen Kommunikationsknotenpunkt übermittelt, wo die Daten der intelligenten Messgeräte verwaltet werden. Dort können VNB, Versorger und Energiedienstleistungsunternehmen (ESCO) auf die Daten zugreifen.

Die Einführung intelligenter Verbrauchsmessgeräte ist eine Grundvoraussetzung für ein intelligentes Stromversorgungsnetz. Beim so genannten „*Smart grid*“ handelt es sich um ein intelligentes Elektrizitätsnetz, in dem Informationen der Ver-

braucher im Netz so kombiniert werden, dass die Stromversorgung wirksamer und wirtschaftlicher geplant werden kann, als es vor Einführung derartiger intelligenter Netze möglich war.

Anwendung des Datenschutzrechts auf die Verarbeitung von über intelligente Verbrauchsmessgeräte erfassten Daten

Wenn die von einem intelligenten Verbrauchsmessgerät generierten und weiterverbreiteten Informationen personenbezogene Daten enthalten, fällt die Verarbeitung dieser Daten nach Auffassung der Datenschutzgruppe unter die Richtlinie 95/46/EG.

Aus den zu diesem Thema vorliegenden allgemeinen Informationen und aus ausführlichen auf einzelstaatlicher Ebene geführten Diskussionen zum Betrieb intelligenter Verbrauchsmessgeräte geht hervor, dass von der Verarbeitung der folgenden Arten von Daten ausgegangen werden kann:

- die eindeutige Identifikationsnummer des intelligenten Verbrauchsmessgeräts und/oder die eindeutige Kennummer des Gebäudes (selbst ohne diese Kenndaten kann das Messgerät möglicherweise anhand seines eindeutigen Energielastdiagramms identifiziert werden);

- Metadaten zur Konfiguration des intelligenten Verbrauchsmessgeräts;

- eine Beschreibung der übermittelten Mitteilung, beispielsweise ob es sich um eine Messgeräteablesung oder um eine Alarmmeldung bei unautorisierten Eingriffen am Gerät handelt;

- Datums- und Zeitstempel;

- Inhalt der Mitteilung.

Der Inhalt der Mitteilung enthält üblicherweise die folgenden Arten von Informationen:

- Ablesedaten des Zählers. Dabei kann es sich um einen einzelnen Ablesewert oder bei komplexeren Tarifen um eine Gruppe mehrerer Ablesewerte handeln;

- Alarmmeldungen. Das Messgerät kann eine Meldung übermitteln, dass aufgrund eines bestimmten Ereignisses der Alarm am Messgerät ausgelöst worden ist;

- Informationen auf Ebene des Netzes, beispielsweise Spannungen, Stromausfälle und Qualität der Energieversorgung;

- Lastgrafiken in unterschiedlichem Detaillierungsgrad.

Die Daten können in Echtzeit an den für die Datenverarbeitung Verantwortlichen übermittelt oder im intelligenten Verbrauchsmessgerät gespeichert werden. Allerdings wird gemäß der Datenschutzrichtlinie in beiden Fällen davon ausgegangen, dass die Daten von dem für die Datenverarbeitung Verantwortlichen erfasst wurden.

Diese Liste ist bei weitem nicht erschöpfend, die Datenschutzgruppe stellt jedoch fest, dass es durch den Betrieb von intelligenten Verbrauchsmessgeräten – und im weiteren Sinne damit durch den Betrieb von jeder Weiterentwicklung intelligenter Stromversorgungsnetze und Geräte – zur Verarbeitung personenbezogener Daten gemäß der Definition in Artikel 2 der Richtlinie 95/46/EG und der Auslegung durch die Datenschutzgruppe in ihrer Stellungnahme 4/2007 kommt. Außerdem ist es aufgrund der zunehmenden Menge der verarbeiteten personenbezogenen Daten, der Möglichkeiten einer Fernsteuerung der Verbindung und der Wahrscheinlichkeit eines Energie-Profiling auf der Grundlage detaillierter Messgeräteablesungen unabdingbar, dass das Grundrecht der betroffenen Personen auf den Schutz ihrer Privatsphäre in angemessener Weise Berücksichtigung findet.

Gründe für die Schlussfolgerung, dass personenbezogene Daten verarbeitet werden:

1. Die Daten, die gemäß der obigen Aufzählung durch intelligente Verbrauchsmessgeräte erzeugt werden, sind in den meisten Fällen eindeutigen Kenndaten wie der Identifikationsnummer eines Verbrauchsmessgeräts zugeordnet. Für Privatverbraucher als Kunden von Energieversorgern ist diese Identifikationsnummer unweigerlich an die Person gebunden, die für das entsprechende Kundenkonto verantwortlich ist. Anders ausgedrückt: Mithilfe dieses Geräts kann die betreffende Person aus der Gruppe der übrigen Verbraucher herausgefiltert werden.

2. Darüber hinaus beziehen sich die als Teil eines intelligenten Verbrauchsmessdienstes gesammelten Daten auf das Energieprofil eines Verbrauchers im Zusammenhang mit seinem Energieverbrauch und werden für Entscheidungen genutzt, die diese Person unmittelbar betreffen. Am offensichtlichsten dient eine entsprechende Entscheidung zur Festlegung der Kosten für die Energieversorgung, allerdings ist sie nicht auf Abrechnungsaspekte beschränkt.

3. Dieser Standpunkt findet seine weitere Bestätigung, wenn die weithin propagierten Vorteile der Einführung intelligenter Verbrauchsmessgeräte wie die Senkung des Gesamtenergieverbrauchs in den Mitgliedstaaten berücksichtigt

werden. Ein derartiges Ziel lässt sich offenkundig nur erreichen, wenn auch der Energieverbrauch der einzelnen Verbraucher gesenkt wird, und nach den Aussagen der Energieversorger und -netze ist dieses Ziel zu einem erheblichen Teil nur erreichbar, indem umfangreiche Datenmengen über das Verhalten dieser Verbraucher gesammelt werden.

Anwendung der Definition des für die Datenverarbeitung Verantwortlichen auf intelligente Verbrauchsmessgeräte

Durch die Richtlinie 95/46/EG werden dem für die Datenverarbeitung Verantwortlichen bestimmte Pflichten bei der Verarbeitung personenbezogener Daten auferlegt. Bevor dargelegt wird, wie diese Pflichten im Kontext der vorliegenden Stellungnahme Anwendung finden, muss die Datenschutzgruppe darstellen, welche juristischen Personen nach ihrer Auffassung unter die Definition des für die Datenverarbeitung Verantwortlichen fallen.

Bei der Einführung von intelligenten Verbrauchsmessgeräten sind verschiedene Organisationen an der Verarbeitung personenbezogener Daten beteiligt, unter anderem – ohne hierauf beschränkt zu sein – Energieversorger, Energienetzbetreiber, Regulierungsstellen, staatliche Stellen, externe Dienstleister und Kommunikationsdienstleister. Angesichts der Zahl und Komplexität der Beziehungen sind bei der Anwendung der maßgeblichen Definitionen mit einiger Wahrscheinlichkeit Schwierigkeiten zu erwarten, allerdings entspricht die Auswertung in dieser Stellungnahme dem von der Datenschutzgruppe in ihrer Stellungnahme 1/2010 verfolgten Konzept zu den Begriffen des für die Datenverarbeitung Verantwortlichen und des Auftragsverarbeiters. Die Verantwortlichkeiten, die sich aus den Rechtsvorschriften zum Datenschutz ergeben, sollten daher in eindeutiger Form so zugewiesen werden, dass die Einhaltung der Datenschutzvorschriften in der Praxis in ausreichender Weise gewährleistet ist.

Energieversorger

In manchen Mitgliedstaaten ist der Energieversorger die juristische Person mit der größten Verantwortung für die Verarbeitung personenbezogener Daten. Dieses Unternehmen hat den Vertrag mit der von der Datenverarbeitung betroffenen Person geschlossen, wodurch die Datenverarbeitung zustandekommt, und dadurch, dass diese Unternehmen entscheiden, welche Daten sie zur Erfüllung ihrer Aufgaben benötigen und wie sie diese erfassen, speichern und verwenden, ließe sich natürlich sagen, dass sie festlegen, wofür und auf welche Weise die personenbezogenen Daten verarbeitet werden. Damit stehen sie eindeutig als die für die Datenverarbeitung Verantwortlichen fest, in deren Verantwortungsbereich die Verarbeitung der personenbezogenen Daten fällt, welche von einem Energiever-

brauchsmessgerät erstellt wurden; die Datenschutzgruppe vertritt daher die Auffassung, dass die Versorger in diesem Kontext unabhängig von der durch intelligente Verbrauchsmessgeräte entstehenden zusätzlichen Komplexität weiterhin zu den für die Datenverarbeitung Verantwortlichen zählen.

Netzbetreiber oder VNB

In anderen Modellen ist der VNB, in dessen Besitz sich das Netz befindet, für Installation und Betrieb des Systems der intelligenten Verbrauchsmessgeräte („Smart Meters“) verantwortlich. Der VNB ist außerdem für die Festlegung verantwortlich, wie die Daten erfasst, gespeichert und verwendet werden. In diesem Modell ist der VNB der für die Datenverarbeitung Verantwortliche. Wenn die Energieversorger berechtigt sind, auf die von den Messgeräten übermittelten Daten zuzugreifen, und die Daten für eigene Zwecke nutzen (beispielsweise für die Rechnungsstellung oder Kundenberatung), gelten sie hinsichtlich der von ihnen verarbeiteten personenbezogenen Daten ebenfalls als für die Datenverarbeitung Verantwortliche.

Sonstige Akteure

Daneben kommen zahlreiche weitere Akteure in Betracht, die bei der Wahrnehmung ihrer Aufgaben in einem Programm zur Einführung intelligenter Verbrauchsmessgeräte gegebenenfalls personenbezogene Daten verarbeiten. Einige dieser Akteure treten möglicherweise erst auf, wenn die vollen Auswirkungen der Verlagerung hin zur Verarbeitung größerer Mengen personenbezogener Daten offenkundig werden; daher wäre es nicht sinnvoll, in der jetzigen Phase eine umfassende Liste aufstellen zu wollen. Außerdem sollten die Unterschiede der Versorgermodelle und Konzepte in den verschiedenen Mitgliedstaaten bedacht werden. Dabei ist allerdings zu berücksichtigen, dass die Gefahr, dass weder die Einhaltung der Vorschriften noch die Anwendung bewährter Verfahren erreicht wird, zunimmt, wenn nicht alle beteiligten Akteure bei ihrer Tätigkeit nach einer gemeinsamen Definition des Begriffs des für die Datenverarbeitung Verantwortlichen handeln. Vor diesem Hintergrund erinnert die Datenschutzgruppe alle beteiligten Akteure an die folgenden wichtigen Punkte:

1. Bei bestimmten Einführungsmodellen wird eine zentrale Kommunikationsstelle eingerichtet, die für die Abwicklung der Datenübertragung zwischen Messgerät und Versorger verantwortlich ist. Diese Stelle ist durchaus in Form eines Datenverarbeiters denkbar, der nur auf Anweisung der Versorger handelt, an die er Daten übermittelt und von denen er Daten erhält. Ist diese Kommunikationsstelle allerdings an der Entscheidung beteiligt, ob personenbezogene Daten gegenüber Dritten offengelegt werden dürfen oder ob solche Daten für

neue Zwecke verarbeitet werden dürfen, kann die Kommunikationsstelle bei dieser Verarbeitung personenbezogener Daten die Rolle des für die Datenverarbeitung Verantwortlichen übernehmen.

2. Auch Energieregulierungsbehörden sind wichtige Akteure. Sie können möglicherweise zur Aufstellung politischer Rahmenvorgaben und zu Forschungszwecken auf Daten zugreifen. Soweit es sich dabei um personenbezogene Daten handelt, übernimmt die betreffende Regulierungsbehörde eindeutig die Rolle eines für die Datenverarbeitung Verantwortlichen.

3. Externe Dienstleister (häufig als Energiedienstleistungsunternehmen bezeichnet) spielen bei der Nutzung der durch intelligente Verbrauchsmessgeräte erzeugten Daten eine zunehmend wichtige Rolle. Wenn personenbezogene Daten dem Energiedienstleistungsunternehmen zugänglich gemacht werden, damit dieses Dienstleistungen für die Verbraucher oder für andere Beteiligte, z. B. für einen Energieversorger, erbringen kann, übernimmt das Energiedienstleistungsunternehmen die Rolle eines für die Datenverarbeitung Verantwortlichen.

Rechtmäßigkeit der Datenverarbeitung und berechtigte Gründe/Zwecke der Datenverarbeitung

Wenn eine bestimmte juristische Person als für die Datenverarbeitung verantwortlich identifiziert wurde, müssen die rechtlichen Anforderungen festgelegt werden, denen der für die Datenverarbeitung Verantwortliche gemäß der Datenschutzrichtlinie unterliegt. Nach Artikel 6 der Richtlinie müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden. Die Verarbeitung personenbezogener Daten gilt als rechtmäßig, wenn einer oder mehrere der sechs Gründe für die rechtmäßige Verarbeitung gemäß Artikel 7 der Richtlinie erfüllt sind.

Die Datenschutzgruppe stellt fest, dass die genaue Art der Zwecke der Verarbeitung personenbezogener Daten, die durch ein intelligentes Verbrauchsmessgerät gespeichert oder übermittelt werden, in vielen, wenn nicht gar allen Mitgliedstaaten erst noch eindeutig geklärt bzw. ordnungsgemäß definiert werden muss. Aus diesem Grund empfiehlt die Arbeitsgruppe, diese Zwecke festzulegen, bevor geltend gemacht werden kann, dass die Datenverarbeitung rechtmäßig ist. Darüber hinaus stellt die Datenschutzgruppe fest, dass jeder Zweck für sich alleine rechtmäßig sein muss und dass es nicht zulässig ist, die Rechtmäßigkeit eines Zwecks zur Begründung der Rechtmäßigkeit eines anderen Zwecks heranzuziehen. Insbesondere ist es nicht zulässig, personenbezogene Daten für andere Zwecke weiterzuverarbeiten, die mit dem Zweck, für den sie ursprünglich erfasst wurden, nicht vereinbar sind.

Nach der Auffassung der Arbeitsgruppe bestehen fünf mögliche Gründe für die Datenverarbeitung, die von den für die Datenverarbeitung Verantwortlichen in diesem Zusammenhang in Anspruch genommen werden können.

Einwilligung

Viele der Fälle, in denen personenbezogene Daten verwendet werden können, beziehen sich auf zusätzliche Dienstleistungen, die der betroffenen Person angeboten werden, beispielsweise zeitabhängige Tarife oder Energieberatungsleistungen. Wenn eine betroffene Person darin einwilligt, eine derartige Dienstleistung anzunehmen, hat der Anbieter der Dienstleistung – entweder ein Versorger oder ein Dritter – wahrscheinlich auch die Gelegenheit, die Einwilligung der betroffenen Person in die Verarbeitung personenbezogener Daten einzuholen.

Die Datenschutzgruppe weist die für die Datenverarbeitung Verantwortlichen darauf hin, dass sie, wenn sie sich auf die Einwilligung der betroffenen Person verlassen, zu beachten haben, dass eine Einwilligung nur dann rechtsgültig ist, wenn die betroffene Person eine Entscheidung in voller Kenntnis der Sachlage treffen konnte. Eine Einwilligung kann nur dann als Grund für die Verarbeitung personenbezogener geltend gemacht werden, wenn die betroffene Person ausreichende Informationen über die Verarbeitung personenbezogener Daten erhalten hat und eine fundierte Entscheidung treffen konnte. Insbesondere dann, wenn verschiedene Funktionen vorliegen, sollte die Einwilligung soweit differenziert sein, dass die verschiedenen Möglichkeiten zum Ausdruck kommen und nicht eine einzige Einwilligung zur Legitimierung abweichender und nicht damit zusammenhängender anderweitiger Zwecke herangezogen wird.

Die Datenschutzgruppe empfiehlt, dass die Industrie wirksame und praxisnahe Mittel entwickelt, mit deren Hilfe die betroffenen Personen ihre Einwilligung erteilen können. Dabei sollte bedacht werden, dass die Einwilligung aus freien Stücken erteilt und damit auch widerrufen werden können muss, d. h. in den Verfahren zur Einholung der Einwilligung ist die Möglichkeit vorzusehen, dass die betroffene Person ohne unverhältnismäßigen Aufwand ihre Meinung ändern kann. Eine mögliche Lösung wäre beispielsweise, dass die Einwilligung an der Messgerätekonsole im Haushalt „per Druckknopf“ erteilt werden kann. Die Verfügbarkeit einer entsprechenden Funktion ist vom konstruktiven Entwicklungsstand des Messgeräts und der Messgerätekonsole abhängig, damit gewährleistet ist, dass das Einwilligungsverfahren seine Gültigkeit behält.

Vertrag

Die Verarbeitung von Daten ist gegebenenfalls auch notwendig, um einen Vertrag erfüllen zu können, bei dem die betroffene Person Vertragspartei ist, oder um auf

Aufforderung der betroffenen Person vor Vertragsabschluss bestimmte Maßnahmen einleiten zu können. Diese Rechtsgrundlage könnte zur Legitimierung der Verarbeitung personenbezogener Daten für die Rechnungserstellung dienen, da ohne ordnungsgemäß erstellte Rechnung der Vertrag über die Energieversorgung nicht erfüllt werden kann.

Hinsichtlich der Rechnungserstellung ist der Faktor der „Erforderlichkeit" in dieser Voraussetzung zu beachten. Anders ausgedrückt, wenn der Grund für die Verarbeitung von Daten in der Erfüllung eines Vertrags besteht, bei dem lediglich eine Vierteljahresrechnung für den Kunden erstellt und von diesem beglichen werden muss, braucht der Versorger keine häufigeren Ablesewerte zu erfassen, um diesen Vertrag zu erfüllen. Der Vertrag müsste dann eine zulässige und rechtsgültige Bestimmung über häufigere Ableseintervalle enthalten oder der Versorger müsste sich für diese Ablesungen auf eine andere Rechtsgrundlage stützen.

Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt

In einigen Mitgliedstaaten ist der Betreiber des Stromnetzes für die Leistung des baulichen Netzes, aber auch für die Verringerung des Gesamtstromverbrauchs verantwortlich. Dieser Stromverbrauch erstreckt sich sowohl auf den Gesamtverbrauch an Elektrizität als auch auf den Verbrauch während Spitzenzeiten. Diese Aufgaben werden im öffentlichen Interesse wahrgenommen und sind ein legitimer Grund für die Installation der intelligenten Verbrauchsmessgeräte.

Rechtliche Verpflichtung

In einigen Mitgliedstaaten ist der Netzbetreiber verpflichtet, bei jeder neuen Installation intelligente Verbrauchsmessgeräte zu installieren und Daten über diese Messgeräte zu erfassen[3].

Berechtigtes Interesse

Gemäß Artikel 7 Buchstabe f der Richtlinie wäre die Verarbeitung dann rechtmäßig, wenn sie für das berechtigte Interesse des für die Datenverarbeitung Verantwortlichen oder eines oder mehrerer Dritter erforderlich ist, gegenüber denen personenbezogene Daten offengelegt werden, sofern nicht das Interesse oder die Grundrechte der betroffenen Person überwiegen.

[3] Siehe Erlass Nr. 2010-1022 (Frankreich) vom 31. August 2010.

Entscheidend ist hierbei, dass der Rückgriff auf diese Rechtsgrundlage von der angemessenen Gewichtung der Interessen und Rechte der betroffenen Personen abhängig ist. Vordergründing scheint es unstrittig, dass eine effizientere Energieversorgung und effizienterer Energieverbrauch im berechtigten Interesse des für die Datenverarbeitung Verantwortlichen und der Gesellschaft insgesamt lägen und dass dies durch die Erfassung personenbezogener Daten aus intelligenten Verbrauchsmessgeräten erreicht werden könnte. Nur weil diese besondere Verwendung personenbezogener Daten scheinbar berechtigt (und für viele wünschenswert) erscheint, bedeutet dies jedoch nicht, dass damit jeder Teil der Datenverarbeitung legitimiert werden kann. Anders ausgedrückt, die Notwendigkeit, den Energieverbrauch zu senken, überwiegt – auch wenn sie ein sinnvolles Ziel der Politik der öffentlichen Hand wäre – nicht in jedem Fall gegenüber den Rechten und dem Interesse der betroffenen Personen.

Es versteht sich von selbst, dass durch praxisnahe Maßnahmen wie Technologien zum besseren Schutz der Privatsphäre und Datenschutz-Folgenabschätzungen, mit denen die Sicherheit und der Schutz der Privatsphäre der durch intelligente Verbrauchsmessgeräte verarbeiteten Daten verbessert werden können, diese Voraussetzung für die Datenverarbeitung dem für die Datenverarbeitung Verantwortlichen eher offenstehen könnte.

Dies ist insbesondere dann von Bedeutung, wenn die Datenverarbeitung entsprechend dem berechtigten Interesse eines für die Datenverarbeitung Verantwortlichen schon dem Wesen nach und in unverhältnismäßiger Weise einen Eingriff in die Privatsphäre darstellt oder die Folgen der Datenverarbeitung ungerechtfertigte Nachteile für die betroffene Person mit sich bringen. Als Beispiele sind unter anderem die Erstellung detaillierter Profile der betroffenen Personen zu nennen, die für den vorgesehenen Zweck nicht benötigt werden, ferner die Weitergabe von Daten an Dritte ohne Kenntnis oder Einwilligung der betroffenen Person oder die Nutzung personenbezogener Daten für Entscheidungen über die Fernabschaltung, ohne dass die Datenschutzrechte und sonstigen Rechte der betroffenen Person angemessen berücksichtigt werden.

Die Datenschutzgruppe erinnert die Industrie außerdem daran, dass in einigen Mitgliedstaaten die Möglichkeit besteht, dass die betroffene Person der Installation der intelligenten Verbrauchsmessgeräte widerspricht und dass in diesen Fällen das Interesse der betroffenen Person gegenüber sämtlichen sonstigen Interessen überwiegt.

Weitere Aspekte der Einhaltung der Rechtsvorschriften, die sich aus der intelligenten Verbrauchsmessung ergeben

Aufgrund des breiten Spektrums der Fragestellungen, die durch die intelligente Verbrauchsmessung aufgeworfen werden, kann die Datenschutzgruppe keine

umfassende Liste der Punkte vorlegen, zu denen Leitlinien vorgelegt werden könnten. Dieser Tätigkeitsbereich ist erst im Aufbau begriffen, weshalb die Datenschutzgruppe davon ausgeht, dass sich im Zuge der Installation weiterer intelligenter Verbrauchsmessgeräte neue Probleme und Lösungen im Bereich des Datenschutzes ergeben werden. Bestimmte generell relevante Aspekte sollten nach Ansicht der Datenschutzgruppe jedoch von allen Akteuren in diesem Bereich ernsthaft in die eigenen Überlegungen einbezogen werden.

Eingebauter Datenschutz („Privacy by Design")

Die Datenschutzgruppe verweist auf ihre Stellungnahme 168, wonach Dienstleistungen und Technologien, die sich auf die Verarbeitung personenbezogener Daten stützen, nach dem Prinzip der „Privacy by default" (datenschutzfreundliche Voreinstellungen) aufgebaut sein sollten. In dieser Hinsicht muss die Einführung intelligenter Verbrauchsmessverfahren so erfolgen, dass der Datenschutz von Anfang an mit einbezogen wird, und zwar nicht nur hinsichtlich der Sicherheitsmaßnahmen, sondern auch dadurch, dass die Menge der verarbeiteten personenbezogenen Daten minimiert wird. In einigen Mitgliedstaaten wurden Einführungspläne entwickelt, nach denen eine Datenschutz-Folgenabschätzung („Privacy Impact Assessment") durchgeführt werden muss; auch die Datenschutzgruppe empfiehlt diese Vorgehensweise.

Die intelligenten Verbrauchsmessgeräte, die gegenwärtig in mehreren Mitgliedstaaten erprobt werden, erfassen je nach Art des mit dem Kunden geschlossenen Vertrags mehrere Ablesewerte. Verfügt der Kunde beispielsweise über einen einfachen Vertrag, bei dem er über den gesamten Tag hinweg den gleichen Stromtarif bezahlt, erfasst das Messgerät einen einzigen Ablesewert pro Tag. Sind im Vertrag mit dem Kunden jedoch je nach Tageszeit unterschiedliche Tarife vorgesehen, erfasst das Messgerät beispielsweise zehn verschiedene Ablesewerte pro Tag. In der einfachsten Ausführung würde durch den eingebauten Datenschutz („Privacy By Design") gewährleistet, dass die Ablesewerte des Messgeräts nur so häufig übermittelt werden, wie es für den Betrieb des Systems oder die Erbringung der Dienstleistung, zu deren Inanspruchnahme der Kunde sein Einverständnis gegeben hat, notwendig ist.

In einer gegenwärtig eingesetzten Ausführung des Verbrauchsmessgeräts werden beispielsweise alle zehn bis sechzig Minuten in Echtzeit Verbrauchsmessdaten erfasst und daraus ein Lastdiagramm erstellt. Die Häufigkeit kann durch Fernabfrage vom Elektrizitätsnetzbetreiber eingestellt werden. Dieses Lastdiagramm wird im Messgerät zwei Monate lang gespeichert und vom Elektrizitätsnetzbetreiber bei Bedarf erfasst. In der Übertragung auf das Konzept des eingebauten Datenschutzes könnte dieses Modell so angepasst werden, dass das Lastdiagramm nur auf Aufforderung erfasst und gespeichert wird.

Auch durch die technischen Kenngrößen des Netzes sollte gewährleistet werden, dass die erfassten Daten im Haushalt verbleiben, sofern nicht die Weitergabe an andere Empfänger erforderlich ist oder die betroffene Person der Übermittlung zustimmt. Außerdem sollte das System so aufgebaut sein, dass selbst bei der Übermittlung personenbezogener Daten alle Datenelemente, die nicht für den Zweck der Übermittlung unabdingbar sind, herausgefiltert oder entfernt werden. Das übergeordnete Ziel sollte also darin bestehen, möglichst geringe Datenmengen zu verarbeiten und zu übermitteln.

Die Datenschutzgruppe empfiehlt außerdem, die Systeme so auszulegen, dass der Zugang zu personenbezogenen Daten nur soweit ermöglicht wird, wie es erforderlich ist, damit der für die Datenverarbeitung Verantwortliche seine Aufgaben wahrnehmen kann. Sämtliche Beteiligten, die auf personenbezogene Daten zugreifen, sollten darauf überprüft werden, ob sie legitime und zuständige Empfänger der personenbezogenen Daten sind, und dürfen nur auf diejenigen personenbezogenen Daten zugreifen können, die sie zur Wahrnehmung ihrer Aufgaben benötigen. Über diesen Rahmen hinaus dürfen sie nicht auf personenbezogene Daten zugreifen können.

Speicherung personenbezogener Daten

Vor der Einführung „intelligenter“ Systeme hat die Energiewirtschaft Verfahren entwickelt, um personenbezogene Daten für einen begrenzten Bereich von Verwendungszwecken aufbewahren zu können, beispielsweise für die Rechnungsstellung. Mit intelligenten Verbrauchsmesssystemen stellen sich neue Herausforderungen. Da erheblich größere Datenmengen verarbeitet werden, müssen die Leitlinien und Verfahrensweisen für die Datenspeicherung für neue Verwendungszwecke festgelegt und für bereits bestehende Zwecke überarbeitet werden. Um sicher sein zu können, dass bestimmte Daten nur so lange gespeichert bleiben, wie dies für einen bestimmten, rechtmäßigen Zweck erforderlich ist, müssen die Verarbeitungszwecke, um die es hierbei geht, klarer verstanden werden können. Damit können die für die Datenverarbeitung Verantwortlichen ihrerseits nachweisen, dass personenbezogene Daten nur so lang wie nötig gespeichert werden. Häufig wird als Verwendungszweck beispielsweise angegeben, dass anhand der über ein Messgerät erfassten Daten der Verbraucher in Fragen der effizienten Energienutzung beraten werden kann. In bestimmten Fällen können im Rahmen dieses Service Vergleiche über mehrere Jahre hinweg angeboten werden, weshalb dreizehn Monate als geeigneter Zeitraum für die Speicherung personenbezogener Daten für diesen Verwendungszweck genannt wurden. Ein derart langer Aufbewahrungszeitraum wäre allerdings nur dann akzeptabel, wenn die betroffene Person der Inanspruchnahme eines entsprechenden Service zugestimmt hat. Für andere Dienstleistungsangebote müsste ein wesentlich kürzerer Speicherungszeitraum vorgeschrieben werden.

Darüber hinaus wäre denkbar, dass die Verbraucher einen Großteil dieser Daten auf dem Messgerät oder einem vergleichbaren Zwischengerät (bei dem es sich nicht um das für die Rechnungsstellung verwendete Gerät handelt) speichern könnten. Die betroffene Person könnte dann eine selbstständige Entscheidung über die Datenspeicherung treffen. In diesem Fall wäre es sinnvoll, dass die Verbraucher durch ein System mit Erinnerungs- oder Aufforderungsmeldungen bei der Verwaltung dieser Daten unterstützt werden.

Verarbeitung personenbezogener Daten durch Dritte

Es ist abzusehen, dass Dritte bzw. Energiedienstleistungsunternehmen in erheblichem Umfang an der Einführung und Unterstützung intelligenter Verbrauchsmessungen beteiligt sein werden; die Datenschutzgruppe hält daher eine genaue Prüfung dieses Sachverhalts für notwendig. Einfluss und Beteiligung Dritter variieren je nach Mitgliedstaat, allerdings ist klar, dass die Einführung intelligenter Verbrauchsmessungen, mit denen besonders weitreichende Eingriffe in die Privatsphäre einhergehen, dazu führen könnte, dass sich ein Handel mit Energieprofilen zum Vorteil derjenigen entwickelt, die Energiedienstleistungen am Markt anbieten möchten.

Zur technischen Unterstützung bei der Einhaltung der Vorschriften wurde die Einrichtung eines zentralen Informations- und Kommunikationsknotenpunkts vorgeschlagen, der für alle, die auf die Verbraucherdaten zugreifen möchten, als „Schleuse“ dient, ferner ein Kodex, der von allen Beteiligten unterzeichnet werden muss, sowie eine industrieweite Charta. Die Datenschutzgruppe unterstreicht in aller Deutlichkeit, dass die Sicherheitsmaßnahmen umso strenger sein müssen, je weitreichender die Eingriffe in die Privatsphäre sind. Die Datenschutzgruppe ersucht daher die zuständigen Regulierungsbehörden mit Nachdruck um Prüfung der Zulässigkeit von Datenverarbeitungsmaßnahmen, die einen weitgehenderen Eingriff in die Privatsphäre darstellen.

Die Grundlage hierfür wäre in jedem Fall die Einwilligung des Verbrauchers, wobei die Industrie dafür zu sorgen hat, dass die betroffene Person diese Einwilligung aus einer informierten Position heraus erteilen kann. Wie die Datenschutzgruppe betont, wäre es nicht akzeptabel, wenn Dritte detaillierte Angaben über den Energieverbrauch der betroffenen Person ohne die Kenntnis und das Einverständnis der betroffenen Person verarbeiten würden.

Sicherheit

Im Rahmen des Verfahrens des eingebauten Datenschutzes werden in Risikoabschätzungen für Sicherheit und Datenschutz die möglichen Risiken für die Da-

tensicherheit aufgezeigt. Aufgrund der neuartigen und noch gar nicht abzuschätzenden Perspektiven, die sich durch intelligente Stromversorgungsnetze und die damit einhergehenden Technologien eröffnen, bedeutet die Aufgabe, die Sicherheitsanforderungen bereits im Vorfeld abzuschätzen, eine besondere Herausforderung.

Vor diesem Hintergrund wird in dieser Stellungnahme empfohlen, zur Risikominderung einen End-to-End-Ansatz zu verfolgen, in den sämtliche Parteien eingebunden werden und ein breites Spektrum an Fachwissen genutzt wird. Darüber hinaus sollten Sicherheitsaspekte möglichst früh in die Netzarchitektur einfließen und nicht erst später nachträglich aufgenommen werden.

Die Datenschutzgruppe betont, dass die betroffenen Personen nur dann sicher sein können, dass ihre personenbezogenen Daten auf sichere Weise verarbeitet werden und ihr Grundrecht auf Datenschutz gewahrt wird, wenn ausreichend belastbare Sicherheitsvorkehrungen vorhanden sind. Diese Sicherheitsvorkehrungen sollten sich auf den gesamten Prozess erstrecken – einschließlich der im Haushalt untergebrachten Teile des Netzes, der Übermittlung personenbezogener Daten über das Netz sowie der Speicherung und Verarbeitung personenbezogener Daten durch Lieferanten, Netze und anderen für die Datenverarbeitung Verantwortlichen.

Die Datenschutzgruppe geht davon aus, dass intelligente Verbrauchsmessgeräte eine lange Lebensdauer erreichen werden, und weist daher darauf hin, dass die Datenschutzmaßnahmen im Laufe der Zeit aktualisiert und optimiert und regelmäßig überprüft und getestet werden müssen.

Angesichts der zunehmenden Mengen an personenbezogenen Daten, die verarbeitet werden, nimmt offenkundig auch das Risiko für den Schutz der Daten zu. Daher empfiehlt die Datenschutzgruppe, dass die technischen und organisatorischen Schutzmaßnahmen zumindest die folgenden Bereiche abdecken sollten:

- vorbeugende Maßnahmen gegen die unbefugte Offenlegung personenbezogener Daten;

- Aufrechterhaltung der Datenintegrität als Schutz gegen unbefugte Veränderungen der Daten;

- wirksame Authentifizierung der Identität aller Empfänger personenbezogener Daten;

- Unterbrechungen wichtiger Dienste durch Angriffe auf die Sicherheit personenbezogener Daten sind zu vermeiden;

- Vorkehrungen für die Durchführung sachgemäßer Prüfungen personenbezogener Daten, die auf einem Zähler gespeichert sind oder von diesem übertragen werden;
- Angemessene Zugangskontrollen und Speicherungszeiträume;
- Aggregierung von Daten, wenn Daten auf Einzelebene nicht benötigt werden.

Individuelle Rechte einschließlich der an betroffene Personen übermittelten Informationen

Mit der Einführung intelligenter Verbrauchsmessgeräte entstehen auch komplexe und neuartige Abläufe für die Verarbeitung personenbezogener Daten. Die meisten betroffenen Personen haben weder von der Art dieser Abläufe noch von den möglichen Auswirkungen auf ihre Privatsphäre eine Vorstellung. Wenn sie aber keine Kenntnis von der Verarbeitung der personenbezogenen Daten haben, können sie hierüber auch keine Entscheidungen in voller Kenntnis der Sachlage treffen. Die Pflicht, die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten zu informieren, ist eines der Grundprinzipien der Datenschutzrichtlinie. In Artikel 10 ist die Bereitstellung dieser Informationen geregelt und der für die Datenverarbeitung Verantwortliche wird dazu verpflichtet, der betroffenen Person die folgenden Informationen vorzulegen:

- die Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,
- die Zweckbestimmungen der Verarbeitung,
- weitere Informationen, die eine faire Datenverarbeitung ermöglichen. Hierzu zählen die Identität der Empfänger der personenbezogenen Daten sowie das Bestehen von Auskunfts- und Berichtigungsrechten.

Die für die Datenverarbeitung Verantwortlichen, die für die Installation und Wartung der Zähler verantwortlich sind, sind gehalten, den betroffenen Personen zu erklären, welche Informationen aus dem Messgerät erfasst werden und wofür sie verwendet werden.

Soweit Dritte an der Verarbeitung personenbezogener Daten für die Erbringung bestimmter Dienstleistungen für die betroffenen Personen beteiligt sind, sollten die betroffenen Personen in ähnlicher Weise unterrichtet werden. In bestimmten Fällen ist es möglicherweise angebracht, eine unabhängige Überprüfung oder Überwachung des Zugriffs Dritter auf personenbezogene Daten und der Nutzung dieser Daten durch Dritte zu ermöglichen, damit eine Irreführung der betroffenen Personen ausgeschlossen ist.

Rechte der betroffenen Person

Die für die Datenverarbeitung Verantwortlichen sind verpflichtet, die Rechte der betroffenen Personen auf Dateneinsicht und gegebenenfalls auf Berichtigung oder Löschung der über sie gespeicherten Daten zu beachten. Da ein zentraler Bestandteil des Projekts der intelligenten Verbrauchsmessungen in der Einführung eines „haushaltsinternen Netzes“ (in dem der Verbraucher aus dem intelligenten Verbrauchsmessgerät unmittelbar Informationen über seine Verbrauchsmuster und Tarife erhält) besteht, bedeutet dies zugleich die Möglichkeit, dass die betroffenen Personen ihre Rechte unter Verwendung von Instrumenten, die einen direkten Zugriff auf die Daten ermöglichen, wahrnehmen können.

Mit bestimmten Technologien lässt sich die Dateneinsichtnahme für die betroffenen Personen jedoch möglicherweise nicht erreichen. Eines der in einigen Mitgliedstaaten derzeit getesteten Messgeräte weist beispielsweise nur ein kleines Textanzeigefenster auf. Der Verbraucher kann also weder auf die vom Messgerät bereits übermittelten Daten noch auf die Anzeigegrafiken wie z. B. das Lastdiagramm (das im Messgerät gespeichert ist) zugreifen. Dieses Anzeigefenster dürfte also nicht ausreichen, um die Forderung der betroffenen Person auf Dateneinsicht zu erfüllen.

Verarbeitung von Daten im Rahmen von Verbrechensprävention und -aufklärung

Die Datenschutzrichtlinie untersagt die Verarbeitung personenbezogener Daten in den Fällen, in denen sie im Hinblick auf den Zweck unverhältnismäßig ist. Das detaillierte Bild, das intelligente Verbrauchsmessgeräte liefern und mit dem sie die Versorger über die Energieverbrauchsmuster informieren, könnte auch die Aufklärung verdächtiger und in bestimmten Fällen gesetzeswidriger Tätigkeiten ermöglichen. Die Datenschutzgruppe erinnert die Industrie daran, dass das Bestehen einer solchen Möglichkeit jedoch nicht automatisch die breit angelegte Verarbeitung von Daten für diesen Zweck rechtlich legitimiert. Von besonderer Bedeutung ist dabei, dass personenbezogene Daten, die eine angebliche Straftat betreffen, als sensible Daten eingestuft würden und die für die Datenverarbeitung Verantwortlichen diese Daten daher nur verarbeiten dürften, wenn Artikel 8 Absatz 5 der Richtlinie zur Anwendung käme.

Schlussfolgerung

Mit der Einführung intelligenter Verbrauchsmessungen, die den Weg für intelligente Stromversorgungsnetze frei machen, entsteht ein völlig neues, komplexes Modell gegenseitiger Wechselbeziehungen, das besondere Herausforderungen an

die Anwendung des Datenschutzrechts stellt. Aus den Antworten auf den Fragebogen der Generaldirektion Energie geht hervor, dass die Situation in den EU-Mitgliedstaaten sehr unterschiedlich ist, sowohl hinsichtlich der Fortschritte bei der Einführung als auch hinsichtlich der Energieversorgungssysteme, wodurch sich die Sachlage weiter kompliziert. Eindeutig klar ist jedoch die immense Tragweite intelligenter Verbrauchsmessungen: Vor Ende dieses Jahrzehnts dürften entsprechende Systeme in den Haushalten der überwiegenden Mehrheit der Bürger Europas installiert sein.

In dieser Stellungnahme wird die Anwendbarkeit des Datenschutzrechts erläutert; dabei wird dargelegt, dass von den Messgeräten personenbezogene Daten verarbeitet werden und somit die Datenschutzvorschriften Anwendung finden.

Mit dieser Stellungnahme wird aufgezeigt, dass intelligente Verbrauchsmessungen das Potenzial für vielfältige neue Formen der Datenverarbeitung und der Kundendienstleistungen bieten. Egal wie die Datenverarbeitung erfolgt – ob auf ähnliche Weise wie zu den Zeiten vor Einführung intelligenter Systeme oder in völlig neuartiger Form –, der für die Datenverarbeitung Verantwortliche muss eindeutig ermittelt werden und sich der aus dem Datenschutzrecht erwachsenden Pflichten, auch in Bereichen wie „eingebautem Datenschutz“ („Privacy by Design“), Datensicherheit und Rechte der betroffenen Person, bewusst sein. Die betroffenen Personen müssen in geeigneter Form darüber unterrichtet werden, wie ihre Daten verarbeitet werden, und sich über die grundlegenden Unterschiede darin, wie ihre Daten verarbeitet werden, im Klaren sein, so dass sie ihre Einwilligung in rechtsgültiger Form geben können.

Brüssel, den 4. April 2011

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Arbeitsdokument 1/2011 über die EU-Regeln für Verstöße gegen die Datenschutzvorschriften mit Empfehlungen für zukünftige Politikentwicklungen (WP 184)

Angenommen am 5. April 2011

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten −

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 (ABl. L 281 vom 23.11.1995, S. 31),

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

gestützt auf ihre Geschäftsordnung −

hat folgendes Arbeitsdokument angenommen:

I. EINLEITUNG

1. Das vorliegende Dokument der Artikel-29-Datenschutzgruppe enthält eine Bestandsaufnahme der Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation und der Art und Weise, wie die Mitgliedstaaten die Vorschriften dieser Richtlinie über Verstöße gegen den Datenschutz in nationales Recht umsetzen[1].

2. Mit dieser Bilanz soll ein dreifaches Ziel verfolgt werden: ***Erstens*** möchte die Artikel-29-Datenschutzgruppe umfassende Kenntnis über den aktuellen Stand der Dinge erlangen. Dazu gehören sowohl grundlegende Aspekte wie der Stand der Umsetzung als auch komplexere, wie beispielsweise die Ermittlung der Unterschiede in der Vorgehensweise in verschiedenen Bereichen (z. B. der Anwendungsbereich der Vorschriften; nationale Leitlinien, in denen einige Aspekte der Richtlinie weiterentwickelt werden; die zuständige Behörde des Mitgliedstaaten usw.). Durch das Aufzeigen etwaiger abweichender Entwicklungen in den Mitgliedstaaten kann diesen geholfen werden, selbst in dieser späten Phase noch ihre Positionen anzugleichen und eine fragmentierte Umsetzung zu vermeiden.

[1] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung, unter anderem, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt L 337 vom 18.12.2009, S. 11.

3. ***Zweitens***: die Bestandsaufnahme soll den nationalen Datenschutzbehörden helfen, bestimmte Ergebnisse zur Kenntnis zu nehmen. Sie wurden darauf aufmerksam gemacht, dass Folgemaßnahmen erforderlich sind, die in dem vorliegenden Arbeitsdokument beschrieben sind. Ein Ergebnis der Bestandsaufnahme ist, dass die zuständigen Behörden weiter darauf hinwirken sollten, dass interne Regeln und Verfahren festgelegt werden, nach denen die zuständigen Behörden und betroffene Einzelpersonen von den für die Verarbeitung der Daten Verantwortlichen benachrichtigt werden. Wenn man in Betracht zieht, dass die für die Verarbeitung der Daten Verantwortlichen in zunehmendem Maße grenzüberschreitende Verstöße gegen den Schutz personenbezogener Daten melden werden, wird darüber hinaus deutlich, dass die Behörden gemeinsam Methoden der Zusammenarbeit besprechen müssen.

4. ***Drittens***: Die Bestandsaufnahme hat der Artikel-29-Datenschutzgruppe die Gelegenheit gegeben, das Thema weiter zu vertiefen und einige Schlussfolgerungen bezüglich zukünftiger Politikentwicklungen im Bereich der Meldung von Verstößen zu ziehen. Diese Schlussfolgerungen ergänzen die Stellungnahmen, die die Artikel-29-Datenschutzgruppe bei anderen Gelegenheiten[2] zu diesem Thema abgegeben hat. Sie bauen auf den gemeldeten Verstößen gegen den Datenschutz auf, die diejenigen nationalen Datenschutzbehörden, die die Anzeigepflicht für Datenschutzverstöße bereits anwenden, gesammelt haben. Nach Ansicht der Artikel-29-Datenschutzgruppe sollten diese Ergebnisse bei künftigen Politikentwicklungen in Bezug auf Verstöße berücksichtigt werden. Politikentwicklungen werden insbesondere in den folgenden beiden Kontexten erwartet:

   a) Ergänzung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation, die Datenschutzverletzungen betreffen. In Artikel 4 Absatz 5 der Richtlinie wird der Kommission die Befugnis zur Annahme technischer Durchführungsmaßnahmen (gemäß Artikel 290 AEUV nach der Annahme des Vertrags von Lissabon als „übertragene Befugnisse" bezeichnet) übertragen, um eine einheitliche Umsetzung und Anwendung der Bestimmungen in genau festgelegten Bereichen sicherzustellen (d. h. Umstände, Form und Verfahren der in den Bestimmungen vorgeschriebenen Informationen und Anzeigen).

---

[2] Siehe Papier der Artikel-29-Datenschutzgruppe „Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten", angenommen am 1.12.2009 (WP 168); Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), angenommen am 10.02.2009 (WP 159); Stellungnahme 2/2008 zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), angenommen am 15.05.2008 (WP 150).

b) Erweiterung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation, die Datenschutzverletzungen betreffen, im Zusammenhang mit der Überprüfung der Richtlinie 95/46. Die Kommission hat sich gegenüber dem Europäischen Parlament dazu verpflichtet, unverzüglich angemessene Vorbereitungsarbeiten einzuleiten. Dazu gehört auch die Konsultation interessierter Kreise mit dem Ziel, diesbezügliche Vorschläge – sofern anwendbar – bis Ende 2011 vorzulegen[3]. Diese Verpflichtung wurde in der Mitteilung der Kommission „*Gesamtkonzept für den Datenschutz in der Europäischen Union*“[4] bekräftigt.

5. Die oben genannten Punkte werden wie folgt behandelt: Nach einer Zusammenfassung der wichtigsten Vorschriften zur Verletzung des Schutzes personenbezogener Daten in der Datenschutzrichtlinie für elektronische Kommunikation (Abschnitt II) werden die einschlägigen Rechtsvorschriften der Mitgliedstaaten zusammengefasst (Abschnitt III). Die Zusammenfassung basiert auf den Informationen, die von den nationalen Datenschutzbehörden bereitgestellt wurden. Sie werden hier jedoch nicht wiedergegeben, da die Umsetzung ein fortschreitender Prozess ist. In Abschnitt IV werden Maßnahmen aufgezeigt, die von den zuständigen Behörden und von der Artikel-29-Datenschutzgruppe mit Blick auf die Festlegung interner Prozesse und Kooperationsverfahren durchzuführen sind. In den Abschnitten V und VI wird insofern der Schwerpunkt auf die neuen Politikentwicklungen gelegt, als darin der Gesamtanwendungsbereich und die Verfahren für die erwarteten Aktionspläne in Bezug auf die Verletzung des Schutzes personenbezogener Daten in Erinnerung gerufen und Politikempfehlungen gegeben werden.

6. Die hier zum Ausdruck gebrachten Meinungen präjudizieren nicht möglicherweise speziellere Leitlinien, die – auch im Zusammenhang mit der Annahme der technischen Durchführungsmaßnahmen gemäß Artikel 4 Absatz 5 der Datenschutzrichtlinie für elektronische Kommunikation durch die Kommission – aufgestellt werden können.

II. DATENSCHUTZVERLETZUNGEN GEMÄSS DER DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION

7. Die revidierte Datenschutzrichtlinie für elektronische Kommunikation legt erstmals in der EU einen Rahmen für eine Verpflichtung zur Anzeige von

[3] Siehe die Erklärung, die die Kommission 2009 zur Anzeigepflicht für Datenschutzverstöße vor dem Europäischen Parlament im Zusammenhang mit der Reform des Rechtsrahmens für die elektronische Kommunikation abgegeben hat.

[4] KOM(2010) 609 endgültig vom 4.11.2010

Verstöße gegen die Datenschutzvorschriften fest. Dieser Rahmen findet nur auf die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung (z. B. Anbieter von Kommunikationsnetzen und Internetzugangsanbieter).[5] Der Rahmen enthält bestimmte Kernelemente, die zwingend in den Rechtvorschriften der Mitgliedstaaten umgesetzt werden müssen.

II. 1 Gemeinsame Kernelemente

8. Folgende Kernelemente sind in der Datenschutzrichtlinie für elektronische Kommunikation niedergelegt:

   a. ***Definition von Datenschutzverletzung*** gemäß Artikel 2 Buchstabe i: Eine Verletzung des Schutzes personenbezogener Daten ist „*eine Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden*". Eine Verletzung des Datenschutzes kann nur vorliegen, wenn es um „personenbezogene Daten" in der Definition von Artikel 2 Buchstabe a der Datenschutzrichtlinie[6] geht. Eine Verletzung des Datenschutzes umfasst die unbefugte Weitergabe oder den unberechtigten Zugang zu personenbezogenen Daten, aber auch eine einfache unbeabsichtigte Vernichtung oder Veränderung, auf die kein (oder höchstwahrscheinlich kein) unberechtigter Zugang folgt.

   b. Rechtliche ***Kriterien*** für die Benachrichtigung von Personen und Behörden (Artikel 4 Absatz 3 Unterabsätze 1 und 2). Anhand der Kriterien entscheidet sich, wann eine Stelle, in der es zu einer Datenverletzung gekommen ist, dazu verpflichtet ist, die Behörden und betroffenen Personen zu unterrich-

---

[5] Wie definiert in Artikel 2 der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste in der durch die Richtlinie 2009/140/EG und Verordnung 544/2009 geänderten Fassung („Rahmenrichtlinie"). Sie gilt für Anbieter von gewöhnlich gegen Entgelt erbrachten Diensten, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Netze bestehen. Die Definition nimmt die Bereitstellung von Inhalten und von Diensten der Informationsgesellschaft aus, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Netze bestehen.

[6] Richtlinie 1995/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; Amtsblatt L 281 vom 23.11.1995. Artikel 2 Buchstabe a der Datenschutzrichtlinie: „*alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.*"

ten. Die Datenschutzrichtlinie für elektronische Kommunikation schreibt die Benachrichtigung von Personen im folgenden Fall vor: „*Ist anzunehmen, dass durch die Verletzung personenbezogener Daten die personenbezogenen Daten, oder Teilnehmer oder Personen in ihrer Privatsphäre, beeinträchtigt werden…*“. Alle Datenschutzverletzungen sind den Behörden zu melden.

c. ***Inhalt und Zeitpunkt der Benachrichtigung.*** Der Zeitpunkt der Benachrichtigung von Personen ist gemäß Artikel 4 Absatz 3 Unterabsätze 1 und 2 „… unverzüglich…“. In der Benachrichtigung sind die Art der Verletzung des Schutzes personenbezogener Daten, die Kontaktstellen und die Maßnahmen zur Begrenzung der möglichen nachteiligen Auswirkungen aufzuführen. In der Benachrichtigung an die zuständige nationale Behörde müssen auch die von dem Betreiber infolge der Verletzung ergriffenen Maßnahmen dargelegt werden.

d. Mögliche Ausnahmen im Zusammenhang mit ***technischen Schutzmaßnahmen*** (Artikel 4 Absatz 3 Unterabsatz 3) und mit der Strafverfolgung.

9. Auch wenn dieser Rahmen harmonisierte Vorschriften in der ganzen EU sicherstellen sollte, könnten einige der nachfolgend beschriebenen Faktoren zu unterschiedlichen Vorgehensweisen in den Mitgliedstaaten führen.

II. 2 Bereiche, in denen es zu unterschiedlichen Vorgehensweisen kommen könnte

10. Es gibt drei Bereiche, in denen sich unterschiedliche Vorgehensweisen ergeben können. Sie werden nachfolgend beschrieben.

11. ***Anwendungsbereich der Verpflichtung:*** Die Verpflichtung zur Meldung von Verstößen gegen die Datenschutzvorschriften findet gemäß der Datenschutzrichtlinie für elektronische Kommunikation auf die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung. Erwägungsgrund 59 der Richtlinie soll die Mitgliedstaaten allerdings zu einer Ausdehnung des Anwendungsbereichs anhalten (Unterstreichung hinzugefügt): „*… Bis zu einer Überprüfung aller einschlägigen gemeinschaftlichen Rechtsvorschriften auf diesem Gebiet durch die Kommission sollte die Kommission in Abstimmung mit dem Europäischen Datenschutzbeauftragten unverzüglich geeignete Maßnahmen ergreifen, um die gemeinschaftsweite Anwendung der in der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) enthaltenen Leitlinien für die Anzeigepflicht bei Verstößen gegen die Datensicherheit, ungeachtet des Sektors oder der Art der betreffenden Daten, zu fördern.*“

12. ***Leitlinien der zuständigen Behörden:*** Die Datenschutzrichtlinie für elektronische Kommunikation (Artikel 4 Absatz 4) erlaubt es den zuständigen nationalen Behörden ausdrücklich, zu den drei nachfolgend genannten Punkten Leitlinien anzunehmen und Anweisungen zu erteilen:

    a) Umstände, unter denen die Benachrichtigung seitens der Betreiber über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist;

    b) Format der Benachrichtigung und

    c) Verfahrensweise für die Benachrichtigung.

    Der vorgenannte Punkt (a) berechtigt die zuständigen nationalen Behörden beispielsweise dazu, bestimmte personenbezogene Informationen festzulegen, bei deren Beeinträchtigung wegen ihrer Sensibilität das Kriterium automatisch als erfüllt gilt und die Benachrichtigungspflicht ausgelöst würde.[7] Sie können danach auch festlegen, für welche Situationen, in denen das Kriterium nicht erfüllt ist, keine Benachrichtigungspflicht besteht. Je nachdem, ob und wie die zuständigen Behörden diese Befugnis nutzen, werden sich zumindest in Bezug auf diese Punkte Unterschiede in der Vorgehensweise ergeben. Für Leitlinien und Anweisungen der zuständigen Behörden kann die Kommission jedoch Durchführungsmaßnahmen erlassen. Siehe Abschnitt V und VI.

13. ***Technische Schutzmaßnahmen:*** Unterschiede können sich auch bei der Anwendung der Ausnahmeregel in Bezug auf die technischen Schutzmaßnahmen ergeben. Mit diesen Maßnahmen werden die Daten für alle Personen verschlüsselt, die nicht befugt sind, Zugang zu den Daten zu haben. Unterschiede können auftreten, da es gemäß Artikel 4 Absatz 3 den zuständigen nationalen Behörden obliegt, zu bewerten, ob die technischen Maßnahmen geeignet sind und ob sie angewendet werden.

III. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN IN DEN MITGLIEDSTAATEN

14. Die Artikel-29-Datenschutzgruppe hat den Stand der Umsetzung der neuen Vorschriften zur Verletzung des Schutzes personenbezogener Daten in den Rechtsvorschriften der Mitgliedstaaten überprüft. Diese Überprüfung ist in ihrem Umfang begrenzt (sie deckt nur die wichtigsten Bereiche ab) und basiert auf dem aktuellen Stand der Umsetzung. Die Situation ändert sich na-

[7] Eine solche Beeinträchtigung würde „nachteilige Auswirkungen“ im Sinne von Artikel 4 Absatz 3 Unterabsatz 2 (zusätzlich zu den in Erwägungsgrund 61 festgelegten Fällen, die immer nachteilige Auswirkungen haben) darstellen.

türlich. Deshalb sollten die Ergebnisse nur als Zwischenergebnisse angesehen werden, die Änderungen unterworfen sind. Jedes Mal, wenn Mitgliedstaaten Vorschriften zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation erlassen, wird das einen Einfluss auf die Ergebnisse haben. Im Folgenden werden die Ergebnisse zusammengefasst:

15. ***Stand der Umsetzung.*** Stichtag für die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation ist der 25. Mai 2011. Derzeit befinden sich die Mitgliedstaaten, in denen öffentliche Konsultationen durchgeführt werden, in der Minderheit. Die meisten Mitgliedstaaten haben erste Entwürfe ausgearbeitet, die wenigsten dieser Entwürfe haben allerdings den Stand von Gesetzesvorhaben erreicht. Bislang scheint noch kein Mitgliedstaat Rechtsvorschriften erlassen zu haben.

16. Im Prinzip bedeutet das, dass die Umsetzungsanstrengungen noch nicht sehr weit gediehen sind. Leider scheint es einer großen Anzahl von Mitgliedstaaten nicht möglich zu sein, die Frist einzuhalten.

17. ***Gemeinsame Kernelemente.*** Die Informationen, die die Datenschutzbehörden zu der Situation in den jeweiligen Mitgliedstaaten gesammelt haben, deuten darauf hin, dass sich die meisten Mitgliedstaaten bei der Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation sehr eng an den Wortlaut der Richtlinie halten. Im Einzelnen:

    a. **Definitionen.** Die meisten Mitgliedstaaten scheinen die Definitionen aus der Datenschutzrichtlinie für elektronische Kommunikation übernommen zu haben.

    b. **Kriterien für die Benachrichtigung von Einzelpersonen.** Die meisten Mitgliedstaaten scheinen die Kriterien übernommen zu haben. Einige Mitgliedstaaten haben jedoch Änderungen eingefügt. Die Tschechische Republik schlägt beispielsweise vor, „schwerwiegenden" hinzuzufügen; Schweden hat vorgeschlagen, eine Benachrichtigung verpflichtend zu machen, wenn sich die Verletzung „in einem größeren Ausmaß [auf die Teilnehmer oder Nutzer, deren Daten betroffen sind,] auswirkt."

18. ***Bereiche, in denen mit unterschiedlichen Vorgehensweisen zu rechnen ist.*** Die Angaben der Mitgliedstaaten zeigen, dass sich einige kleine Unterschiede in der Vorgehensweise ergeben haben. Sie werden nachfolgend aufgeführt.

    a. **Anwendungsbereich.** Trotz der Anreize, den Anwendungsbereich auf andere Akteure als die Anbieter elektronischer Kommunikationsdienste auszuweiten, haben die meisten Mitgliedstaaten dies nicht getan. Ausnahmen

sind Deutschland und Österreich. Das liegt allerdings daran, dass diese Mitgliedstaaten bereits Vorschriften für Verstöße gegen die Datenschutzvorschriften erlassen hatten, die sektorübergreifend anwendbar sind. Auch in anderen Mitgliedstaaten haben die nationalen Datenschutzbehörden als gute Praxis angeregt, sie und die betroffenen Personen grundsätzlich zu benachrichtigen. Dies ist zum Beispiel im Vereinigten Königreich und in Irland der Fall.

b. **Leitlinien:** Fast die Hälfte der Mitgliedstaaten, die Bestimmungen entworfen oder Rechtsvorschriften vorgeschlagen haben, sehen die Annahme von Leitlinien vor.

Verschiedene Stellen sind für die Annahme der Leitlinien zuständig. In den meisten Fällen werden damit die nationalen Datenschutzbehörden betraut (wie in Estland, Luxemburg, dem Vereinigten Königreich und möglicherweise auch Frankreich[8]) oder die nationalen Regulierungsbehörden für elektronische Kommunikation (Schweden und Finnland). In anderen Fällen wird die Zuständigkeit geteilt (Deutschland).

In den meisten Mitgliedstaaten entsprechen die Vorschriften über die Aspekte, die in den Leitlinien zu regeln sind, denen der Datenschutzrichtlinie für elektronische Kommunikation. In einigen Fällen werden jedoch weitere Aspekte erfasst. Dies ist in Estland der Fall (die nationale Datenschutzbehörde kann Ausnahmen von der Verpflichtung zur Benachrichtigung festlegen) und möglicherweise in Frankreich.[9] In einigen Fällen scheint der Umfang der Leitlinien noch unbestimmt zu sein (Italien) und in einigen Fällen scheint er eingeschränkter zu sein als in der Richtlinie. Die meisten zuständigen Behörden haben bislang noch keine Leitlinien entwickelt. Einige zuständige Behörden verfügten jedoch bereits über bewährte Verfahren oder Leitlinien (wie im Vereinigten Königreich, in Irland und Deutschland).

IV. ZUKÜNFTIGE MASSNAHMEN, DIE VON DEN ZUSTÄNDIGEN NATIONALEN BEHÖRDEN UND DER ARTIKEL-29-ARBEITSGRUPPE DURCHZUFÜHREN SIND

19. Die Bestandsaufnahme hat gezeigt, dass das Problembewusstsein und der Stand der Umsetzung der Benachrichtigungsverfahren im Fall einer Verletzung des Schutzes personenbezogener Daten von Land zu Land noch sehr

[8] Nach dem derzeitigen Stand der noch nicht abgeschlossenen Diskussionen: künftige Rechtsvorschriften können andere Regelungen enthalten.

[9] Siehe Fußnote 8.

unterschiedlich sind. Wie oben dargelegt, haben einige Mitgliedstaaten bereits Erfahrungen in diesem Bereich, während andere das noch nicht haben.

a) Einrichtung einer Plattform zur Sensibilisierung der Behörden für Sicherheitsverletzungsverfahren

20. Die Artikel-29-Datenschutzgruppe ist der Ansicht, dass Handlungsbedarf besteht, so dass alle nationalen Datenschutzbehörden auf den gleichen Stand gebracht werden. Zu diesem Zweck ist die Artikel-29-Datenschutzgruppe entschlossen, eine Untergruppe zu bilden, die als Plattform für einen Meinungs- und Wissensaustausch dienen soll. Das Ziel der Plattform ist die Förderung harmonisierter Verfahren und Konzepte, die bei Benachrichtigungen im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten in den Mitgliedstaaten anzuwenden sind.[10]

21. Anfänglich möchte sich die Artikel-29-Datenschutzgruppe dabei insbesondere auf die folgenden Bereiche konzentrieren (diese Liste kann sich je nach Bedarf ändern): *(i)* Schaffung eines Wissenspools in Bezug auf die Umstände, unter denen eine Benachrichtigung von Einzelpersonen erforderlich ist; *(ii)* Erstellung von Leitlinien in Bezug auf das Verfahren und den Zeitpunkt der Benachrichtigung (sowohl der nationalen Datenschutzbehörden als auch der betroffenen Personen); und *(iii)* Festlegung der Kriterien für die Bewertung der Wirksamkeit technischer Schutzmaßnahmen.

b) Koordinierung der Verfahren bei grenzüberschreitenden Datenschutzverletzungen

22. Darüber hinaus sollte die Plattform zur Koordinierung der Verfahren bei grenzüberschreitenden Datenschutzverletzungen herangezogen werden. Es wird erwartet, dass eine große Zahl von Datenschutzverletzungen einen grenzüberschreitenden Bezug haben wird. Der für die Verarbeitung der Daten Verantwortliche könnte zum Beispiel in einem Mitgliedstaat niedergelassen sein und die Verletzung ereignet sich aber in einem oder mehreren anderen Mitgliedstaaten, z. B. wenn ein Hacker dort in eine Anlage eingedrungen ist. Es könnte auch passieren, dass die am meisten betroffenen Personen nicht in dem Mitgliedstaat sind, in dem sich die Verletzung ereignet hat, oder dass sich die Datenschutzverletzung zeitgleich in mehreren Einrichtungen ereignet hat. In anderen Fällen könnte es unklar sein, wo sich die Datenschutzverletzung ereignet hat, während die Auswirkungen in vielen Mit-

[10] Es sei angemerkt, dass die Mitgliedstaaten selbst die zuständige nationale Behörde bestimmen, die die Anforderungen gemäß Artikel 3 der Rahmenrichtlinie erfüllen muss. Das heißt, dass in einigen Mitgliedstaaten die nationalen Datenschutzbehörden für die Entgegennahme der Meldung einer Verletzung des Schutzes personenbezogener Daten zuständig sein werden. In anderen könnten es dagegen andere Organe sein, wie beispielsweise die nationalen Regulierungsbehörden. Unabhängig davon gehen die nationalen Datenschutzbehörden davon aus, dass sie einbezogen werden.

gliedstaaten zu spüren sind. In allen diesen Fällen (und möglicherweise noch in anderen) könnte der Koordinierungsbedarf zwischen den zuständigen Behörden groß sein.

23. Daher ist die Artikel-29-Arbeitsgruppe entschlossen, Koordinierungsmaßnahmen einzuleiten. Dazu sollten zunächst untersucht werden, welche Rechtsvorschriften bei grenzüberschreitenden Verstößen gegen die Datenschutzvorschriften zur Anwendung kommen und welche Behörden zuständig sind. Das würde auch eine Prüfung der Informations- und Anzeigepflicht sowie die Schaffung der entsprechenden Verfahren mit sich bringen.

24. Die Plattform wird so bald wie möglich eingerichtet. Dies ist besonders hilfreich, da sie die Artikel-29-Datenschutzgruppe auch dabei unterstützen würde, Anregungen für Legislativmaßnahmen der EU im Zusammenhang mit Datenschutzverletzungen zu geben (siehe Abschnitte V und VI).

V. ZUKÜNFTIGE EU-LEGISLATIVMASSNAHMEN IN BEZUG AUF DIE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

25. Wie oben dargelegt, werden – nachfolgend näher beschrieben – in zweierlei Hinsicht legislative Entwicklungen im Bereich der Verletzung des Schutzes personenbezogener Daten erwartet.

26. Zunächst werden Entwicklungen bei der ***Datenschutzrichtlinie für elektronische Kommunikation*** erwartet. Diese Richtlinie gibt den umfassenden Rechtsrahmen für Verstöße gegen die Datenschutzvorschriften vor. Zur Sicherstellung einer einheitlichen Durchführung und Anwendung des Rahmens werden der Kommission Befugnisse übertragen (Artikel 4 Absatz 5). Diese Ermächtigung ist gerechtfertigt, um sicherzustellen, dass die Menschen unionsweit ein gleich hohes Schutzniveau genießen und dass Stellen, in denen es zu Sicherheitsverletzungen kommt, nicht mit unterschiedlichen Anzeigepflichten belastet sind. Die Befugnisse beziehen sich insbesondere auf die Umstände, das Format und die Verfahren für die Erteilung von Informationen und für Benachrichtigungen. Das sind die Bereiche, in denen die zuständigen nationalen Behörden zur Ausgabe von Leitlinien befugt sind.

27. Das Verfahren zur Annahme technischer Durchführungsmaßnahmen kann unter anderem wegen der Konsultationspflichten mehr als ein Jahr dauern[11]. Bevor die Kommission Maßnahmen annehmen kann, muss sie erst verschie-

[11] Das Verfahren umfasst die Vorbereitung der Maßnahmen (nach Konsultationen mit den Interessengruppen), die Stellungnahme des Ausschusses, das sich aus Vertretern der Mitgliedstaaten zusammensetzt, und die endgültige Annahme durch die Kommission. Das Europäische Parlament hat ein Mitspracherecht.

dene Stellen konsultieren. Gemäß Artikel 4 Absatz 5 sind dies insbesondere die ENISA, der Europäische Datenschutzbeauftragte und die Artikel-29-Datenschutzgruppe. Derselbe Artikel schreibt weiterhin vor, dass auch andere *relevante Interessengruppen* miteinbezogen werden, insbesondere um sich über die besten verfügbaren technischen und wirtschaftlichen Methoden für die Durchführung zu informieren.

28. ***Politikentwicklungen bezüglich der Datenschutzverletzungen wurden auch im Rahmen der Überprüfung der Richtlinie 95/46 angekündigt.*** Die Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation gab den Legislativorganen die Möglichkeit, Pflichten im Fall einer Datenschutzverletzung einzuführen. Angesichts des Anwendungsbereiches der besagten Richtlinie waren die Pflichten auf die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste beschränkt. Diese sektorspezifischen Vorschriften müssen jedoch ergänzt werden, indem auch alle für die Verarbeitung der Daten Verantwortlichen zur Benachrichtigung verpflichtet werden. Dies soll im Zusammenhang mit der Überprüfung der Richtlinie 95/46 geschehen. Die Mitteilung der Kommission „*Gesamtkonzept für den Datenschutz in der Europäischen Union*" hat die Ansicht der Kommission bestätigt, dass es wichtig ist, dass Personen informiert werden, wenn ihre Daten versehentlich oder unrechtmäßig gelöscht oder geändert werden, wenn sie verlorengegangen sind oder wenn Unbefugte darauf zugegriffen oder sie weitergegeben haben. Nach der Mitteilung beabsichtigt die Kommission eine Prüfung der Modalitäten für die Einführung einer Anzeigepflicht bei Datenschutzverstößen in der allgemeinen Datenschutzregelung, die alle Sektoren abdeckt und mit der Anzeigepflicht gemäß der Datenschutzrichtlinie für elektronische Kommunikation übereinstimmen sollte.[12]

29. Die Artikel-29-Datenschutzgruppe begrüßt dies, da sie davon überzeugt ist, dass sektorübergreifende Meldungen von Sicherheitsverletzungen dem Einzelnen helfen, die notwendigen Schritte für eine Begrenzung des möglichen, aus der Verletzung resultierenden Schadens zu unternehmen. Außerdem wird die Anzeigepflicht von Datenschutzverletzungen Unternehmen dazu anhalten, für mehr Datensicherheit zu sorgen, und ihre Rechenschaftspflicht stärken.

VI. EMPFEHLUNGEN FÜR ZUKÜNFTIGE ENTWICKLUNGEN BEI DER MELDUNG VON DATENSCHUTZVERLETZUNGEN

30. Nachdem sowohl die Situation in den Mitgliedstaaten (Abschnitt III) als auch die aktuelle Situation auf EU-Ebene (Abschnitte II und IV) analysiert wurde,

[12] Siehe Seiten 6 – 7 der Mitteilung der Kommission „*Gesamtkonzept für den Datenschutz in der Europäischen Union*", KOM(2010) 609 endgültig vom 4.11.2010.

möchte die Artikel-29-Datenschutzgruppe die folgenden Schlussfolgerungen und Empfehlungen formulieren:

Anwendungsbereich der Verpflichtung

31. Die Artikel-29-Datenschutzgruppe unterstützt die Einführung einer Pflicht zur Anzeige von Datenschutzverstößen in dem allgemeinen Rahmen, die auf alle für die Verarbeitung der Daten Verantwortlichen ausgeweitet wird. Die Rechtfertigungsgründe für diese Verpflichtung gelten auch vollumfänglich für andere für die Verarbeitung von Daten Verantwortliche als die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste. **Deshalb begrüßt es die Artikel-29-Datenschutzgruppe, dass die Kommission eine solche Ausweitung im Rahmen der Überprüfung der Richtlinie 95/46 in Betracht zieht.**

Kernelemente (Definitionen, Kriterien) der Rechtsvorschriften über Datenschutzverletzungen

32. Die meisten Mitgliedstaaten scheinen die Kernelemente der Sicherheitsverletzungsvorschriften der Datenschutzrichtlinie für elektronische Kommunikation in sehr ähnlicher Form zu übernehmen. Das umfasst die Definitionen, Kriterien und andere wichtige Punkte. Entsprechend wird erwartet, dass die zuständigen nationalen Behörden und relevanten Akteure bei Sicherheitsverletzungen zunehmend nach diesen Vorgaben vorgehen sollten. Diese Vorgaben und Verfahren werden sich deshalb in den nächsten Jahren in den EU-Mitgliedstaaten „verfestigen".

33. Dies lässt darauf schließen, dass **die Kommission** bei der Ausweitung der Verpflichtung auf andere Akteure, **auf dieselben oder auf sehr ähnliche Kernelemente bauen sollte wie in der Datenschutzrichtlinie für elektronische Kommunikation**. Das gilt für die Definition und insbesondere für die Kriterien für die Benachrichtigung der betroffenen Personen, wonach eine Benachrichtigung erforderlich ist, wenn anzunehmen ist, dass die Verletzung personenbezogener Daten die personenbezogenen Daten oder Personen in ihrer Privatsphäre beeinträchtigt.

34. Nachdem Erfahrungen bei der Anwendung dieser Kriterien gewonnen wurden, wäre es kontraproduktiv, auf andere für die Verarbeitung von Daten Verantwortliche als die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste andere Kriterien anzuwenden. Darüber hinaus wurden die spezifischen Vorschriften für den Fall der Verletzung des Schutzes personenbezogener Daten in der geänderten Datenschutzrichtlinie für elektronische Kommunikation während des Gesetzgebungsverfahrens, das der Annahme der Datenschutzrichtlinie für elektronische Kommunikation voraus-

ging, ausgiebig diskutiert. Bei dieser Debatte wurden die Stellungnahmen der Artikel-29-Datenschutzgruppe[13] und des Europäischen Datenschutzbeauftragten[14] zusammen mit den Ansichten anderer Interessengruppen berücksichtigt. Die Vorschriften, in die die Standpunkte der verschiedenen Interessengruppen eingeflossen sind, sind das Ergebnis eines Interessenausgleichs: einerseits bieten die Kriterien, die die Pflicht zur Benachrichtigung von Einzelpersonen auslösen, grundsätzlich einen angemessenen Schutz, andererseits stellen sie keine überzogenen oder unnötigen Anforderungen. Letztendlich ändert sich nichts an dem Sachverhalt der Verletzung personenbezogener Daten, ob nun der für die Verarbeitung der Daten Verantwortliche ein Transportunternehmen, eine Bank, ein Unternehmen oder eine Stelle des öffentlichen Sektors ist. Die Vorschriften müssen also dieselben sein, wenn die Bedingungen für alle gleich sein sollen. Dieser Ansatz scheint durch die Aussage der Kommission in der Mitteilung „*Gesamtkonzept für den Datenschutz in der Europäischen Union*" bestätigt zu werden, wonach es „*auch für diese Aspekte […] eines konsequenten kohärenten Ansatzes [bedarf]*", während gleichzeitig gesagt wird, dass die Datenschutzrichtlinie für elektronische Kommunikation nicht in die Prüfung einbezogen wird.

Übertragene Befugnisse/Durchführungsmaßnahmen

35. Viele Mitgliedstaaten beziehen sich auf die Vorschrift in der Datenschutzrichtlinie für elektronische Kommunikation, die es ihren zuständigen nationalen Behörden erlaubt, Leitlinien für die Umstände, das Format und die Verfahren vorzugeben, die auf die Informations- und Benachrichtigungspflicht anzuwenden sind. Das sind auch die Aspekte, die die Kommission mit Hilfe von Durchführungsmaßnahmen regeln könnte.

36. Die Artikel-29-Datenschutzgruppe empfiehlt einen harmonisierten Rahmen für den Fall der Verletzung des Schutzes personenbezogener Daten in allen Mitgliedstaaten. Dieser sollte ihrer Meinung nach auf den Erfahrungen der zuständigen nationalen Behörden aufbauen, die bereits mit Sicherheitsverletzungen befasst sind.

a) Zeitplanung

37. Angesichts des langwierigen Verfahrens zum Erlass von Durchführungsmaßnahmen und der vorgeschriebenen Konsultation der verschiedenen Interessengruppen, der ENISA, der Artikel-29-Datenschutzgruppe und des Euro-

[13] Siehe die vorgenannten Stellungnahmen 150 und 159 der Artikel-29-Datenschutzgruppe.

[14] Zweite Stellungnahme des Europäischen Datenschutzbeauftragten zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. C 128 vom 6.6.2009, S. 28.

päischen Datenschutzbeauftragten ***fordert die Artikel-29-Datenschutzgruppe die Kommission dazu auf, die Durchführungsmaßnahmen so bald wie möglich anzugehen***. Die Artikel-29-Datenschutzgruppe schlägt vor, dass die Kommission hierzu unter anderem eine Erhebung über die ersten Verfahren macht, die von den zuständigen Behörden entwickelt werden. Auf der Grundlage der Rückmeldungen soll sie dann Durchführungsmaßnahmen vorschlagen. Die Erfahrungen, die in den Mitgliedstaaten gesammelt werden, können sehr hilfreiche Anregungen geben. Es scheint besonders wichtig zu sein, die Umstände einheitlich festzulegen, unter denen alle relevanten Datenschutzverletzungen angezeigt werden, insbesondere in Bezug auf Einrichtungen, die in mehreren Mitgliedstaaten angesiedelt sind. Ein spätes Eingreifen würde das Risiko erhöhen, dass sich unterschiedliche Vorgehensweisen unter den Mitgliedstaaten verfestigen.

b) Inhalt

38. Auf der Grundlage des Rahmens der Datenschutzrichtlinie für elektronische Kommunikation empfiehlt die Artikel-29-Datenschutzgruppe der Kommission, in folgenden Bereichen von ihren übertragenen Befugnissen Gebrauch zu machen.

Erstens: Festlegung der Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten gemeldet werden muss. Dies erfordert die Präzisierung der Kriterien für die Benachrichtigung von Einzelpersonen. So könnte die Benachrichtigungspflicht beispielsweise grundsätzlich greifen, wenn sensible Daten verletzt wurden. Eine Harmonisierung in diesem Bereich ist insbesondere für Akteure wichtig, die in mehr als einem Mitgliedstaat tätig sind (d. h. es wäre nicht erstrebenswert, wenn die zuständigen Behörden einem Betreiber für dieselbe Verletzung des Schutzes personenbezogener Daten unterschiedliche Anforderungen zur Benachrichtigung stellen würden).

Zweitens: Festlegung der Vorgehensweise im Fall einer Datenschutzverletzung. Dazu könnten beispielsweise konkretere Fristen für die Meldung einer Verletzung an die Behörden gehören. Die Vorgehensweise könnte auch bestimmte Verfahrensschritte vorsehen, zum Beispiel die Überprüfung der Systemsicherheit oder die Hinzuziehung forensischer Ermittler zur Untersuchung der Fakten und Umstände der Datenschutzverletzung.

Drittens: Basierend auf den Erfahrungen der zuständigen nationalen Behörden, auch aus der Anwendung der Artikel 19, 20 und 21 der Richtlinie 95/46 fordert die Artikel-29-Datenschutzgruppe die Kommission dazu auf, EU-Standardmuster zu erstellen, die für die Benachrichtigung zu verwenden sind. Bei den Standardmustern an die zuständigen Behörden sollten zumin-

dest Kopfzeilen enthalten sein, d. h. Beschreibung der Verletzung, die Folgen, die unternommenen/vorgeschlagenen Maßnahmen, um den Behörden bei der Bewertung der Verletzung im Rahmen ihrer Kontrollbefugnisse zu helfen.

Viertens: Die Artikel-29-Datenschutzgruppe befürwortet die Festlegung der Modalitäten für die Zustellung der Benachrichtigung an Einzelpersonen im Wege von Durchführungsbefugnissen, wobei Leitlinien dazu herausgegeben werden sollten, ob eine Zustellung per E-Mail oder eine telefonische Benachrichtigung zuzulassen ist. Auch für die Fälle, in denen eine Benachrichtigung der Personen über die Presse usw. gestattet ist (wenn die Empfänger beispielsweise nicht bekannt sind), sollten Leitlinien verfasst werden. Dabei sollten die zuständigen Behörden Ermessensspielraum für die Beurteilung der jeweiligen Umstände haben.

Fünftens: Darüber hinaus sollte für das Format der Informationen zu Datenschutzverletzungen, die die Anbieter in einem Verzeichnis erfassen müssen, Leitlinien verfasst werden.[15]

Sechstens: Basierend auf den Erfahrungen, die die zuständigen Behörden in den Mitgliedstaaten sammeln, und aufgrund der Kommentare der in Artikel 4 Absatz 5 genannten Interessengruppen ersucht die Artikel-29-Datenschutzgruppe die Kommission, Leitlinien für die technischen Schutzmaßnahmen festzulegen, die bei entsprechender Anwendung eine Ausnahme von der Benachrichtigungspflicht begründen.

c) Anwendungsbereich

39. Schließlich ist die Artikel-29-Datenschutzgruppe der Ansicht, dass alle Durchführungsmaßnahmen, die gemäß der Datenschutzrichtlinie für elektronische Kommunikation entwickelt wurden, auch auf alle anderen für die Verarbeitung der Daten Verantwortlichen anwendbar sein sollen. Die Kommission sollte sich folglich nicht zu sektorspezifischen Maßnahmen verleiten lassen und sich stattdessen auf die Ausarbeitung von allgemein anwendbaren Maßnahmen konzentrieren. Doppelarbeit ist zu vermeiden.

Brüssel, den 5. April 2011

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

[15] Gemäß Artikel 4 Absatz 4 Unterabsatz 2 müssen die betroffenen Stellen ein Verzeichnis über die Verletzungen führen; die Angaben darin müssen ausreichend sein, damit die zuständigen Behörden die Einhaltung der Anzeigepflichten prüfen können.

Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (WP 185)

Angenommen am 16. Mai 2011

INHALT

1. Einleitung

2. Hintergrund: verschiedene Infrastrukturen für die Geolokalisierung
   2.1 Daten der Basisstation
   2.2 GPS-Technologie
   2.3 Wi-Fi
      2.3.1 Wi-Fi-Zugangspunkte

3. Gefahren für den Datenschutz

4. Rechtsrahmen
   4.1 Von Telekombetreibern verarbeitete Daten von Basisstationen
   4.2 Verarbeitung von Basisstations-, Wi-Fi- und GPS-Daten durch Anbieter von Diensten der Informationsgesellschaft
      4.2.1 Anwendbarkeit der geänderten Datenschutzrichtlinie für elektronische Kommunikation
      4.2.2 Anwendbarkeit der Datenschutzrichtlinie

5. Verpflichtungen aus Datenschutzgesetzen
   5.1 Für die Verarbeitung der Daten Verantwortliche
      5.1.1 Für die Verarbeitung Verantwortliche einer Infrastruktur für die Geolokalisierung
      5.1.2 Anbieter von Geolokalisierungsanwendungen und -diensten
      5.1.3 Entwickler des Betriebssystems
   5.2 Verantwortlichkeiten Dritter
   5.3 Berechtigter Grund
      5.3.1 Intelligente mobile Endgeräte
      5.3.2 Wi-Fi-Zugangspunkte
   5.4 Information
   5.5 Die Rechte der betroffenen Personen
   5.6 Aufbewahrungsfristen

6. Schlussfolgerungen

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

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

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

gestützt auf ihre Geschäftsordnung,

hat folgendes Dokument angenommen:

1. Einleitung

Geografische Informationen spielen eine wichtige Rolle in unserer Gesellschaft. Fast alle menschlichen Aktivitäten und Entscheidungen weisen eine geografische Komponente auf. Im Allgemeinen steigt der Wert einer Information, wenn sie mit einem Standort verbunden ist. Es können alle Arten von Informationen Bezug zu einem geografischen Standort haben, wie beispielsweise Finanzdaten, Gesundheitsdaten und andere Verhaltensdaten der Verbraucher. Durch die rasche technologische Entwicklung und die weitverbreitete Nutzung von intelligenten mobilen Endgeräten entsteht eine ganz neue Kategorie standortbezogener Dienste.

Mit Hilfe dieser Stellungnahme soll für Klarheit hinsichtlich des für Geolokalisierungsdienste geltenden Rechtsrahmens gesorgt werden, die auf intelligenten mobilen Endgeräten verfügbar sind und/oder durch diese generiert werden. Die betreffenden Endgeräte können eine Verbindung mit dem Internet erstellen oder sind mit Standortsensoren wie GPS ausgestattet. Beispiele für solche Dienste sind: Karten und Navigation, geopersonalisierte Dienste (einschließlich der Sehenswürdigkeiten der Umgebung), Augmented Reality, Georeferenzierung von Inhalten im Internet (Geotagging), Lokalisierung des Aufenthaltsortes von Freunden, Überwachung von Kindern und standortbezogene Werbung.

Die vorliegende Stellungnahme befasst sich auch mit den drei wichtigsten Arten der Infrastruktur, die zur Bereitstellung von Geolokalisierungsdiensten verwendet werden, nämlich GPS, GSM-Basisstationen und Wi-Fi. Hierbei wird besonderes Augenmerk auf die neue Infrastruktur gerichtet, die auf der Lokalisierung von Wi-Fi-Zugangspunkten basiert.

Es ist der Datenschutzgruppe sehr wohl bewusst, dass es noch viele andere Dienste gibt, die Standortdaten verarbeiten und ebenfalls zu datenschutzrecht-

lichen Bedenken führen können. Das reicht von elektronischen Ticketsystemen zu Mautsystemen für Autos und von Satellitennavigationsdiensten und der Standortbestimmung beispielsweise mit Hilfe von Kameras zur Geolokalisierung von IP-Adressen. Angesichts der raschen technologischen Entwicklung insbesondere im Hinblick auf das Kartografieren drahtloser Zugangspunkte, verbunden mit der Tatsache, dass neue Marktteilnehmer neue standortbezogene Dienste anbieten wollen, die auf einer Kombination aus Basisstation, GPS und Wi-Fi-Daten besteht, hat sich die Datenschutzgruppe entschieden, die rechtlichen Voraussetzungen gemäß der Datenschutzrichtlinie insbesondere für diese Dienste klarzustellen.

In der Stellungnahme wird zuerst die Technologie beschrieben, dann werden die Risiken für den Datenschutz herausgearbeitet und bewertet und schließlich werden Schlussfolgerungen gezogen zur Anwendbarkeit der einschlägigen Artikel auf die verschiedenen für die Verarbeitung Verantwortlichen, die Standortdaten von mobilen Endgeräten erheben und verarbeiten. Dazu gehören zum Beispiel Anbieter der Infrastruktur für die Geolokalisierung, Hersteller von Smartphones und die Entwickler von standortbezogenen Anwendungen.

Diese Stellungnahme bewertet nicht die spezielle Technologie zur Georeferenzierung, die mit dem sogenannten Web 2.0 verknüpft ist, bei dem Nutzer georeferenzierte Informationen in soziale Netzwerke wie Facebook oder Twitter integrieren. Die Stellungnahme wird auch einige andere Technologien zur Geolokalisierung nicht näher untersuchen, die verwendet werden, um Geräte innerhalb eines relativ kleinen Bereichs miteinander zu verbinden (Einkaufszentren, Flughäfen, Bürogebäude usw.), wie Bluetooth, ZigBee, Geofencing und Wi-Fi-basierte RFID-Etiketten. Dennoch gelten viele der Schlussfolgerungen, die in der vorliegenden Stellungnahme in Bezug auf berechtigte Gründe, Informationsrechte und die Rechte der betroffenen Person gezogen werden, auch für diese Technologien, wenn sie dazu genutzt werden, den geografischen Standort von Menschen über ihrer Endgeräte zu bestimmen.

2. Hintergrund: verschiedene Infrastrukturen für die Geolokalisierung

2.1 Daten der Basisstation

Das von den verschiedenen Telekommunikationsbetreibern abgedeckte Gebiet ist in Bereiche aufgeteilt, die gemeinhin als Zellen bekannt sind. Um ein Mobiltelefon nutzen oder eine Verbindung mit dem Internet über die 3G-Kommunikation aufbauen zu können, muss das mobile Endgerät eine Verbindung mit der Antenne (im Folgenden: Basisstation) aufnehmen, die diese Zelle abdeckt. Die Zellen decken Bereiche unterschiedlicher Größe ab. Das hängt von den Interferenzen beispielsweise mit Bergen oder hohen Gebäuden ab.

Immer, wenn ein mobiles Endgerät angeschaltet ist, ist es mit einer bestimmten Basisstation verbunden. Der Telekombetreiber zeichnet diese Verbindungen ständig auf. Jede Basisstation hat eine eindeutige ID und ist unter einem bestimmten Standort registriert. Sowohl der Telekombetreiber als auch viele mobile Endgeräte können die Signale sich überschneidender Zellen nutzen (benachbarte Basisstationen), um so den Standort des mobilen Endgeräts mit steigender Genauigkeit zu schätzen. Diese Technik wird auch Triangulation genannt.

Die Genauigkeit kann durch Informationen wie RSSI (Received Signal Strength Indicator), TDOA (Time Difference of Arrival) und AOA (Angle Of Arrival) weiter vergrößert werden.

Die Daten von Basisstationen können auf innovative Weise genutzt werden, beispielsweise zum Aufspüren von Verkehrsstaus. Auf jeder Straße gibt es für jeden Tagesabschnitt eine bestimmte Durchschnittsgeschwindigkeit. Wenn es länger als erwartet dauert, bis das Endgerät das Gebiet der benachbarten Basisstation erreicht, liegt offensichtlich ein Verkehrsstau vor.

Zusammenfassend lässt sich sagen, dass diese Methode der Standortbestimmung eine schnelle, grobe Standortangabe ermöglicht, jedoch verglichen mit GPS und Wi-Fi-Daten nicht sehr genau ist. Die Genauigkeit beträgt in eng besiedelten Stadtgebieten ungefähr 50 Meter, in ländlichen Gebieten aber bis zu einigen Kilometern.

2.2 GPS-Technologie

In intelligente mobile Endgeräte sind Chipsätze mit GPS-Empfängern eingebaut, die ihren Standort bestimmen.

Bei der GPS-Technologie (Satellitennavigationssystem) werden 31 Satelliten verwendet, die alle in einem der sechs verschiedenen Orbits um die Erde kreisen.[1] Jeder Satellit sendet ein sehr genaues Funksignal.

Das mobile Endgerät kann seinen Standort bestimmen, wenn der GPS-Sensor mindestens vier dieser Signale auffängt. Anders als bei den Daten der Basisstationen geht das Signal nur in eine Richtung. Die die Satelliten betreibenden Einrichtungen können nicht nachverfolgen, welche Endgeräte das Funksignal empfangen haben.

---

[1] Das Satellitennavigationssystem besteht aus Satelliten, die von den Vereinigten Staaten von Amerika aus militärischen Zwecken in die Umlaufbahn gebracht wurden. Die Europäische Kommission plant den Start von Galileo bis 2014. Galileo ist ein Netzwerk aus 18 Satelliten, die eine freie, nichtmilitärische Satellitennavigation ermöglichen. Die ersten zwei Satelliten sollen 2011 in die Umlaufbahn gebracht werden und zwei weitere in 2012. Quelle: European Commission, „Commission presents midterm review of Galileo and EGNOS“, 25. Januar 2011, URL:
http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&it em_id=4835

Mit Hilfe der GPS-Technologie kann die Position mit einer Genauigkeit von vier bis 15 Metern bestimmt werden. Der größte Nachteil von GPS ist der relativ langsame Start.[2] Ein weiterer Nachteil ist, dass es in Gebäuden nicht oder nur schlecht funktioniert. Deshalb wird die GPS-Technologie in der Praxis häufig mit Daten von Basisstationen und/oder kartografierten Wi-Fi-Zugangspunkten kombiniert.

2.3 Wi-Fi

2.3.1 Wi-Fi-Zugangspunkte

Die Verwendung von Wi-Fi-Zugangspunkten ist eine relative neue Quelle für Informationen zur Geolokalisierung. Die Technologie ähnelt der Verwendung von Basisstationen. Sie stützen sich beide auf eine eindeutige ID (von der Basisstation oder dem Wi-Fi-Zugangspunkt), die von einem mobilen Endgerät aufgespürt werden kann und zu einem Dienst gesendet wird, der für jede eindeutige ID den Standort hat.

Die MAC-Adresse (Medium Access Control) ist die eindeutige ID jedes Wi-Fi-Zugangspunktes. Die Mac-Adresse ist eine eindeutige, einer Netzwerkschnittstelle zugewiesene ID. Sie ist üblicherweise in der Hardware hinterlegt, wie Speicherchips und/oder Netzwerkkarten in Computern, Telefonen, Laptops oder Zugangspunkten.[3]

Wi-Fi-Zugangspunkte können als Quelle für die Geolokalisierung herangezogen werden, da sie ihre Verfügbarkeit ständig anzeigen. Die meisten Breitband Internet-Zugangspunkte verfügen standardmäßig auch über eine Wi-Fi-Antenne. Die Standard-Einstellung der am häufigsten genutzten Zugangspunkte in Europa für diese Verbindung ist „an“, auch wenn der Nutzer seine(n) Computer nur mit Kabeln mit dem Zugangspunkt verbunden hat. Gleich einem Radio sendet der Wi-Fi-Zugangspunkt selbst dann ständig seinen Netzwerknamen und seine MAC-Adresse, wenn niemand die Verbindung nutzt und selbst wenn die Inhalte der drahtlosen Kommunikation mit WEP, WPA oder WPA2 verschlüsselt sind.

Es gibt zwei verschiedene Wege, die MAC-Adressen von Wi-Fi-Zugangspunkten zu sammeln:[4]

---

[2] Um die Erkennung des ersten GPS-Signals zu beschleunigen, können sogenannte Rainbow Tables mit den erwarteten Positionen der verschiedenen Satelliten in den nächsten Wochen vorgeladen werden.

[3] Ein Beispiel für eine MAC-Adresse: 00-1F-3F-D7-3C-58. Die MAC-Adresse eines Wi-Fi-Zugangspunktes wird BSSID (Basic Service Set Identifier) genannt.

[4] Aktives und passives Scannen wurden in der IEEE 802.11 standardisiert, um Zugangspunkte zu finden.

1. Aktives Scannen: Versenden von aktiven Abfrage-Paketen[5] an alle Wi-Fi-Zugangspunkte in der Umgebung und Aufzeichnen der Antworten. Diese Antworten enthalten keine Informationen über die mit dem Wi-Fi-Zugangspunkt verbundenen Endgeräte.

2. Passives Scannen: Verzeichnen der regelmäßigen Beacon-Frames, die jeder Zugangspunkte sendet (üblicherweise zehnmal je Sekunde). Als eine nicht dem Standard entsprechende Alternative zeichnen einige Geräte alle von den Zugangspunkten übermittelten Wi-Fi-Frames auf, einschließlich derjenigen, die keine Beacon-Signale übertragen. Wenn diese Art Scannen ohne die richtige Anwendung des eingebauten Datenschutzes (Privacy by Design) durchgeführt wird, kann es zur Erhebung von Daten führen, die zwischen Zugangspunkten und den mit ihnen verbundenen Geräten ausgetauscht werden. Auf diese Weise könnten die MAC-Adressen von Desktop-Computern, Laptops und Druckern aufgezeichnet werden. Diese Art von Scannen könnte auch zur rechtswidrigen Aufzeichnung des Inhalts der Mitteilungen führen. Die Inhalte sind leicht lesbar, wenn der Inhaber eines Wi-Fi-Zugangspunktes keine Wi-Fi-Verschlüsselung (WEP/WPA/ WPA2) ermöglicht hat.

Der Standort eines Wi-Fi-Zugangspunktes kann auf zwei verschiedene Arten berechnet werden:

1. Statisch/einmal: die für die Verarbeitung Verantwortlichen sammeln die Mac-Adressen von Wi-Fi-Zugangspunkten selbst, indem sie mit Fahrzeugen herumfahren, die mit Antennen ausgestattet sind. Sie zeichnen den genauen Breiten- und Längengrad des Fahrzeuges zu dem Zeitpunkt auf, wenn das Signal eingefangen wird. So können sie den Standort der Zugangspunkte unter anderem anhand der Signalstärke errechnen.

2. Dynamisch/ständig: die Nutzer von Geolokalisierungsdiensten sammeln automatisch die MAC-Adressen, die ihre Wi-Fi-fähigen Geräte empfangen, wenn sie beispielsweise eine Online-Karte nutzen, um ihre Position zu bestimmen (Wo bin ich?). Das mobile Endgerät sendet dann dem Anbieter der Geolokalisierungsdienste alle verfügbaren Informationen zu, einschließlich der MAC-Adressen, der SSIDs und der Signalstärke. Der für die Verarbeitung Verantwortliche kann diese ständigen Beobachtungen dazu nutzen, den Standort der Wi-Fi-Zugangspunkte zu berechnen oder deren Berechnung in seiner Datei mit den kartografierten Wi-Fi-Zugangspunkten zu verbessern.

Es muss angemerkt werden, dass mobile Endgeräte keine Verbindung mit den Wi-Fi-Zugangspunkten aufnehmen müssen, um Wi-Fi-Informationen zu sam-

[5] Zum Sammeln der MAC-Adressen sendet der Sammler einen Probe-Request-Frame an alle Zugangspunkte.

meln. Sie spüren Zugangspunkte (im aktiven oder passiven Scannermodus) automatisch auf und sammeln automatisch Daten über sie.

Darüber hinaus senden Mobiltelefone, die eine Geolokalisierung erfragen, nicht nur Wi-Fi-Daten sondern oft auch andere Standortinformationen, über die sie verfügen, einschließlich GPS- und Basisstationsdaten. Das ermöglicht es dem Anbieter, den Standort „neuer" Wi-Fi-Zugangspunkte zu berechnen und/oder die bestehenden Berechnungen der Wi-Fi-Zugangspunkte zu verbessern, die bereits in der Datenbank verzeichnet sind. Auf diese Weise wird die Erhebung von Informationen über Wi-Fi-Zugangspunkte auf eine sehr wirksame Weise dezentralisiert, ohne dass dies den Kunden unbedingt bewusst ist.

Zusammenfassung: die Geolokalisierung auf der Basis von Wi-Fi-Zugangspunkten ermöglicht eine schnelle und basierend auf ständigen Messungen, immer genauere Positionsbestimmung.

3. Gefahren für den Datenschutz

Ein intelligentes mobiles Endgerät ist sehr eng mit einer bestimmten Person verbunden. Die meisten Menschen neigen dazu, ihr Mobiltelefon dicht bei sich zu tragen – von der Hosentasche oder Tasche zum Nachttisch an ihrem Bett.

Es kommt selten vor, dass ein solches Gerät an eine andere Person verliehen wird. Den meisten Menschen ist es bewusst, dass ihr mobiles Endgerät eine Reihe von sehr persönlichen Informationen enthält, von E-Mails zu privaten Bildern und vom Browserverlauf beispielsweise zu einer Kontaktliste.

Dies ermöglicht es den Anbietern von auf der Geolokalisierung basierenden Diensten, einen persönlichen Überblick über die Gewohnheiten und Muster der Inhaber solcher Endgeräte zu bekommen und umfassende Profile zu erstellen. Von dem Muster der Inaktivität bei Nacht können Rückschlüsse auf den Schlafplatz gezogen werden und aus einem regelmäßigen Reisemuster am Morgen kann der Standort des Arbeitgebers geschlossen werden. Das Muster kann auch Daten umfassen, die basierend auf dem sogenannten *Social Graph*[6] aus den Bewegungsmustern der Freunde erschlossen werden.

Ein Verhaltensmuster kann *besondere Datenkategorien* enthalten, wenn es zum Beispiel Besuche im Krankenhaus oder an religiösen Orten aufzeigt oder die Anwesenheit bei politischen Demonstrationen oder an bestimmten anderen Orten,

[6] Der Begriff „Social Graph" weist auf die Sichtbarkeit von Freunden in sozialen Netzwerken hin sowie auf die Möglichkeiten, Verhaltensmerkmale anhand der Daten über diese Freunde zu erschließen.

die Daten zum Beispiel über das Sexualleben offenbaren. Diese Profile können für Entscheidungen herangezogen werden, die den Inhaber massiv beeinträchtigen.

Die Technologie von intelligenten mobilen Endgeräten ermöglicht die ständige Überwachung von Standortdaten. Smartphones können ständig Signale von Basisstationen und Wi-Fi-Zugangspunkten sammeln. Technisch ist es möglich, die Überwachung im Geheimen durchzuführen, ohne den Inhaber zu informieren. Die Überwachung kann auch im Halbgeheimen erfolgen, wenn die Leute „vergessen" oder nicht richtig darüber informiert werden, dass die Dienste zur Standortbestimmung „eingeschaltet" sind oder wenn die Zugangseinstellungen der Standortdaten von „privat" auf „öffentlich" verstellt werden.

Selbst wenn Personen ihre Standortdaten im Internet bewusst über Aufenthaltsort- und Georeferenzierungsdienste verfügbar machen, schafft der uneingeschränkte globale Zugang neue Probleme, die von Datendiebstahl zu Einbrüchen und sogar zu körperlichen Angriffen und Stalking führen.

Wie bei anderen neuen Technologien auch, liegt ein großes Risiko in Bezug auf die Nutzung der Standortdaten in der schleichenden Ausweitung der Zweckbestimmung. Das heißt, dass basierend auf der Verfügbarkeit eines neuen Datentyps neue Zweckbestimmungen entwickelt werden, die zum Zeitpunkt der ursprünglichen Erhebung der Daten nicht vorhergesehen wurden.

4. Rechtsrahmen

Die Datenschutzrichtlinie (95/46/EG) ist der einschlägige Rechtsrahmen. Sie findet in jedem Fall Anwendung, in dem personenbezogene Daten als Folge der Verarbeitung von Standortdaten verarbeitet werden. Die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung) findet nur auf die Verarbeitung von Daten der Basisstation von öffentlichen elektronischen Kommunikationsdiensten und -netzen (Telekombetreiber) Anwendung.

4.1 Von Telekombetreibern verarbeitete Daten von Basisstationen

Telekombetreiber verarbeiten im Rahmen der Bereitstellung von öffentlichen elektronischen Kommunikationsdiensten[7] ständig Daten von Basisstationen. Sie können dies auch tun, um Dienste mit Zusatznutzen bereitzustellen. Dieser Fall wurde bereits von der Datenschutzgruppe in der Stellungnahme 5/2005 (WP 115)

[7] Merke, dass die Bereitstellung von öffentlichen Wi-Fi-Hotspots durch Telekombetreiber auch als öffentlicher elektronischer Kommunikationsdienst gilt und deshalb vorrangig die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation erfüllen sollte.

behandelt. Obwohl einige der Beispiele in der Stellungnahme durch die ausgeweitete Nutzung der Internettechnologie und der Sensoren in immer kleineren Endgeräten zwangsläufig überholt sind, bleiben die rechtlichen Schlussfolgerungen und Empfehlungen aus dieser Stellungnahme in Bezug auf die Verwendung der Daten von Basisstationen gültig.

1. Da sich Standortdaten von Basisstationen auf bestimmte oder bestimmbare Personen beziehen, unterliegen sie den Bestimmungen zum Schutz personenbezogener Daten, die in der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 niedergelegt sind.

2. Die Richtlinie 2002/58/EG vom 12. Juli 2002 (in der durch die Richtlinie 2009/136/EG geänderten Fassung) ist gemäß der Definition in Artikel 2 Buchstabe c dieser Richtlinie ebenfalls anzuwenden:

   „Standortdaten" Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

Wenn ein Telekombetreiber einen hybriden Geolokalisierungsdienst anbietet, der auch auf der Verarbeitung anderer Arten von Standortdaten wie GPS oder Wi-Fi-Daten basiert, gilt diese Tätigkeit als öffentlicher elektronischer Kommunikationsdienst. Der Telekombetreiber muss die vorherige Einwilligung seiner Kunden sicherstellen, wenn er diese Geolokalisierungsdaten Dritten anbietet.

4.2 Verarbeitung von Basisstations-, Wi-Fi- und GPS-Daten durch Anbieter von Diensten der Informationsgesellschaft

4.2.1 Anwendbarkeit der geänderten Datenschutzrichtlinie für elektronische Kommunikation

Typischerweise sind Unternehmen, die Lokalisierungsdienste und -anwendungen anbieten, die auf einer Kombination von Basisstations-, GPS- und Wi-Fi-Daten basieren, Anbieter von *Diensten der Informationsgesellschaft*. Als solche sind sie aufgrund der strengen Definition von elektronischen Kommunikationsdiensten ausdrücklich von der Datenschutzrichtlinie für elektronische Kommunikation ausgeschlossen (Artikel 2 Absatz c der geänderten Rahmenrichtlinie (unverändert).[8]

[8] Richtlinie 2002/21/EG vom 7. März 2002, Artikel 2 Buchstabe c: *„elektronische Kommunikationsdienste": gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;*

Die Datenschutzrichtlinie für elektronische Kommunikation findet keine Anwendung auf die Verarbeitung von Standortdaten durch Dienste der Informationsgesellschaft, selbst wenn eine solche Verarbeitung über ein öffentliches elektronisches Kommunikationsnetz erfolgt. Ein Nutzer kann sich entscheiden, GPS-Daten über das Internet zu übermitteln, zum Beispiel, wenn er Navigationsdienste des Internets nutzt. In diesem Fall wird das GPS-Signal unabhängig von dem GSM-Netzwerk in die Anwendungsebene der Internetkommunikation übertragen. Der Anbieter des Telekommunikationsdienstes fungiert als reiner Kanal. Er kann ohne sehr einschneidende Methoden wie *Deep Packet Inspection* keinen Zugang zu GPS-und/oder Wi-Fi- und/oder Basisstationsdaten erhalten, die von und zu einem intelligenten mobilen Endgerät zwischen einem Nutzer/Teilnehmer und einem Dienst der Informationsgesellschaft gesendet werden.

4.2.2 Anwendbarkeit der Datenschutzrichtlinie

Ist die geänderte Datenschutzrichtlinie für elektronische Kommunikation nicht anwendbar, findet gemäß Artikel 1 Absatz 2 die Richtlinie 95/46/EG Anwendung: „*Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar*."

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

Erwägungsgrund 26 der Richtlinie legt besondere Betonung auf den Begriff „bestimmbar". Es steht zu lesen: „*Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen*."

Erwägungsgrund 27 der Richtlinie legt den breiten Geltungsbereich des Schutzes dar: „*In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden*."

In ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" hat die Datenschutzgruppe umfangreiche Leitlinien zur Definition personenbezogener Daten bereitgestellt.

Intelligente mobile Endgeräte
Intelligente mobile Endgeräte sind untrennbar mit natürlichen Personen verbunden. Normalerweise liegt eine direkte und indirekte Identifizierbarkeit vor.

Erstens hat der, den GSM- und mobilen Internetzugang bereitstellende Telekombetreiber üblicherweise ein Verzeichnis mit dem Namen, der Adresse und Bankverbindung jedes Kunden zusammen mit verschiedenen Kennnummern des Geräts wie IMEI und IMSI.

Zweitens wird für den Kauf zusätzlicher Software für das Endgerät (*Anwendungen oder Apps*) gewöhnlicherweise eine Kreditkartennummer benötigt. Dadurch wird die Kombination aus Kennnummer(n) und Standortdaten um Daten zur direkten Identifizierung bereichert.

Indirekte Identifizierbarkeit kann durch eine Kombination aus Kennnummer(n) des Endgeräts in Verbindung mit einem oder mehreren errechneten Standort/en erzielt werden.

Jedes intelligente mobile Endgerät hat zumindest ein Kennzeichen, die MAC-Adresse. Das Endgerät kann noch andere eindeutige Identifikationsnummer haben, die von dem Entwickler des Betriebssystems hinzugefügt wurden. Diese Kennzeichen können im Zusammenhang mit Geolokalisierungsdiensten übermittelt und weiter verarbeitet werden. Es ist eine Tatsache, dass der Standort eines bestimmten Gerätes sehr präzise bestimmt werden kann, insbesondere wenn die verschiedenen Infrastrukturen zur Geolokalisierung kombiniert werden. Ein solcher Standort kann auf ein Haus oder einen Arbeitgeber hinweisen. Insbesondere durch wiederholte Beobachtungen ist es möglich, den Inhaber des Endgeräts zu identifizieren.

Bei der Berücksichtigung der verfügbaren Mittel zur Identifizier muss die Entwicklung berücksichtigt werden, dass die Menschen dazu tendieren, immer mehr persönliche Standortdaten im Internet bekannt zu geben, indem sie beispielsweise den Standort ihres Wohn- oder Arbeitsplatzes zusammen mit anderen Identifizierungsdaten angeben. Eine solche Offenlegung kann auch ohne ihr Wissen erfolgen, wenn sie von anderen Leuten mit geografischen Tags versehen werden. Diese Entwicklung macht es einfacher, einen Standort oder ein Verhaltensmuster mit einer spezifischen Person in Verbindung zu bringen.

Gemäß Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ sollte auch angemerkt werden, dass es in dem oben beschriebenen Kontext ein Kennzeichen möglich macht, den Nutzer eines spezifischen Endgeräts ausfindig zu machen und Rückschlüsse über ihn zu ziehen, selbst wenn sein wirklicher Name nicht bekannt ist.

Wi-Fi-Zugangspunkte
Diese indirekte Identifizierbarkeit trifft auch auf Wi-Fi-Zugangspunkte zu.[9] Die MAC-Adresse eines Wi-Fi-Zugangspunktes in Verbindung mit seinem berechneten Standort ist untrennbar verbunden mit dem Standort des Inhabers dieses Zugangspunktes.

Basierend auf der Signalstärke und den ständigen Aktualisierungen des Standortes durch die Nutzer seines Geolokalisierungsdienstes kann ein vernünftig ausgestatteter, für die Verarbeitung Verantwortlicher einen in zunehmendem Maße genauen Standort eines Wi-Fi-Zugangspunktes berechnen.

Mit Hilfe dieser Mittel kann häufig eine kleine Gruppe von Wohnungen oder Häusern identifiziert werden, in denen der Inhaber eines Zugangspunktes lebt. Wie leicht es ist, diesen Inhaber mit Hilfe der MAC-Adresse zu identifizieren, hängt von der Umgebung ab:

- In dünn besiedelten Gebieten, in denen die MAC-Adresse auf ein einziges Haus hinweist, kann der Inhaber des Hauses direkt mit Hilfe von Grundbüchern, Telefonbüchern, Wählerverzeichnissen oder sogar anhand einer einfachen Suchmaschinenabfrage bestimmt werden.[10]

- In dichter besiedelten Gebieten ist es möglich, mit Hilfe der Signalstärke und/oder SSID (die jeder mit einem Wi-Fi-fähigen Gerät aufspüren kann) den genauen Standort des Zugangspunktes zu ermitteln. So kann häufig die Identität der Person/en festgestellt werden, die an dem genauen Ort (Haus oder Wohnung) lebt/leben, an dem sich der Zugangspunkt befindet.

- In sehr dicht besiedelten Gebieten weist die MAC-Adresse selbst mit Hilfe der Informationen über die Signalstärke auf mehrere Wohnungen hin, in denen sich der Zugangspunkt möglicherweise befindet. In diesen Fällen ist es ohne unvertretbaren Aufwand nicht möglich, genau festzustellen, wer in der Wohnung lebt, in der der Zugangspunkt ermittelt wurde.

Die Tatsache, dass es in einigen Fällen derzeit nicht möglich ist, den Inhaber eines Endgeräts ohne unvertretbaren Aufwand zu ermitteln, ändert nichts an der generellen Schlussfolgerung, dass die Kombination einer MAC-Adresse und einem WI-Fi-Zugangspunkt mit seinem berechneten Standort als personenbezogene Daten zu behandeln ist.

[9] Wi-Fi-Zugangspunkte können sogar direkt identifizierbar sein, wenn der Anbieter des Internetzugangs ein Verzeichnis aller MAC-Adressen der Wi-Fi-Router führt, die er für seine identifizierten Kunden bereithält.

[10] Die Verfügbarkeit solcher Register oder Verzeichnisse unterscheidet sich von Mitgliedstaat zu Mitgliedstaat.

Unter diesen Umständen und angesichts der Tatsache, dass es unwahrscheinlich ist, dass der für die Verarbeitung Verantwortliche dazu in der Lage ist, zwischen Fällen zu unterschieden, in denen der Inhaber eines Wi-Fi-Zugangspunktes identifizierbar ist und solchen, in denen er es nicht ist, sollte der für die Verarbeitung Verantwortliche alle Daten über Wi-Fi-Router als personenbezogene Daten behandeln.

Es muss daran erinnert werden, dass der Zweck der Verarbeitung dieser Geolokalisierungsdaten nicht die Identifizierung der Nutzer sein muss. Ob es ohne unverhältnismäßigen Aufwand möglich ist, die Inhaber von Wi-Fi-Zugangspunkten zu ermitteln, hängt stark von den technischen Möglichkeiten des für die Verarbeitung Verantwortlichen oder jeder sonstigen Person ab, die die Inhaber ermitteln möchte.

5. Verpflichtungen aus Datenschutzgesetzen

5.1 Für die Verarbeitung der Daten Verantwortliche

Im Zusammenhang mit Geolokalisierungsdiensten, die von Diensten der Informationsgesellschaft bereitgestellt werden, können drei Funktionsbereiche mit unterschiedlichen Verantwortlichkeiten in Bezug auf die Verarbeitung personenbezogener Daten unterschieden werden. Diese sind: der für die Verarbeitung einer Infrastruktur für die Geolokalisierung Verantwortliche; der Anbieter einer bestimmten Anwendung oder eines bestimmten Dienstes zur Geolokalisierung und der Entwickler des Betriebssystems eines intelligenten mobilen Endgeräts. In der Praxis übernehmen Unternehmen häufig viele Rollen zur selben Zeit, beispielsweise, wenn sie ein Betriebssystem mit einer Datenbank mit kartografierten Wi-Fi-Zugangspunkten und einer Werbeplattform verbinden.

5.1.1 Für die Verarbeitung Verantwortliche einer Infrastruktur für die Geolokalisierung

Ähnlich den Telekombetreibern bei der Verarbeitung des Standortes eines spezifischen Endgeräts mit Hilfe der Basisstationen, verarbeiten die Inhaber von Datenbanken mit kartografierten Wi-Fi-Zugangspunkten personenbezogene Daten, wenn sie den Standort eines bestimmten intelligenten mobilen Endgeräts errechnen. Da sie beide die Zwecke und die Mittel dieser Verarbeitung bestimmen, sind sie beide für die Verarbeitung Verantwortliche im Sinne der Definition von Artikel 2 Buchstabe d der Datenschutzrichtlinie.

Es muss betont werden, dass das spezielle Endgerät entscheidend für die Berechnung seines Standortes ist, indem es seine eigenen Standortdaten (oft eine Kombination aus GPS, Wi-Fi und Basisstation) und die eindeutigen IDs von nahege-

legenen Wi-Fi-Zugangspunkten an den Inhaber der Datenbank übermittelt.[11] Ein solches Gerät erfüllt auch das Kriterium von Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie, *Mittel, die im Hoheitsgebiet eines Mitgliedstaates belegen sind*.

Da die MAC-Adresse eines Wi-Fi-Zugangspunktes in Kombination mit seinem errechneten Standort als personenbezogene Daten behandelt werden sollte, führt die Erhebung dieser Daten auch zur Verarbeitung personenbezogener Daten. Ungeachtet der Art, auf die diese Daten erhoben werden (einmalig oder ständig) sollte der Eigentümer einer solchen Datenbank die Verpflichtungen aus der Datenschutzrichtlinie erfüllen.

5.1.2 Anbieter von Geolokalisierungsanwendungen und -diensten

Intelligente mobile Endgeräte ermöglichen die Installation von Software Dritter, sogenannter *Anwendungen*. Solche Anwendungen können die Standortdaten (und andere Daten) von einem intelligenten mobilen Endgerät unabhängig von dem Entwickler des Betriebssystems und/oder dem für die Verarbeitung der Infrastruktur für die Geolokalisierung Verantwortlichen verarbeiten.

Beispiele solcher Dienste sind: Wettervorhersagen für die Regenwahrscheinlichkeit in den nächsten paar Stunden in einer ganz bestimmten Region; Dienste, die Informationen über nahegelegene Geschäfte anbieten; Dienste, die die Identifizierung eines verlorenen Mobiltelefons anbieten oder die den Standort von Freunden anzeigen.

Der Anbieter einer Anwendung, die zur Verarbeitung von Standortdaten fähig ist, ist der für die Verarbeitung der personenbezogenen Daten Verantwortliche, die aus der Installation und der Verwendung der Anwendung resultieren.

Natürlich ist es nicht immer erforderlich, gesonderte Software auf einem intelligenten mobilen Endgerät zu installieren. Viele Dienste zur Geolokalisierung sind auch über einen Browser zugänglich. Ein Beispiel hierfür ist die Nutzung einer Online-Karte, die eine Person durch eine Stadt führt.

5.1.3 Entwickler des Betriebssystems

Der Entwickler des Betriebssystems eines intelligenten mobilen Endgeräts kann ein für die Verarbeitung der Standortdaten Verantwortlicher sein, wenn das Endgerät direkt mit dem Nutzer interagiert und personenbezogene Daten erhebt (bei-

[11] Das mobile Endgerät kann die verschiedenen Standortdaten, die es empfängt, übermitteln, damit der für die Verarbeitung Verantwortliche den Standort des Endgeräts berechnen kann oder damit es seinen Standort selbst berechnen kann. In beiden Fällen ist das Gerät ein wesentliches Mittel für die Verarbeitung.

spielsweise durch das Anfordern einer Erstregistrierung als Nutzer und/oder durch die Erhebung von Standortinformationen zur Verbesserung der Dienste). Als ein für die Verarbeitung Verantwortlicher muss der Entwickler die Grundsätze des eingebauten Datenschutzes anwenden, um eine heimliche Überwachung entweder durch das Endgerät selbst oder durch verschiedene Anwendungen und Dienste zu verhindern.

Ein Entwickler ist auch der für die Verarbeitung der Daten Verantwortliche, die er verarbeitet, wenn das Endgerät eine Phone-Home-Funktion für seinen Aufenthaltsort hat. Da in diesem Fall der Entwickler über die Mittel und Zwecke des Datenstroms entscheidet, ist er der für die Verarbeitung dieser Daten Verantwortliche. Ein verbreitetes Beispiel einer solchen „Phone-Home-Funktion" ist die automatische Bereitstellung von Zeitzonen-Aktualisierungen basierend auf dem Standort.

Außerdem ist der Entwickler ein für die Verarbeitung Verantwortlicher, wenn er eine Werbeplattform anbietet und/oder eine Web-Shop-ähnliche Umgebung für Anwendungen und wenn das Gerät dazu in der Lage ist, personenbezogene Daten aus der Installation und Verwendung von Anwendungen zur Geolokalisierung unabhängig von dem Anbieter der Verwendung zu verarbeiten.

5.2 Verantwortlichkeiten Dritter

Es gibt zahlreiche Dritte, die Online tätig sind und die (weitere) Verarbeitung der Standortdaten ermöglichen. Dazu gehören Browser, soziale Netzwerke oder Kommunikationsmedien, die beispielsweise die „Georeferenzierung" ermöglichen. Wenn sie auf ihrer Plattform Einrichtungen zur Geolokalisierung einbetten, haben sie eine wichtige Verantwortung für die Entscheidung bezüglich der Standardeinstellung der Anwendung (standardmäßig „an" oder „aus"). Auch wenn sie nur in dem Ausmaß für die Verarbeitung Verantwortliche sind, in dem sie selbst aktiv personenbezogene Daten verarbeiten, haben sie beispielsweise in Bezug auf die Sichtbarkeit und Qualität der Informationen zur Verarbeitung von Geolokalisierungsdaten eine Schlüsselrolle in Bezug auf die Rechtmäßigkeit der Verarbeitung von Daten durch für die Verarbeitung Verantwortliche wie die Anbieter spezieller Anwendungen.

5.3 Berechtigter Grund

5.3.1 Intelligente mobile Endgeräte

Wenn Telekombetreiber die Daten der Basisstation nutzen wollen, um einem Kunden Dienste mit Zusatznutzen anzubieten, müssen sie nach der geänderten

Datenschutzrichtlinie für elektronische Kommunikation die vorherige Einwilligung des Kunden einholen. Sie müssen auch sicherstellen, dass der Kunde über die Bedingungen der Verarbeitung informiert ist.

Angesichts der Sensibilität der Verarbeitung von (Mustern von) Standortdaten ist die *vorherige Einwilligung in Kenntnis der Sachlage* auch die wichtigste Grundlage, um die Verarbeitung von Daten in Bezug auf die Verarbeitung der Standorte eines intelligenten mobilen Endgeräts im Zusammenhang mit Diensten der Informationsgesellschaft zu legitimieren.

Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie muss die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage als freie Willensbekundung der betroffenen Person gegeben werden.

Abhängig von der Art der verwendeten Technologie spielt das Endgerät des Nutzers eine relativ aktive Rolle bei der Verarbeitung der Daten zur Bestimmung der Geoposition. Das Gerät kann Standortdaten von verschiedenen Quellen an jeden Dritten übertragen. Diese technische Fähigkeit sollte nicht mit der Rechtmäßigkeit einer solchen Datenverarbeitung verwechselt werden. Wenn die Standardeinstellungen eines Betriebssystems die Übertragung von Standortdaten ermöglicht, sollte das fehlende Einschreiten durch den Nutzer nicht fälschlicherweise als freiwillige Einwilligung missverstanden werden.

In dem Ausmaß, in dem Entwickler von Betriebssystem und andere Dienste der Informationsgesellschaft Standortdaten selbst aktiv verarbeiten (beispielsweise wenn sie Zugang zu Standortinformationen von oder durch das Gerät erhalten) müssen sie ebenfalls von ihren Nutzern die vorherige Einwilligung in Kenntnis der Sachlage einholen. Es muss klar sein, dass eine solche Einwilligung freiwillig weder durch die zwingende Annahme der allgemeinen Geschäftsbedingungen eingeholt werden kann noch durch die Möglichkeit zum Opt-out. Lokalisierungsdienste sollten standardmäßig ausgeschaltet sei. Die Standardeinstellung sollte „aus" sein und der Nutzer sollte dann die Möglichkeit haben, stufenweise bei bestimmten Anwendungen auf „an" zu stellen.

Einwilligung von Arbeitnehmern

Die Einwilligung als rechtmäßige Grundlage für die Verarbeitung ist im Beschäftigungsumfeld problematisch. In ihrer Stellungnahme zur Verarbeitung personenbezogener Daten von Beschäftigten schrieb die Datenschutzgruppe: „*Wird eine Einwilligung vom Beschäftigten erbeten und ist die Nichteinwilligung mit tatsächlichen oder potenziellen Nachteilen für ihn verbunden, so ist eine solche Einwilligung nicht gültig im Sinne von Artikel 7 oder Artikel 8, da sie nicht freiwillig erfolgt. Wenn der Arbeitnehmer keine Möglichkeit zur Ablehnung hat, kann nicht von Einwilligung gesprochen werden. (…) Probleme*

entstehen dort, wo die Einwilligung Einstellungsvoraussetzung ist. Der Arbeitnehmer hat theoretisch das Recht, die Einwilligung zu verweigern, aber er muss in diesem Fall damit rechnen, dass er die Chance auf eine bestimmte Stelle verliert. Unter solchen Umständen wird die Einwilligung nicht freiwillig erteilt und ist daher nicht gültig.“[12] Statt die Einwilligung zu suchen, müssen Arbeitgeber prüfen, ob es nachweisbar erforderlich ist, den genauen Aufenthaltsort des Arbeitnehmers aus einem rechtmäßigen Grund zu überwachen. Dieses Erfordernis muss dann gegen die Grundrechte und Grundfreiheiten der Arbeitnehmer abgewogen werden. In den Fällen, in denen die Notwendigkeit angemessen gerechtfertigt werden kann, könnte die Rechtsgrundlage für die Verarbeitung auf dem berechtigten Interesse des für die Verarbeitung Verantwortlichen basieren (Artikel 7 Buchstabe f der Datenschutzrichtlinie). Der Arbeitgeber muss stets nach der am wenigsten einschneidenden Maßnahme suchen, eine ständige Überwachung vermeiden und beispielsweise ein System auswählen, das eine Warnung sendet, wenn ein Arbeitnehmer eine vorab gesetzte virtuelle Grenze überschreitet. Ein Arbeitnehmer muss die Möglichkeit haben, jedesÜberwachungsgerät außerhalb der Arbeitszeiten auszuschalten. Es muss ihm gezeigtwerden, wie das geht. Fahrzeugortungsgeräte sind keine Geräte zur Überwachung der Mitarbeiter. Ihre Funktion ist es, Fahrzeuge zu orten oder den Standort der Fahrzeuge zu überwachen, in denen sie eingebaut sind. Arbeitgeber sollten sie nicht als Gerät ansehen, mit dem sie das Verhalten oder den Aufenthaltsort von Fahrern oder anderen Mitarbeiten überprüfen können, indem sie beispielsweise Warnungen in Bezug auf die Geschwindigkeit des Fahrzeuges senden.

Einwilligung von Kindern

In einigen Fällen muss die Einwilligung von Kindern von ihren Eltern oder anderen gesetzlichen Vertretern gegeben werden. Das bedeutet beispielsweise, dass der Anbieter einer Anwendung zur Geolokalisierung die Eltern über die Erhebung und die Nutzung der Standortdaten ihrer Kinder informieren muss und ihre Einwilligung einholen muss, bevor er weiter Informationen über die Kinder erhebt und nutzt. Einige Anwendungen zur Geolokalisierung wurden speziell für die elterliche Überwachung entworfen. Sie zeigen beispielsweise ständig den Standort des Geräts auf einer Website an oder senden einen Alarm, wenn das Gerät ein vorher festgelegtes Gebiet verlässt. Die Nutzung solcher Anwendungen ist problematisch. In ihrer Stellungnahme 2/2009[13] zum Schutz der personenbezogenen Daten von Kindern schrieb die Artikel-29-Datenschutzgruppe: *Es sollte niemals vorkommen, dass Kinderaus Sicherheitsgründen mit einem Übermaß an Überwachung*

[12] WP48, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten.

[13] WP160, Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen).

konfrontiert werden, die ihre Selbstbestimmung einschränken würde. Vor diesem Hintergrund gilt es, das richtige Gleichgewicht zwischen dem Schutz der Intimität und Privatsphäre von Kindern und ihrer Sicherheit zu finden.

Der Rechtsrahmen sieht vor, dass Eltern dafür verantwortlich sind, dass das Recht der Kinder auf Privatsphäre gewährleistet ist. Wenn Eltern entscheiden, dass die Nutzung einer solchen Anwendung unter bestimmten Umständen berechtigt ist, müssen die Kinder wenigstens informiert werden. Sobald dies vernünftigerweise möglich ist, müssen sie an der Entscheidung über die Nutzung einer solchen Anwendung beteiligt werden.

Die Einwilligung muss für den konkreten Fall und für jeden der unterschiedlichen Zwecke gegeben werden, aus denen die Daten verarbeitet werden. Der für die Verarbeitung Verantwortliche muss es sehr deutlich klarstellen, ob sein Dienst darauf beschränkt ist, auf die freiwillige Frage „Wo bin ich jetzt gerade?“ eine Antwort zu geben oder ob sein Zweck darin besteht, Antworten auf die Fragen zu finden „Wo bist du, wo warst du und wo wirst du nächste Woche sein?“. Anders ausgedrückt: Der für die Verarbeitung Verantwortliche muss besondere Aufmerksamkeit auf die Einwilligung für die Zwecke richten, die die betroffene Person nicht erwartet, wie beispielsweise das Erstellen von Profilen und/oder Behavioural Targeting.

Wenn sich der Zweck der Verarbeitung grundlegend ändert, muss der für die Verarbeitung Verantwortliche erneut die Einwilligung für den konkreten Fall einholen. Wenn ein Unternehmen beispielsweise ursprünglich angegeben hat, es würde personenbezogene Daten Dritten nicht mitteilen, dies aber jetzt tun möchte, muss es die aktive vorherige Einwilligung jedes Kunden einholen. Eine ausbleibende Antwort (oder eine andere Art von Opt-out-Szenario) reicht nicht aus.

Es muss unterschieden werden zwischen der Einwilligung in einen einmaligen Dienst und in ein regelmäßiges Abonnement. Um beispielsweise einen bestimmten Dienst zur Geolokalisierung zu nutzen, kann es möglicherweise erforderlich sein, diesen Dienst an dem Gerät oder in dem Browser einzustellen. Wenn die Geolokalisierungsfunktion auf „an“ steht, kann jede Website die Standortdetails des Nutzers des betreffenden intelligenten mobilen Endgerätes lesen. Um die Risiken einer geheimen Überwachung zu verhindern, ist die Artikel-29-Datenschutzgruppe der Ansicht, dass das Gerät ständig warnen sollte, wenn der Geolokalisierungsdienst eingeschaltet ist. Das könnte beispielsweise mittels eines dauerhaft zu sehenden Icons gemacht werden.

Die Datenschutzgruppe empfiehlt den Anbietern von Geolokalisierungsanwendungen oder -diensten die individuelle Einwilligung nach einer angemessenen Zeitspanne zuerneuern (selbst, wenn keine Änderung in der Art der Verarbeitung erfolgt ist). Es wäre beispielsweise nicht richtig, Standortdaten weiterhin zu ver-

arbeiten, wenn die betreffende Person den Dienst während der letzten zwölf Monate nicht aktiv genutzt hat. Selbst wenn eine Person den Dienst genutzt hat, sollte sie zumindest einmal im Jahr (oder häufiger, wenn die Art der Verarbeitung dies erforderlich macht) an die Art der Verarbeitung ihrer personenbezogenen Daten erinnert werden und es sollte ihr eine einfache Möglichkeit zum Ausschalten aufgezeigt werden.

Schließlich muss die betroffene Person die Möglichkeit haben, ihre Einwilligung auf eine sehr einfache Weise und ohne negative Auswirkungen auf die Verwendung des Endgeräts zurückzuziehen. Unabhängig von den europäischen Datenschutzrichtlinien, hat das World Wide Web Consortium (W3C) einen Normentwurf für Geolocation API herausgegeben, der die Notwendigkeit der vorherigen, ausdrücklichen Einwilligung in Kenntnis der Sachlage betont.[14] W3C erklärt insbesondere , dass der Widerruf einer Einwilligung respektiert werden muss und rät denjenigen, die die Normen umsetzen, zu berücksichtigen, dass „*der unter einer bestimmte URL gespeicherte Inhalt sich so ändert, dass die vorher gewährten Standortgenehmigungen in Bezug auf den Nutzer nicht mehr zutreffen. Oder die Nutzer könnten einfach ihrer Meinung geändert haben.*“

Beispiel einer bewährten Praxis für Anbieter von Geolokalisierungsanwendungen

Eine Anwendung, die Standortdaten verwenden möchte, informiert den Nutzer deutlich über die Zwecke, für die die Daten genutzt werden sollen und erfragt die ausdrückliche Einwilligung für jeden möglichen Zweck. Der Nutzer wählt aktiv das Maß der Granularität der Geolokalisierung (beispielsweise auf Länderebene, Städteebene, Postleitzahlenebene oder so genau wie möglich). Sobald der Dienst zur Standortbestimmung aktiviert ist, ist ständig ein Icon auf jedem Bildschirm sichtbar, der anzeigt, dass die Dienste zur Standortbestimmung aktiviert sind. Der Nutzer kann seine Einwilligung jederzeit zurückziehen, ohne hierfür die Anwendung verlassen zu müssen. Der Nutzer hat auch die Möglichkeit, alle auf dem Endgerät gespeicherten Standortdaten einfach und dauerhaft zu löschen.

5.3.2 Wi-Fi-Zugangspunkte

Auf der Grundlage der Datenschutzrichtlinie können Unternehmen für den speziellen Zweck des Anbietens von Geolokalisierungsdiensten ein berechtigtes Interesse an der erforderlichen Erhebung und Verarbeitung von MAC-Adressen und errechneten Standorten von Wi-Fi-Zugangspunkten haben.

[14] W3C Geolocation API: http://www.w3.org/TR/geolocation-API/

Der berechtigte Grund gemäß Artikel 7 Buchstabe f der Datenschutzrichtlinie erfordert ein Gleichgewicht zwischen dem berechtigten Interessen des für die Verarbeitung Verantwortlichen und den Grundrechten der betroffenen Personen. Angesichts der halbstatischen Natur der Wi-Fi-Zugangspunkte stellt das Kartografieren von Wi-Fi-Zugangspunkten im Prinzip eine geringere Gefahr für die Privatsphäre der Inhaber dieser Zugangspunkte dar, als die Standortortung in Echtzeit durch die intelligenten, mobilen Endgeräte.

Das Gleichgewicht zwischen den Rechten des für die Verarbeitung Verantwortlichen und den Rechten der betroffenen Personen ist dynamisch. Damit die für die Verarbeitung Verantwortlichen ihre berechtigten Interessen langfristig über die Interessen der betroffenen Personen stellen können, müssen sie Garantien einführen und umsetzen. Dazu gehört zum Beispiel das Recht, sich einfach und dauerhaft von der Datenbank abzumelden, ohne dem für die Verarbeitung dieser Datenbank Verantwortlichen zusätzliche personenbezogene Daten geben zu müssen. Sie können beispielsweise eine Software nutzen, die es automatisch feststellt, wenn eine Person mit einem bestimmten Zugangspunkt verbunden ist.[15]

Darüber hinaus ist die Erhebung und Verarbeitung von SSIDs für das Anbieten von Geolokalisierungsdiensten nicht erforderlich. Deshalb geht die Erhebung und Verarbeitung von SSIDs über den Zweck des Anbietens von Geolokalisierungsdiensten hinaus, die auf dem Kartografieren des Standortes von Wi-Fi-Zugangspunkten basieren.

5.4 Information

Die verschiedenen für die Verarbeitung Verantwortlichen müssen sicherstellen, dass die Inhaber der intelligenten mobilen Endgeräte gemäß Artikel 10 der Datenschutzrichtlinie angemessen über die Schlüsselelemente der Verarbeitung informiert werden. Dazu zählen beispielsweise die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmung der Verarbeitung, die Art Daten, die Dauer der Verarbeitung, das Vorliegen von Auskunfts-, Berichtigungs- und Löschungsrechten der betroffenen Personen sowie ihr Recht, die Einwilligung zurückzuziehen.

---

[15] Folgendes ist ein möglicher Anwendungsfall:
1. Eine betroffene Person geht auf eine spezielle Website, über die sie die MAC-Adresse ihres Wi-Fi-Zugangspunktes eingeben kann.
2. Wenn die MAC-Adresse in der Datenbank mit den kartografierten Wi-Fi-Zugangspunktenerscheint, kann der für die Verarbeitung Verantwortliche eine Überprüfungsseite zeigen, die ein Skript enthält, das nach der ARP-Tabelle des Internetgeräts fragt. Theoretisch können die WLAN MAC-Adressen über den Befehl „ARP-a“ gezeigt werden. Mit Hilfe des Codes in dem Browser, wie Java, kann die ARP-Tabelle im Hintergrund produziert werden.
3. Wenn die MAC-Adresse in der ARP-Tabelle auftaucht, steht fest, dass der mit dem WLAN verbundene Nutzer auch der Nutzer mit dem Zugang zu der lokalen WLAN MAC-Adresse ist. Der für die Verarbeitung Verantwortliche überprüft auf diese Weise die Anfrage nach Löschung auf eine automatische und einfache Weise.

Die Gültigkeit der Einwilligung ist untrennbar verbunden mit der Qualität der Informationen über den Dienst. Die Informationen müssen klar, umfassend und für ein breites, nicht technisch versiertes Publikum verständlich sowie ständig und einfach zugänglich sein.

Die Informationen müssen auf ein breites Publikum abgestimmt sein. Die für die Verarbeitung Verantwortlichen können nicht davon ausgehen, dass ihre Kunden allein weil sie ein intelligentes mobiles Endgerät haben, technisch versierte Personen sind. Die Informationen müssen altersgemäß sein, wenn der für die Verarbeitung Verantwortliche weiß, dass das Gerät jüngere Menschen anspricht.

Wenn Anbieter von Geolokalisierungsanwendungen den Standort eines Endgerätes häufiger als einmal berechnen wollen, müssen sie ihre Kunden so lange informieren, wie die die Standortdaten verarbeiten. Sie müssen es ihren Kunden auch ermöglichen, die Einwilligung zu verlängern oder zu widerrufen. Damit diese Ziele erreicht werden, sollten die Anbieter der Anwendungen eng mit dem Entwickler des Betriebssystems zusammenarbeiten. Der Entwickler ist technisch in der besten Position, eine dauerhaft sichtbare Erinnerung daran zu schaffen, dass die Standortdaten verarbeitet werden. Der Entwickler kann auch gut kontrollieren, dass keine Anwendungen angeboten werden, die den Standort der intelligenten mobilen Geräte heimlich überwachen.

Wenn der Entwickler des Betriebssystems eine Phone-Home-Funktion oder andere Mittel des Zugangs zu auf dem Endgerät gespeicherten Daten geschaffen hat oder wenn er auf einem anderen Weg, beispielsweise durch dritte Werbetreibende, Zugang zu den Daten erhält, muss er die betroffene Person im Voraus über die (spezifischen und berechtigten) Zweckbestimmungen informieren, für die er diese Daten verarbeiten will. Er muss die betroffene Person auch über die Dauer der Verarbeitung informieren.

Die Verpflichtung zur Informierung der betroffenen Personen besteht auch für die für die Verarbeitung der Datenbanken mit geografisch bestimmten Wi-Fi-Zugangspunkten Verantwortlichen. Sie müssen die Allgemeinheit auf eine angemessene Weise über ihre Identität und die Zweckbestimmungen der Verarbeitung informieren und ihnen sonstige einschlägige Informationen geben. Die reine Erwähnung einer möglichen Erhebung von Daten über Wi-Fi-Zugangspunkte in einer speziellen Datenschutzerklärung, die auf die Nutzer einer Geolokalisierungsanwendung abzielt, reicht nicht aus. Es gibt genügend Mittel, sowohl Online als auch Offline, mit Hilfe derer die Allgemeinheit informiert werden kann.

5.5 Die Rechte der betroffenen Personen

Die betroffenen Personen haben das Recht, von den verschiedenen für die Verarbeitung Verantwortlichen Zugang zu den Standortdaten zu erhalten, die diese von

den intelligenten mobilen Endgeräten erhoben haben. Sie haben auch ein Recht auf Informationen bezüglich der Zweckbestimmungen der Verarbeitung und der Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden. Die Information muss in einem Format erteilt werden, das von Menschen gelesen werden kann. Das heißt, es muss ein geografischer Standort genannt werden und nicht abstrakte Zahlen beispielsweise der Basisstationen.

Die betroffenen Personen haben auch ein Zugangsrecht zu den möglichen Profilen, die aufgrund dieser Standortdaten erstellt wurden. Wenn Standortdaten gespeichert werden, sollte es den Nutzern ermöglicht werden, diese zu aktualisieren, zu berichtigen oder zu löschen.

Die Datenschutzgruppe empfiehlt, dass die für die Verarbeitung Verantwortlichen sichere Wege suchen, mit denen Online ein direkter Zugang zu Standortdaten und möglichen Profilen bereitgestellt werden kann. Es ist unabdingbar, dass ein solcher Zugang ermöglicht wird, ohne weitere personenbezogene Daten zur Überprüfung der Identität der betroffenen Personen abzufragen.

5.6 Aufbewahrungsfristen

Anbieter von Geolokalisierungs- und Anwendungsdiensten sollten Aufbewahrungsfristen für die Standortdaten festlegen, die den Zeitraum nicht überstiegen, der für die Zwecke benötigt wird, für die die Daten erhoben wurden oder weiter verarbeitet werden. Sie müssen sicherstellen, dass Standortdaten oder die anhand dieser Daten erstellten Profile nach einem angemessenen Zeitraum gelöscht werden.

Sollte es für den Entwickler des Betriebssystems und/oder den für die Verarbeitung einer Infrastruktur zur Geolokalisierung Verantwortlichen nachweislich erforderlich sein, anonyme Standortdaten für den Zweck der Aktualisierung oder Verbesserung des Dienstes zu erheben, muss mit äußerster Sorgfalt vorgegangen werden, um zu vermeiden, dass die Daten (indirekt) erkennbar gemacht werden. Selbst wenn ein mobiles Endgerät mit einem wahllos zugewiesenen Unique Device Identifier (UDID) identifiziert wird, sollte eine solche Kennnummer maximal für die Dauer von 24 Stunden für Betriebszwecke gespeichert werden. Nach diesem Zeitraum sollte die UDID weiter anonymisiert werden. Dabei muss berücksichtigt werden, dass eine wahre Anonymisierung in zunehmendem Maße schwieriger wird und dass die kombinierten Standortdaten dennoch zu einer Identifizierung führen könnten. Eine solche UDID sollte weder mit früheren noch zukünftigen UDIDs des Endgeräts verknüpft werden können noch sollte sie mit einem festen Kennzeichen des Nutzers oder des Telefons (wie die MAC-Adresse, IMEI oder IMSI-Nummer oder einer sonstigen Kontonummer) verknüpfbar sein.

In Bezug auf die Daten über Wi-Fi-Zugangspunkte ist Folgendes zu beachten. Sobald die MAC-Adresse eines Wi-Fi-Zugangspunktes basierend auf der ständigen Beobachtung von Inhabern intelligenter, mobiler Endgeräte einem neuen Standort zugeordnet ist, muss der vorherige Standort umgehend gelöscht werden. So soll die weitere Nutzung der Daten für unangemessene Zwecke verhindert werden. Dazu zählt Marketing, das auf Personen abzielt, die ihren Standort gewechselt haben.

6. Schlussfolgerungen

Mit Hilfe von Technologien zur Geolokalisierung wie Daten von Basisstationen, GPS und kartografierten Wi-Fi-Zugangspunkten können intelligente, mobile Endgeräte durch alle möglichen für die Verarbeitung Verantwortlichen aufgespürt werden. Die Zwecke reichen hierbei von Behavioural Targeting zur Überwachung von Kindern.

Da Smartphones und Tablet-PCs untrennbar mit ihrem Inhaber verbunden sind, bieten die Bewegungsmuster dieser Endgeräte eine sehr persönliche Einsicht in das Privatleben ihrer Eigentümer. Eine der großen Gefahren ist, dass die Inhaber nicht wissen, dass sie ihren Standort übermitteln und an wen. Eine weitere, damit in Verbindung stehende Gefahr ist die Ungültigkeit der Einwilligung, dass bestimmte Anwendungen ihre Standortdaten nutzen dürfen, da die Schlüsselelemente der Verarbeitung unverständlich, veraltet oder ansonsten unzureichend sind.

Es bestehen verschiedene Verpflichtungen für die unterschiedlichen Betroffenen, von den Entwicklern der Betriebssysteme zu den Anbietern von Anwendungen und Dritten wie sozialen Netzwerken, die auf ihren Plattformen Funktionen der Standortbestimmung für mobile Endgeräte einbetten.

6.1 Rechtsrahmen

- Der EU-Rechtsrahmen für die Verwendung von Geolokalisierungsdaten von intelligenten mobilen Endgeräten ist in erster Linie die Datenschutzrichtlinie. Standortdaten von intelligenten mobilen Endgeräten sind personenbezogene Daten. Die Kombination aus der eindeutigen MAC-Adresse und dem berechneten Standort eines Wi-Fi-Zugangspunktes sollte als personenbezogene Daten behandelt werden.

- Darüber hinaus findet die überarbeitete Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG nur bei der Verarbeitung der Basisstationsdaten durch Telekombetreiber Anwendung.

6.2 Für die Verarbeitung Verantwortliche

- Es können die folgenden drei Arten von für die Verarbeitung Verantwortlichen unterschieden werden: für die Verarbeitung einer Infrastruktur für die Geolokalisierung Verantwortlicher (insbesondere für die Verarbeitung von kartografierten Wi-Fi-Zugangspunkten Verantwortlicher), Anbieter von Geolokalisierungsanwendungen und -diensten und Entwickler der Betriebssysteme intelligenter mobiler Endgeräte.

6.3 Berechtigte Gründe

- Da die Standortdaten intelligenter mobiler Endgeräte sehr persönliche Details über das Privatleben ihrer Nutzer offenlegen, ist der wichtigste berechtigte Grund die vorherige Einwilligung in Kenntnis der Sachlage.

- Die Einwilligung kann nicht durch allgemeine Geschäftsbedingungen eingeholt werden.

- Die Einwilligung muss für den konkreten Fall und für die verschiedenen Zwecke, aus denen die Daten verarbeitet werden, erteilt werden. Dazu gehören auch das Erstellen von Profilen oder Behavioural Targeting durch den für die Verarbeitung Verantwortlichen. Wenn sich der Zweck der Verarbeitung grundlegend ändert, muss der für die Verarbeitung Verantwortliche erneut die Einwilligung für den konkreten Fall einholen.

- Standortdienste müssen standardmäßig ausgeschaltet sein. Eine Möglichkeit zum Opt-out stellt keinen angemessenen Mechanismus zur Einholung der Einwilligung des Nutzers in Kenntnis der Sachlage dar.

- Die Einwilligung ist problematisch in Bezug auf Arbeitnehmer und Kinder. In Bezug auf Arbeitnehmer können Arbeitgeber diese Technologie nur dann anwenden, wenn sie nachweislich für einen rechtmäßigen Zweck erforderlich ist und dieselben Ziele nicht mit weniger einschneidenden Maßnahmen erreicht werden können. In Bezug auf Kinder müssen die Eltern beurteilen, ob die Nutzung einer solchen Anwendung unter bestimmten Umständen berechtigt ist. Sie müssen ihre Kinder zumindest informieren. Sobald es vernünftigerweise möglich ist, müssen die Kinder an der Entscheidung über die Nutzung einer solchen Anwendung beteiligt werden.

- Die Datenschutzgruppe empfiehlt, den Anwendungsbereich der Einwilligung zeitlich zu begrenzen und die Nutzer mindestens einmal im Jahr zu erinnern. Die Datenschutzgruppe empfiehlt auch eine ausreichende Granularität bei der Einwilligung in Bezug auf die Genauigkeit der Standortdaten.

- Die betroffenen Personen müssen die Möglichkeit haben, ihre Einwilligung auf eine sehr einfache Weise und ohne negative Auswirkungen auf die Verwendung des Endgeräts zurückzuziehen.

- In Bezug auf das Kartografieren von Wi-Fi-Zugangspunkten können Unternehmen ein berechtigtes Interesse an der erforderlichen Erhebung und Verarbeitung der MAC-Adressen und berechneten Standorte von Wi-Fi-Zugangspunkten für den speziellen Zweck haben, dass sie Geolokalisierungsdienste anbieten. Das Gleichgewicht der Interessen zwischen den Rechten des für die Verarbeitung Verantwortlichen und den Rechten der betroffenen Personen macht es erforderlich, dass der für die Verarbeitung Verantwortliche die Möglichkeit des einfachen und dauerhaften Opt-out aus der Datenbank gibt, ohne zusätzliche personenbezogene Daten einzufordern.

6.4 Information

- Die Informationen müssen klar, umfassend und für ein breites, nicht technisch versiertes Publikum verständlich sowie ständig und einfach zugänglich sein. Die Gültigkeit der Einwilligung ist untrennbar verbunden mit der Qualität der Informationen über den Dienst.

- Dritte wie Browser und soziale Netzwerke spielen eine Schlüsselrolle in Bezug auf die Sichtbarkeit und Qualität der Informationen zur Verarbeitung von Geolokalisierungsdaten.

6.5 Die Rechte der betroffenen Personen

- Die verschiedenen für die Verarbeitung von Informationen zur Geolokalisierung von intelligenten mobilen Endgeräten Verantwortlichen sollten ihren Kunden den Zugang zu ihren Standortdaten in einem Format ermöglichen, das von Menschen gelesen werden kann. Die Nutzer sollten auch die Möglichkeit haben, die Daten zu ändern und zu löschen, ohne dass überflüssige personenbezogene Daten erhoben werden.

- Die betroffenen Personen haben auch das Recht, Zugang zu möglicherweise auf diesen Standortdaten erstellten Profilen zu nehmen, diese zu berichtigen oder zu löschen.

- Die Datenschutzgruppe empfiehlt das Einrichten eines (sicheren) Online-Zugangs.

6.6 Aufbewahrungsfristen

- Die Anbieter von Geolokalisierunganwendungen oder -diensten sollten Aufbewahrungspolitiken einführen, die sicherstellen, dass Daten zur Geolokalisie-

rung oder anhand solcher Daten erstellte Profile nach einem angemessenen Zeitraum gelöscht werden.

- Wenn der Entwickler des Betriebssystems und/oder der für die Verarbeitung der Infrastruktur zur Geolokalisierung Verantwortliche eine Kennnummer wie die MAC-Adresse oder die UDID in Bezug auf die Standortdaten verarbeitet, darf die Kennnummer höchstens für die Dauer von 24 Stunden für Betriebszwecke gespeichert werden.

Brüssel, den 16. Mai 2011

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

V. Internationale Konferenz der Datenschutzbeauftragten

33. Konferenz vom 1. – 3. Novemer 2011 in Mexiko-Stadt

Entschließung über die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)

Heute hat sich das Internet zur wichtigsten Technologie für die Übermittlung jeder Art von Kommunikation entwickelt, sei es Sprache, Video oder Daten, und es wurde zur Grundlage fast aller geschäftlicher Transaktionen und sozialer Interaktionen. Angesichts der drohenden Erschöpfung der Adressen, die vom gegenwärtig genutzten Internet Protokoll Version 4 (IPv4) zur Verfügung gestellt werden, angesichts der anhaltenden enormen weltweiten Nachfrage für Internetadressen und angesichts der Notwendigkeit des Internets zur Unterstützung einer wachsenden Palette neuer Geräte, einschließlich Sensoren und intelligenter Zähler (das „Internet der Dinge"), wurde ein neues Internetprotokoll (IPv6 – IP Version 6) standardisiert, entwickelt und im Laufe der letzten 10 Jahren getestet und muss nun umgesetzt werden.

Obwohl IPv6 im Vergleich zu IPv4 eine Reihe praktischer Vorteile aufweist, können seine Eigenschaften auch zu bestimmten Risiken für den Datenschutz und die Privatsphäre führen, was von der Konfiguration des neuen Protokolls und vor allem von der für die Zuteilung und Zuweisung der IPv6-Adresse gewählten Strategie abhängt. Diese Risiken müssen beim Einsatz der neuen Version des Internetprotokolls angesprochen und kontrolliert werden.

Die Internationale Konferenz gibt folgende Empfehlungen:

- Die Nutzung temporärer und nicht permanenter IPv6-Adressen („dynamische Adressen") muss für jeden Nutzer durch die Beibehaltung der dynamischen Zuweisung von IPv6-Adressen durch ISPs möglich bleiben. Internetzugangsanbieter und Betreiber von Gateways sollte die Nutzung dynamischer IP-Adressen als Standardeinstellung anbieten. Nutzer sollten außerdem in der Lage sein, ihre IP-Adresse während einer Sitzung durch einfaches Verfahren zu ändern. Die Gesetzgeber oder Regulierungsbehörden sollten, soweit erforderlich, es in Erwägung ziehen, entsprechende Verpflichtungen in ihre nationale Rechtsrahmen hinzuzufügen, sofern dies nicht bereits geschehen ist.

- Der Einsatz temporärer und nicht permanenter IPv6-Adressen muss mit den IPv6-Autokonfigurationsfunktionen möglich bleiben, indem alle vorhandenen

Möglichkeiten der Pseudorandomisierung der Schnittstellenkennung („Privacy Extensions“) genutzt werden. Gerätehersteller – vor allem Hersteller mobiler Geräte – sollten solche Möglichkeiten schnell in ihre Produkte integrieren. Der Einsatz dynamischer Adressen für Endgeräte sollte als Standardfunktion aktiviert werden.

- Als Standardeinstellung sollten Anbieter, Protokolle, Produkte und Dienstleistungen die Nutzung temporärer und nicht permanenter Adressen anbieten.

- Wie jeweils anwendbar, sollten Netzwerke und Applikationen alle Sicherheitsfunktionen von IPv6 (IPSec) in vollem Umfang nutzen, um die Sicherheit, Integrität und Vertraulichkeit zu gewährleisten.

- Immer wenn Standortinformationen für die Nutzung der Dienste auf mobilen Geräten und anderen über IPv6 verbundenen Geräten notwendig ist, sollten solche Informationen z. B. durch Verschlüsselung gegen rechtswidriges Abhören und Missbrauch geschützt werden.

- Alle für die Ausarbeitung und Umsetzung aller weiteren Entwicklungen des IP-Protokolls verantwortlichen Akteure müssen sicherstellen, dass solche Normen und Vorgaben die Datenschutzrechte und Werte von Anfang an vollständig berücksichtigen.

Die Internationale Konferenz begrüßt es, dass die International Working Group on Data Protection in Telecommunications (IWGDPT) derzeit über einen umfassenden Bericht zu diesen Fragen diskutiert. In dem Bericht sollen insbesondere die Auswirkungen einer datenschutzfreundlichen Umsetzung von IPv6 auf dem Gebiet der Strafverfolgung untersucht werden. Die IWGDPT wird gebeten, ihren Bericht unter Berücksichtigung der oben genannten Empfehlungen abzuschließen.

VI. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 49. Sitzung am 4./5. April 2011 in Montreal

Datenaufzeichnung in Fahrzeugen (Event Data Recording – EDR): Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller

– Übersetzung –

Hintergrund

1. Der rasante technologische Fortschritt in der Informationsgesellschaft, insbesondere im Bereich Intelligente Verkehrssysteme (IVS), hat eine zunehmende Verarbeitung personenbezogener Daten in Fahrzeugen (PKW und LKW) sowohl für private als auch für kommerzielle Zwecke zur Folge.

2. Die nahezu allgegenwärtige Internetanbindung und immer größere Bandbreiten ermöglichen eine permanente Vernetzung sogenannter „Smart Vehicles“ (Intelligente Fahrzeuge) und somit den Zugriff auf angefallene Daten. Diese alarmierende technische Entwicklung führt zu einer Eingliederung intelligenter Fahrzeuge in das sog. „Internet of Things“, das die Verknüpfung von physischen Objekten, also Sachen, mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur beschreibt.

3. Ohne geeignete Maßnahmen zum Schutz der Privatsphäre wird es weder Fahrern noch Passagieren solcher „Smart Vehicles“ möglich sein, die Verarbeitung ihrer Daten zu kontrollieren oder zu überwachen. Sie werden sich dieser Verarbeitung vielmehr gar nicht bewusst sein.

4. Ungeachtet der mannigfaltigen Erscheinungsformen technologischer Anwendungen in Fahrzeugen behandelt dieses Arbeitspapier ausschließlich die Aspekte der Datenaufzeichnung.

Datenaufzeichnung in Fahrzeugen (EDR): Definitionen und Fakten

5. Im Moment eines Unfalls oder sonstigen Schadenseintritts werden verschiedene, durch Sensoren erfasste Daten mittels eines in das Fahrzeug eingebauten Geräts, des „Event Data Recorder“ (EDR) oder auch Unfalldatenspeichers, gespeichert. Diese Geräte verarbeiten die Daten typischerweise inner-

halb eines begrenzten Zeitraums im Zusammenhang mit einem Schaden, Unfall oder sonstigen Störfall (unmittelbar vor, während und nach dem Ereignis).

6. Der EDR kann sowohl ab Werk als auch nachträglich in das Fahrzeug eingebaut werden. Die gespeicherten Daten können mittels spezieller, für Endverbraucher meistens nicht frei verkäuflicher Software heruntergeladen werden.

7. Die im Schadensfall gesammelten und registrierten Daten beziehen sich nicht ausschließlich auf technische Gegebenheiten des Fahrzeugs (wie etwa den Kraftstoffverbrauch oder die Funktionsfähigkeit des Airbags) und den Schadenszeitpunkt, sondern lassen darüber hinaus (direkt oder indirekt) Rückschlüsse auf das Fahrerverhalten zu (z. B. Bremsöldruck zu Beginn und Ende des Bremsvorgangs, Geschwindigkeit, Bremsverhalten, Motordrehzahl, Gaslast, Verwendung oder Nichtverwendung von Sicherheitsgurten).

8. Es handelt sich somit um personenbezogene Daten des Fahrers und ggf. auch der Passagiere (z. B. hinsichtlich der Daten über die Benutzung des Sicherheitsgurtes).

EDR in Verbindung mit anderen „On-Board-Systemen"

9. Im Rahmen vertraglicher Vereinbarungen mit Mobilfunkanbietern sind die EDRs mit den im Fahrzeug verbauten Kommunikationssystemen verbunden, die im Falle eines entsprechenden Vorfalls die relevanten Informationen an bestimmte Empfangsstationen übermitteln. Die Übermittlung erfolgt durch ein Unfallerkennungssystem (oder eingebautes Notrufsystem), das zu diesem Zweck automatisch oder auch manuell aktiviert wird. In den USA[1] und der EU[2] wurden bereits Initiativen ins Leben gerufen, die den Einbau dieser Systeme und die Einführung allgemeiner technischer Standards in den verschiedenen Transportsektoren befördern sollen.

10. Um mehr Beweismaterial zu einem Unfall zu erhalten, operieren EDRs vereinzelt auch mit eingebauten Videokameras (sog. Video Event Data Recor-

[1] Die US National Highway Traffic Safety Administration (NHTSA) hat im August 2006 entschieden, dass Hersteller nicht verpflichtet sind, EDRs in Neufahrzeuge einzubauen. Dennoch verlangt die NHTSA von den Herstellern den Einbau von EDRs, um jedenfalls einen Mindestdatensatz speichern zu können. Dieser soll 15 Typen von Unfalldaten beinhalten, darunter: Geschwindigkeit vor dem Unfall, Gaslast, Bremsverhalten, Geschwindigkeitsveränderungen, Sicherheitsgurtnutzung, Status der Airbag-Kontrolllampe und die Airbagauslösungszeit. Die Hersteller müssen sich mit diesen Standards bis September 2012 einverstanden erklären; http://www.nhtsa.gov/EDR

[2] Zur „E-call Intiative" der Europäischen Union im Einzelnen: Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, eCAll: Time for Deployment, Brüssel, 21.8.2009, KOM(2009) 434 endg.; http://ec.europa.eu/information_society/activities/esafety/ecall/index_de.htm.

der – VEDR), wodurch nochmals erheblich mehr Informationen über das Verhalten des Fahrers sowie über an dem Unfall beteiligte Dritte gespeichert werden.

Personenbezogene Fahrerdaten Daten beim Einsatz von EDR

11. Personenbezogene Fahrerdaten, die mittels EDR bzw. VEDR insbesondere im Zusammenhang mit elektronischen Kommunikations- und Lokalisierungssystemen gesammelt wurden, lassen sich von einer stetig wachsenden Anzahl von Interessengruppen zu den verschiedensten Zwecken verwenden:

    a. Hersteller, Fahrer (ebenso wie andere, in Verkehrsunfälle verwickelte Personen), Eigentümer (z. B. Autovermieter oder Firmenflottenverwalter) und Versicherungsgesellschaften könnten die EDR-Daten nutzen, um bei Rechtsstreitigkeiten Zeugenaussagen zu überprüfen;

    b. Polizei und andere Behörden (z. B. könnte die für die Sicherheit des Straßenverkehrs zuständige Behörde die Informationen zur Vervollständigung der Beweislage bei einem Verkehrsunfall nutzen);

    c. Arbeitgeber, aus organisatorischen und Sicherheitsgründen;

    d. Versicherungsgesellschaften, zur Einteilung der Kunden in spezifische Tarifgruppen (z. B. nach der Fahrweise oder nach Regionen, in die gefahren wird);

    e. Forschung, zur Verbesserung der Verkehrsinfrastruktur;

    f. Werbe- und Marketingagenturen könnten auf Grundlage der Daten Verhaltensanalysen durchführen, um so spezifisch zugeschnittene Angebote zu platzieren;

    g. andere Dienstleister (z. B. Pannenhilfe).

12. Die oben aufgeführten Entwicklungen erfordern besonders sorgfältige Überlegungen in Bezug auf den Datenschutz und die Persönlichkeitsrechte sowohl der Fahrer als auch aller potentiellen Passagiere. Ein angemessener Ausgleich mit anderen individuellen Rechten und Interessen und mit dem öffentlichen Interesse an der Sicherheit des Straßenverkehrs muss erreicht werden.

13. Die Europäische Kommission hat 2008 eine Mitteilung betreffend einen Aktionsplan[3] zum Thema Intelligente Verkehrssysteme veröffentlicht. Gleich-

[3] Aktionsplan zum Einsatz intelligenter Verkehrssysteme In Europa (COM(2008) 886).

zeitig hat die Kommission eine entsprechende Richtlinie vorgeschlagen, die kürzlich durch den Rat und das Europäische Parlament verabschiedet wurde[4]. Diese Richtlinie, die bis Februar 2012 durch die Mitgliedsstaaten umgesetzt werden muss, verlangt beim Einsatz intelligenter Verkehrssysteme die Verwendung anonymer Daten, soweit dies angemessen ist[5]. Der Datenschutz und ein verantwortungsvoller Umgang mit den gesammelten Informationen sind in dem Aktionsplan wie in der Richtlinie von zentraler Bedeutung, um das Ziel effizienterer, umweltfreundlicher und sichererer Mobilität im Fracht- und Passagierverkehr innerhalb der Europäischen Union zu erreichen.

14. Durch das Rahmenprogramm für Forschung und technologische Entwicklung in der Europäischen Union wurde eine Vielzahl von Forschungsprojekten aufgelegt, die inzwischen teilweise abgeschlossen sind oder immer noch andauern, um die Sicherheit auf den Straßen zu erhöhen[6]. In einigen Jurisdiktionen wurden Gesetzesvorschläge entwickelt[7], in anderen sogar bereits Gesetze verabschiedet, die (unter anderem) auf den Schutz der Privatsphäre des Fahrers im Zusammenhang mit dem Einsatz von EDR abzielen[8].[9]

15. Zeitgleich wird von Seiten der Datenschutzbeauftragten ein Anstieg der EDR-Verwendung zur Verwaltung von Fahrzeugflotten registriert.[10] Im Rahmen der europäischen E-call Initiative hat die Artikel 29-Datenschutzgruppe bereits eine Reihe von Empfehlungen unterbreitet[11].

---

4 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, Abl. L 207/1, 2010.

5 Art. 10 Abs. 3 der Richtlinie 2010/40/EU.

6 Vgl. Intelligent Car Brochure, p. 16 auf: http://ec.europa.eu/information_society/activities/intelligentcar/docs/right_column/intelligent_car_brochure.pdf.

7 Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381)*.

8 Kalifornien war der erste Staat, der gesetzlich verfügt hat, dass die Hersteller ihren Kunden gegenüber den Einbau von EDRs oder „black boxes" offenbaren müssen. Zur Gesetzgebung in Bezug auf Privatsphäre im Zusammenhang mit Datenaufzeichnung in Fahrzeugen siehe die Website der National Conference of State Legilatures auf: http://www.ncsl.org. Detaillierte Informationen zum aktuellen Stand in Sachen Datenaufzeichnung in Fahrzeugen in den U.S.A. finden sich auf der Seite der National Highway Traffic Safety Administration (http://www.nhtsa.gov/EDR).

9 Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381)*.

10 Französische Datenschutzbehörde (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommendation relative à la mise en oeuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme public ou privé; Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en oeuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules; Italienische Datenschutzbehörde (Garante per la protezione dei dati personali) on Geolocation in Public Transportation and Passenger Security, 5 June 2008, http://www.garanteprivacy.it , doc. no. 1672796

11 Artikel 29-Datenschutzgruppe, Working document on data protection and privacy implications in eCAll initiative, WP 125, http//ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_de.pdf

16. Die anstehende umfassende Einführung dieser Systeme, die Komplexität der Materie sowie die absehbaren notwendigen Investitionen (möglicherweise auch in Hinsicht auf die Verkehrsinfrastruktur) bedingen die dringliche Notwendigkeit eines klaren Regelwerkes, dem gleichwohl eine ausführliche öffentliche Auseinandersetzung mit der Thematik vorausgehen sollte. Der Entwicklung und Ausgestaltung eines solchen Regelwerkes sollte der Gedanke innewohnen, den Datenschutz von vornherein in die Gesamtkonzeption einbeziehen, anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme beheben zu wollen[12].

17. Vor diesem Hintergrund

ruft die Arbeitsgruppe die Regierungen dazu auf,

a) in Zusammenarbeit mit den Datenschutzbeauftragten und den betreffenden Interessenvertretern aus Industrie und Wirtschaft, ein angemessenes gesetzgeberisches Regelwerk darzulegen, zu definieren bzw. zu bestätigen (damit die Verarbeitung personenbezogener Daten auf gesetzmäßige Weise erfolgt und Missbrauch der durch EDR und möglicherweise andere intelligente Technologien in Fahrzeugen gesammelten und/oder übermittelten Daten ausgeschlossen oder eingeschränkt wird),

b) die Umsetzung der erforderlichen technischen Standards zu fördern und zu unterstützen, und

empfiehlt:

I. Transparenz

Jedwede Verwendung von Daten, die durch EDRs (oder andere intelligente Technologien) entstanden sind, sollte für den Fahrzeugeigentümer sowie die jeweiligen Fahrzeugnutzer in vollem Umfang transparent sein. Die Nutzer sind in die Lage zu versetzen, sich auf einfachstem Wege ein vollständiges Bild über die Erhebung und Speicherung sowie den Zweck der Verwendung aller sie betreffenden persönlichen Informationen machen zu können.

Zu diesem Zweck sollten:

a. *Hersteller/Systemintegratoren* ihre Kunden sorgfältig über die Verarbeitung personenbezogener Daten einschließlich der Möglichkeiten der Fahrzeugposi-

[12] Vgl. ISO/TR Technical Report 12859 on Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems.

tionsbestimmung aufklären. In dem Fahrzeug sollte ein (schriftlicher oder stimmlicher) Hinweis erfolgen. Ausdrückliche und detaillierte Informationen sollten im Benutzerhandbuch vorhanden sein.

b. *Datenverarbeitende Stellen* (wie etwa Arbeitgeber, Versicherer, Autovermietungen etc.) die Nutzer vollständig über (i) den Zweck der Verarbeitung erhobener Daten; (ii) die Kategorie(n) zu verarbeitender personenbezogener Daten; (iii) die Empfänger bzw. die Kategorien der Empfänger der Daten; und (iv) ihre Zugriffsrechte informieren.

II. Einwilligung des Eigentümers

Jegliches zur Speicherung personenbezogener Daten fähiges Gerät sollte regelmäßig nur nach der freiwilligen Einwilligung des ausführlich informierten Eigentümers und nach ausdrücklichem Hinweis an den Nutzer aktiviert werden. Zwingend notwendige Einbauten, die geeignet sind, personenbezogene Daten zu speichern oder an Dritte zu übermitteln, bedürfen einer gesetzlichen Grundlage, aus der vorgesehene Zweck der Speicherung personenbezogener Daten eindeutig hervorgeht.

III. Datenqualität

Die Datenaufzeichnung sollte nur solche personenbezogene Daten umfassen, deren Verarbeitung im Verhältnis zu dem Zweck ihrer Verarbeitung erforderlich und angemessen ist. Der Nutzung anonymisierter Daten sollte der Vorzug gegeben werden, wo immer dies möglich ist.

Entscheidungen anlässlich besonderer Vorkommnisse in Zusammenhang mit dem Fahrzeug sollten nicht ausschließlich von den Informationen aus der Datenaufzeichnung abhängig gemacht werden. Zu Zwecken der Qualitätsanalyse sind die aufgezeichneten Daten durch ausgewiesene Sachverständige zu prüfen und sorgfältig unter Heranziehung weiterer Nachweise und Begleitumstände abzugleichen.

IV. Privacy by Design

Das Leitmotiv bei der Entwicklung und Einführung von Systemen zur Datenaufzeichnung in bzw. der Interaktion mit Fahrzeugen sollte es sein, den Datenschutz und den Schutz der Privatsphäre von vornherein in die Gesamtkonzeption einzubeziehen. Derartige Systeme sollten darauf ausgerichtet sein, die Notwendigkeit der Verarbeitung personenbezogener Daten zu minimieren und zugleich einen potentiellen Missbrauch personenbezogener Daten zu verhindern.

V. Zugriff auf (personenbezogene) Daten

Vor einer Einführung ist das Augenmerk auf den Schutz der Privatsphäre zu richten und klar festzulegen, wer unter welchen Voraussetzungen (z. B. Richtervorbehalt) auf die aufgezeichneten personenbezogenen Daten zugreifen darf. Dies gilt insbesondere in Hinsicht auf solche personenbezogenen Daten, die nicht ausschließlich vom Fahrer stammen. Ihm selbst ist das freie und vollumfängliche Zugriffsrecht auf seine eigenen Daten grundsätzlich zuzuerkennen. Hinsichtlich aller anderen Personen, deren personenbezogene Daten aufgezeichnet werden könnten, sollten klare und zweckmäßige Methoden zur Wahrung und ggf. Durchsetzung ihrer Rechte bereitgestellt werden. Eine vorherige Folgenabschätzung in Bezug auf den Datenschutz und den Schutz der Privatsphäre ist ein nützliches Instrument für eine solche Analyse.

VI. Datensicherheit und -integrität

Standardisierte Sicherheitsmaßnahmen zur Vermeidung unrechtmäßigen Zugriffs, Verlustes oder rechtswidriger Veränderung der aufgezeichneten Daten müssen festgelegt und universell umgesetzt werden. Um das Risiko unerwünschter Datentransfers und anderer schwerwiegender Angriffe von außen zu verringern, sollten zusätzlich verlässliche Verschlüsselungstechniken und Authentifizierungssysteme verwendet werden. Für den Endverbraucher sollte klar erkennbar sein, dass die im Fahrzeug verbauten Systeme zur Datenaufzeichnung und -übermittlung diesen Standards vollauf gerecht werden. Im Zusammenhang untereinander vernetzter Systeme sind entsprechende Sicherheitsmaßnahmen sogar von noch größerer Bedeutung.

VII. Überwachung von Arbeitnehmern

Darüber hinaus sind gesetzliche Regelungen zum Schutz von Arbeitnehmern vor Überwachung durch den Arbeitgeber zu beachten und zu respektieren, wenn dieser Systeme installiert, die der Verhaltenskontrolle von Arbeitnehmern oder der Ortung der Fahrzeugposition dienen (z. B. Fahrtenschreiber oder Lokalisierungsdienste).

2. 50. Sitzung am 12./13. September 2011 in Berlin

Privacy by Design und Smart Metering: Minimierung personenbezogener Informationen zur Wahrung der Privatsphäre

– Übersetzung –

Hintergrund

Aufgrund der kontinuierlichen Entwicklung des Smart Grids ändert sich die Rolle des Energieversorgungsbetriebs. Historisch gesehen stand bei den Energieversorgern die Aufrechterhaltung einer regelmäßigen Versorgung zu möglichst niedrigen Kosten im Vordergrund. Interaktionen mit Kunden bezogen sich weitgehend auf die Abrechnung und die Minimierung des Kreditrisikos. Doch mit der aktuellen Neugestaltung der elektrischen Systeme durchlaufen diese Interaktionen eine radikale Umgestaltung, da die Smart Meter es den Energieversorgern ermöglichen, so detailliert wie noch nie zuvor und fast in Echtzeit Informationen über das Nutzungsverhalten ihrer Privatkunden zu erlangen. Diese Änderung ermöglicht die Entwicklung einer Reihe neuer Dienstleistungen und Nutzwerte sowohl für die Verbrauchenden als auch die Energieversorger.

Zur Aufrechterhaltung des Vertrauens der Verbrauchenden werden das Smart-Grid und das Smart Metering die Entstehung einer neuen, auf Kundeneinbindung ausgerichteten Beziehung zwischen Versorgungsunternehmen und Privatpersonen erforderlich machen. Datenschutz und Datensicherheit werden die dualen Eckpfeiler dieser Beziehung sein.

Smart Meters

Im Rahmen des Smart Grids wird das Smart Meter die Technologie sein, die dem Verbrauchenden am meisten auffällt – der intelligente Zähler, der „wichtige erste Schritt“ auf dem Weg zu einem umfassenderen intelligenten Stromnetz als Ganzes.[1] Diese Messgeräte mit integrierter wechselseitiger Kommunikation und verbesserter individueller Nutzungsinformation werden den Energieverbrauchenden die Kontrolle und die Regulierung ihres eigenen Verbrauchs erlauben und es den Energieversorgern ermöglichen, eine bedarfsgerechte Versorgung zu gewährleisten und den Lastausgleich zu steuern. Sie werden ebenfalls eine wichtige Rolle

[1] European Commission Staff Working Paper, Interpretative note on directive 2009/72/ec concerning common rules for the internal market in electricity and directive 2009/73/ec concerning common rules for the internal market in natural gas, p. 7, online:
http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_retail_markets.pdf

bei der Entwicklung verbesserter Strategien zur Energieeinsparung spielen, um den internationalen Kampf gegen die Erderwärmung zu unterstützen, während sie den Verbrauchenden ermöglichen, ihren Verbrauch mit Hilfe von Informations- und Rückkoppelungssystemen zu reduzieren.[2] Ein Pike Forschungsbericht aus dem Jahr 2009 weist darauf hin, dass 250 Millionen intelligente Stromzähler weltweit bis zum Jahr 2015 installiert werden könnten.[3] Diese Zähler werden eine entscheidende Rolle in den fortgeschrittenen Mess-Infrastrukturen der Versorgungsunternehmen spielen, welche, ohne hier näher darauf einzugehen, ebenfalls die Integration angemessener Datenschutzmaßnahmen in den Systemen erfordern.

Es existiert keine standardisierte universelle Definition des Begriffs „Smart Meter"; vielmehr wurde der Begriff auf eine Vielzahl von Geräten angewandt, die unterschiedliche Funktionalitäten umfassen. Es gibt jedoch einige grundlegende gemeinsame Charakteristika bei den meisten aktuell entwickelten intelligenten Zählern. Als wesentlichste dieser Eigenschaften erweist sich die relativ feingranulare digitale Messung des Energieverbrauchs von Haushalten – zum Beispiel die Ablesung des Energieverbrauchs im Minutentakt. Aber auch eine gröbere Taktung wie die stündliche Ablesung ermöglicht die Erhebung von Intervallverbrauchsdaten, wodurch Zeittarif-Abrechnungen ermöglicht werden, die tageszeitabhängige Strompreisunterschiede beim Verbrauch berücksichtigen. Eine Digitalanzeige zum Energieverbrauch der Haushalte (z. B. aktueller Verbrauch pro Intervall oder zurückliegender Verbrauch pro Intervall) wird in der Regel mit der Möglichkeit zur Übermittlung dieser Informationen an ein anderes Gerät (z. B. Smartphone oder Fernsehen) vorhanden sein. Intelligente Messgeräte können auch mit einem internen Speicher ausgestattet sein, der die Speicherung aller Ablesungen aus einem Zeitraum von mindestens sechs Monaten ermöglicht.

Intelligente Messgeräte sind daneben tendenziell mit einer bidirektionalen Kommunikationsfunktionalität ausgestattet. Diese ermöglicht es den Versorgungsunternehmen, die Messgeräte aus der Ferne abzulesen (bei einer deutlichen Kostenreduzierung im Vergleich zu Messgeräten, die vor Ort durch einen Beschäftigten des Energieversorgers abgelesen werden). Diese Funktion ermöglicht den Verbrauchenden zunehmend die Kontrolle ihres Energieverbrauchs pro zurückliegendem Intervall in Online-Web-Portalen. Die bidirektionale Kommunikation erlaubt den Versorgungsunternehmen auch die Aktivierung von Lastausgleichsfunktionen, bei denen die Energieversorger den Energieverbrauch durch Kommunikation mit den intelligenten Messgeräten in teilnehmenden Haushalten ermitteln können. In einigen Rechtsräumen kann der Verbrauchende eine spezielle

[2] Pacific Northwest National Laboratory: The Smart Grid: An Estimation of the Energy and CO2 Benefits. http://energyenvironment.pnnl.gov/news/pdf/PNNL-19112_Revision_1_Final.pdf

[3] Pike Research (Nov. 2, 2009) "Smart Meter Installations to Reach 250 Million Worldwide by 2015", online: http://www.pikeresearch.com/newsroom/smart-meter-installations-to-reach-250-million-worldwide-by-2015

Einrichtung an das Gerät anschließen, die automatisch seinen/ ihren Energieverbrauch basierend auf der Netzbelastung kontrolliert. Manche intelligenten Stromzähler mit bidirektionalen Kommunikationsfähigkeiten können auch mit einer ferngesteuerten Aktivierungs- und Deaktivierungsfunktion für die Versorgung ausgestattet sein. Dadurch kann ein Energieversorger mittels Fernsteuerung eine verbrauchende Person zu- oder abschalten.

Obwohl sich das Smart Metering bis heute auf den Verbrauch elektrischer Energie konzentriert, geht man davon aus, dass in der Zukunft die intelligenten Zähler auch für Wasser, Gas und Wärme eingesetzt werden. Dementsprechend sind einige intelligente Zähler darauf ausgelegt, die Messung für unterschiedliche Versorgungsunternehmen durchzuführen, um eine unnötige Verdoppelung der Infrastrukturen zu vermeiden.

Datenschutzrechtliche Probleme beim Smart Metering

Seit seiner Einführung haben sich Gesetzgeber, zahlreiche Datenschutzgruppen und Regulierungsbehörden auf die Notwendigkeit des Schutzes der Privatsphäre der Verbrauchenden beim Smart Grid konzentriert.[4] Es ist davon auszugehen, dass das Smart Grid bis zu acht Mal mehr Daten als das jetzige Stromnetz[5] generieren wird, die in einigen Fällen detaillierte Informationen über eine Person erkennen lassen könnten. Diese Intensivierung der Stromverbrauchsdaten ist verbunden mit dem Fernablesen und -erfassen der Daten, was Fragen in Bezug auf die Transparenz und die Kontrolle der Daten durch den Verbrauchenden aufwirft.[6]

Forschungsergebnisse deuten darauf hin, dass bei der Fortentwicklung des Smart Grids der Lebenswandel der Konsumierenden aus den generierten Informationen abgelesen werden kann – vor allem, da diese Informationen immer detaillierter werden und der charakteristische Stromverbrauch einzelner Geräten diese erkennbar macht. Doch selbst wenn der Stromverbrauch nicht im Minutentakt oder am Gerät aufgezeichnet wird, könnte die permanente Beobachtung des Stromverbrauchs die ungefähre Anzahl der Bewohner in einem Haushalt verraten,

---

4 Beispiele sind die deutsche Energie-Gesetzgebung (Energiewirtschaftsgesetz – EnWG, zuletzt geändert am 28. Juli 2011, Bundesgesetzblatt I, S. 1690), the Information and Privacy Commissioner of Ontario, Canada's series of Smart Grid white papers, and The Article 29 Data Protection Working Party's „Opinion 12/2011 on Smart Metering (WP 183)." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_de.pdf

5 „Accenture Launches Smart Grid Data Management Solution to Reduce Risks and Costs of Smart Grid Deployments," Mar. 18, 2010, online: http://newsroom.accenture.com/article_display.cfm?article_id=4971

6 Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs" http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/80DSK_DatenschutzBeiDerDigitalenMessung.pdf?_blob=publicationFile

wann sie anwesend sind, sowie wann sie wach sind oder schlafen. Dies gefährdet die Unverletzlichkeit der Wohnung, und solche intimen Details des täglichen Lebens erfordern ein hohes Schutzniveau. Diese Informationen sollten ohne das Wissen und das Einverständnis der/des Bewohner(s) nicht zugänglich sein. Die Verbrauchenden müssen die Möglichkeit und die Fähigkeit haben einzugreifen und zu bestimmen, wer auf diese Daten zugreifen darf. Prinzipiell sind alle offengelegten personenbezogenen Daten auf ein Mindestmaß zu beschränken, sowohl im Hinblick auf die Art und die Menge der Daten, als auch in Bezug auf die Übermittlung, die nur an die notwendigen Akteure erfolgen darf.

Die Bedeutung der Erhaltung des Vertrauens der Verbrauchenden in Bezug auf Datenschutz und Smart Metering wurde in vielen Rechtssystemen deutlich. Beispiele hierfür sind:

- **Kalifornien, USA:** Der Versorger PG & E wurde mit Blockaden von Anwohnern konfrontiert, die den Einbau intelligenter Zähler in ihrem Viertel verhindern wollten und sich dabei auf den Schutz der Privatsphäre und auf gesundheitliche Bedenken beriefen.[7]

- **British Columbia, Kanada:** Zahlreiche Beschwerden haben den Datenschutzbeauftragten der Provinz dazu veranlasst, eine Untersuchung von BC Hydro's Smart Meter-Programm ins Leben zu rufen. Dabei stellte er fest: „Datenschutz und Datensicherheit in Bezug auf die Energieverbrauchsdaten ist ein sehr reales Problem für die Bürger."[8]

- **Niederlande:** Ein Gesetzesentwurf aus dem Jahr 2006 wurde abgelehnt, der die obligatorische Einführung von Smart Metern vorsah. Dies geschah teilweise aufgrund eines Berichts, in dem festgestellt wurde, dass die Datenschutzbelange im Zusammenhang mit dem Gesetzesentwurf gegen Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) – Recht auf Achtung des Privat- und Familienlebens – verstoßen könnten.[9]

In diesen und anderen Fällen hätten vorausgehende Initiativen zur Entwicklung und zur Vermittlung des Datenschutzes sowie Schutzmaßnahmen für Smart-Meter-Systeme eine Schlüsselrolle dabei gespielt, Rückschläge in der Entwicklung zu vermeiden.[10]

---

7 http://blogs.sfweekly.com/thesnitch/2010/12/smart_meters_west_marin.php

8 http://www.oipc.bc.ca/news/2011Releases/NR_SmartMeters_28July2011.pdf

9 http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf.

10 http://download.pwc.com/ie/pubs/smart_from_start.pdf

Privacy by Design

In der gleichen Zeit, in der sich das Verhältnis zwischen dem Verbrauchenden und dem Energieversorger verändert hat und die Erhebung von Stromverbrauchsdaten erweitert worden ist, sind weltweit die Grundsätze des Privacy by Design (PbD) angenommen worden. Von seinen Ursprüngen Mitte der 90er Jahre entwickelte sich PbD zu einem weltweiten Standard, der durch eine einstimmig angenommene Entschließung der Internationalen Datenschutzkonferenz im Oktober 2010 als „ein wesentlicher Bestandteil des grundlegenden Schutzes der Privatsphäre" anerkannt worden ist. Der PbD-Standard, von Beginn an bei der Ausgestaltung Schutzvorrichtungen einzuplanen, wurde auch ein Gütesiegel bei Datenschutz- und Datensicherheitsbewertungen von Smart Grid und Smart Metering, siehe Anhang A.

Privacy by Design bietet Organisationen die Möglichkeit, unter Berücksichtigung der Privatsphäre von Anfang an ein positives Gesamtbild zu erzeugen und dabei Datenschutz- und Funktionalitätsanforderungen in Einklang zu bringen. Die Bewegung in Richtung des Smart Grid und insbesondere Smart Metering bildet in seinem aktuellen Entwicklungszustand eine ideale Plattform für die Anwendung von Privacy by Design. Nachstehend geben wir einige Empfehlungen für Smart Meter-Initiativen auf der Grundlage der *Best Practices for Privacy on the Smart Grid*.[11]

Empfehlungen

1) Smart Meter-Initiativen sollten in dem gesamten Rahmen der Projektführung Grundsätze des Datenschutzes aufweisen und proaktiv datenschutzrechtliche Anforderungen in ihre Entwicklung einbinden, um datenschutzgefährdenden Ereignissen vorzubeugen.

Energieversorger sollten Datenschutzverträglichkeitsprüfungen, sog. *Privacy Impact Assessments (PIAs)*, oder gleichartige Bewertungsverfahren als Teil der Anforderungen und der Entwicklungsstufen von Smart Meter-Initiativen durchführen. Innerhalb dieser Evaluierung sollten zwei wichtige Erwägungen angestellt werden. Zuerst sollten Versorgungsunternehmen festlegen, welche auf Smart Meter basierten Informationen für die rechtmäßigen Ziele *erforderlich* sind (und auf welcher Ebene der Identifizierbarkeit), und nicht, welche Informationen durch Smart Meter *verfügbar* sind. Sodann sollten Mechanismen eingesetzt werden, die den Verbrauchenden die Kontrolle über alle verfügbaren, nicht notwendigen Informationen ermöglichen. Zweitens sollten nur die zur Erfüllung der

[11] http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf

festgelegten Zwecke erforderlichen personenbezogenen Daten die Wohnung des Verbrauchenden über den intelligenten Stromzähler verlassen. Um sicherzustellen, dass die Verbrauchenden stets die Kontrolle über ihre Daten behalten, ist es wesentlich, dass sie vollständig über die Daten, die ihre Wohnungen verlassen, informiert werden. Sie sollten in die Lage versetzt werden, darüber zu bestimmen, welche Daten übermittelt werden, und gegebenenfalls eingreifen können.

Studien haben gezeigt, dass Versorgungsunternehmen keine detaillierten Informationen über den Stromverbrauch einzelner Verbrauchender benötigen, um den Netzlastausgleich zu schaffen. Um den Fluss personenbezogener Daten so gering wie möglich zu halten, können Energieversorger Verfahren wie Anonymisierung, Pseudonymisierung oder Datenaggregation anwenden.[12] Es sollten lokale Gateways (Schnittstellen) für einzelne Gebäude oder kleine Wohnviertel eingesetzt werden, die den Verbrauchenden einen Einblick in ihren Energieverbrauch gewähren, ohne dass die Übermittlung von Informationen über identifizierbare Verbrauchende an den Energieversorger nötig ist. Solche Gateways sollten in der Regel nicht von außen zugänglich sein und mit festgelegten Zugangskontrollprofilen arbeiten, während die Kommunikation auf dem push-Verfahren basierten sollte (die durch das Gateway initiiert wird). Andere Maßnahmen, wie zum Beispiel größere Intervalle zwischen den einzelnen Ablesungen, können ebenso verhindern, dass detaillierte Profile über die Lebensführung erstellt werden. Selbstverständlich werden hohe technische Standards für die sichere Speicherung und den Zugriff auf die Daten unerlässlich sein.

2) Smart Meter sollten zum Schutz der Privatsphäre idealerweise datenschutzfreundliche Grundeinstellungen enthalten, ohne dass es einer Handlung seitens des Verbrauchenden bedarf

Um den Datenschutz zu gewährleisten, sollte die Privatsphäre idealerweise durch datenschutzfreundliche Grundeinstellungen geschützt werden. Der Datenschutz sollte sich in dem Modus „keine Aktion erforderlich" befinden; der Verbrauchende sollte nur dann handeln müssen, wenn er über die Grundversorgungsleistungen hinausgehende Dienste nutzen möchte, für die die *Bekanntgabe* weiterer Daten erforderlich ist, nicht aber für den *Schutz* der personenbezogenen Daten. Hier sollten zumindest zwei besondere Überlegungen angestellt werden. Erstens sollte, wenn dem Verbraucher mehrere Optionen angeboten werden (entweder im Hinblick auf die Art des Zählers oder auf dessen Grundeinstellung), die Standardeinstellung die datenschutzfreundlichste Einstellung sein. Zweitens sollte, selbst wenn sich die Verbrauchenden für eine detaillierte Erfassung ihrer Ver-

[12] Vgl. z.B. Kursawe, K., Danezis, G, Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid; and Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing; beide in Fischer-Hübner, S. and Hopper, N (Eds): *Proceedings of the 11th Privacy Enhancing Technologies Symposium,* Waterloo, ON, July 2011

brauchsdaten durch die intelligenten Zähler entschieden haben, vor jeder einzelnen Nutzung oder Weitergabe dieser Daten für andere als die Primärzwecke die informierte, positive Einwilligung dieser Personen eingeholt werden.

3) Der Datenschutz sollte ein wesentlicher Bestandteil bei der Ausgestaltung von Smart Meter-Systemen und -Anwendungen sein

Da Smart Meter-Initiativen in immer mehr Rechtssystemen weltweit zu finden sind, werden eine Reihe von Best Practices der Wirtschaft und rechtliche Anforderungen entwickelt. Diese werden die Bemühungen der Energieversorger und Dritter vorantreiben, datenschutzfreundliche Verfahren für die Erhebung, Nutzung und Übermittlung von Informationen aus den intelligenten Stromzählern zu schaffen. Die Regulierungsbehörden sollten als Grundsätze festlegen, dass die Verbrauchenden volle Transparenz und die Möglichkeit erhalten, den Fluss personenbezogener Daten zu kontrollieren und zu bestimmen. Detaillierte Muster über den Energieverbrauch des Einzelnen sollten nur der betroffenen Person zugänglich sein, es sei denn, diese gibt die Daten weiter.

Allerdings darf der Datenschutz nicht nur auf den rechtlichen oder administrativen Schutz angewiesen sein; er sollte ebenfalls in die Gestaltung der Technologie einfließen. An dem Scheidepunkt der Datenerhebung können Smart Meter eine maßgebliche Rolle dabei spielen zu definieren, welche Daten in das größere Smart Grid-Ökosystem gelangen, und in welcher Form dies geschieht.

4) Smart Meter-Initiativen sollten unnötige Kompromisse zwischen dem Datenschutz und anderen zulässigen Funktionen oder organisatorischen Zielen vermeiden

Datenschutz sollte nicht als Widerspruch zu der Funktionsvielfalt der intelligenten Stromzähler betrachtet werden. Die Verbrauchenden sollten nicht gezwungen werden, sich zwischen Datenschutz und Energieeffizienz/-einsparung zu entscheiden; vielmehr müssen Versorgungsunternehmen durch den Einsatz von *Privacy by Design* sicherstellen, dass alle gesetzmäßigen Ziele (einschließlich des Datenschutzes) in den Smart Meter–Initiativen erreicht werden.

5) Datenschutz und Datensicherheit sollten durchgehend aufrechterhalten werden – Schutz während des gesamten Lebenszyklus

Daten aus intelligenten Stromzählern – insbesondere solche, die einer Person zugeordnet werden können – sollten gut geschützt werden, sowohl bei der Speicherung als auch bei der Übermittlung. Dies erfordert die Entwicklung und Durchführung von Datensicherungsmaßnahmen auf dem Smart Meter selbst (wobei bestmöglich gewährleistet sein muss, dass das Gerät manipulationssicher ist und nicht mehr Daten als notwendig speichert), während der Datenübermittlung (Ver-

schlüsselung, Anonymisierung, Identifikation und Schutz der Metadaten), und während der Verarbeitung und Nutzung (auf das erforderliche Maß beschränkter Zugriff auf Daten, Sicherstellung, dass Dritte entsprechende Schutzstandards erfüllen, sichere Löschung am Ende der Nutzungsdauer etc.).

6) Smart Meter-Initiativen sollten erkennbar und transparent sein und rechenschaftspflichtige Geschäftspraktiken anwenden; gegenüber den Verbrauchenden sollte nachgewiesen werden, dass die Technologie in Übereinstimmung mit den festgelegten Zielen betrieben wird

Energieversorger sollten nachweisen können, dass die angewandten Methoden zur Integration des Datenschutzes in ihren Smart Meter-Initiativen den datenschutzrechtlichen Anforderungen des Projekts gerecht werden. Indem die Nachweisbarkeit der Einhaltung der Vorgaben grundlegender Datenschutzprinzipien in jeder Phase einer Smart Meter-Initiative sichergestellt ist, wird gewährleistet, dass der Energieversorger jederzeit für einen Audit durch Dritte bereit ist.

Für die Verwirklichung von Sichtbarkeit und Transparenz sind wichtige Grundsätze, dass die Verbrauchenden über die Verwendung der von intelligenten Zählern erhobenen personenbezogenen Daten informiert werden und ein durchsichtiger und zugänglicher Beschwerdeprozess eingerichtet wird. Die Verbrauchenden sollten die einfache technische Möglichkeit zur Festlegung von Zugangskontrollprofilen erhalten, um so zu bestimmen, wer welche personenbezogenen Daten erhält.

7) Smart Meter-Initiativen sollten so gestaltet sein, dass sie den Verbrauchendendatenschutz berücksichtigen – die Nutzenden sollen im Mittelpunkt stehen

Die Verbrauchenden sollten alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten und entsprechende Erklärungen erhalten, um ihren Energieverbrauch und ihren Datenschutz regeln zu können.

8) Rechtliche Rahmenbedingungen sollten die Einführung und die Nutzung des datenschutzfreundlichen Einsatzes von Smart Meter fördern.

Die in den vorstehenden Empfehlungen dargestellten Grundsätze sollten in national und international verbindliche Regelungen aufgenommen werden, sofern dies noch nicht geschehen ist.

ANHANG A –
Beispiele von *Privacy by Design* in Smart Grid-Konsultationsdokumenten

Expert Group 2: „Wenn der Datenschutz während der Ausgestaltungsphase des Smart Grid (‚Privacy by Design') berücksichtigt wird, ist es möglich, daraus nutzer- und unternehmensfreundliche Lösungen zu entwickeln"; „Seien Sie sich über das zukünftige Einschleichen von Funktionen bewusst und integrieren Sie Datenschutz- und Datensicherheitsaspekte frühzeitig in die Entwicklung durch die Anwendung der ‚Privacy (and Security) by Design'-Prinzipien."[13]

Artikel 29-Arbeitsgruppe: „Die Einführung intelligenter Verbrauchsmessverfahren muss so erfolgen, dass der Datenschutz von Anfang an mit einbezogen wird, und zwar nicht nur hinsichtlich der Sicherheitsmaßnahmen, sondern auch dadurch, dass die Menge der verarbeiteten personenbezogenen Daten minimiert wird."[14]

Europäische Kommission: „Die Task Force ‚Intelligente Netze' ist übereingekommen, dass ein ‚Privacy-by-Design'-Ansatz erforderlich ist. Dieser Ansatz wird in die Normen eingearbeitet werden, die von den europäischen Normungsgremien entwickelt werden."[15]

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Deutschland): „Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen."[16]

Public Interest Energy Research (PIER) Programm: „Datenschutzrechtliche Erwägungen müssen Entscheidungen zur Architektur und zur Ausgestaltung des Informationsflusses innerhalb dieses Netzwerks antreiben, genauso wie die Strategien zu Smart Grid-Daten, die von einer zunehmenden Anzahl von Einheiten gehalten werden, was sich bei der Erzielung des Nutzens dieser Investition als hilfreich erweisen wird. Da der Datenschutz in die technische Entwicklung integriert werden muss, kann er keine angemessene Berücksichtigung finden, wenn Richtlinien erst nach der vollständigen Entwicklung der Technologien geschaffen werden."[17]

---

13 http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

14 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_de.pdf

15 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:DE:PDF

16 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/80DSK_DatenschutzBeiDerDigitalenMessung.pdf?_blob=publicationFile

17 http://hes-standards.org/doc/SC25_WG1_N1475.pdf

Trans-Atlantic Consumer Dialogue (TACD): „Unterstützen Sie den Datenschutz und die Datensicherheit durch die Ausgestaltung, einschließlich der Datenminimierung, Anonymisierung und Aggregation sowie Modellen, bei denen die Kontrolle der Verbrauchenden über ihre Energieverbrauchsdaten im Vordergrund steht."[18]

National Institute of Standards and Technology (NIST): „Aufgrund des großen Vertrauens in die Technologie den Informationsaustausch muss die Berücksichtigung von Datenschutzrisiken ein Teil des heutigen Geschäftsmodells sein, und die Erwägung der Auswirkungen auf den Datenschutz sollte einen Teil der täglichen Geschäftsaktivitäten ausmachen."[19]

Ontario (Canada) Minister of Energy Directive: „Respektieren und schützen Sie die Privatsphäre der Kunden. Integrieren Sie frühzeitig Datenschutzanforderungen in die Planung und Gestaltung von Smart-Grids, einschließlich der Ausführung von Abschätzungen der Auswirkungen auf die Privatsphäre (Privacy Impact Assessments)".[20]

Center for Democracy and Technology & Electronic Frontier Foundation: „Die Annahme von Datenschutzbestimmungen, die den gesamten Satz an fairen Informationspraktiken umsetzen, wird jetzt, zu Beginn des Einsatzes von Smart Grids, für solide und anpassungsfähige Rahmenbedingungen für den Einbau des Datenschutzes in die sich weiter entwickelnden Smart Grids sorgen. Dadurch bekommen Versorgungsunternehmen und Innovatoren ein festes Rahmenwerk, auf dem sie aufbauen können."[21]

Smart Grid Canada: „Der erfolgreiche Einsatz von Smart Grid beruht letztlich auf dem Vertrauen der Verbrauchenden. Datenschutzrechtliche Bedenken und andere öffentliche Belange, die eine Bedrohung für das Vertrauen der Verbrauchenden darstellen, müssen angegangen werden. Es ist von höchster Priorität, die Probleme in Bezug auf die Integrität zu bestimmen, die Entwicklung von Lösungen und Standards auszuweiten und sie in die in Kanada eingesetzten Smart-Grid-Produkte und -Dienstleistungen einzubauen."[22]

18 http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=

19 http://epic.org/privacy/smartgrid/NIST_Smartgrid_Priv_Guidelines.pdf

20 http://www.wise.uwaterloo.ca/SmartGrid/Minister_directive_smart_grid_20101123.pdf

21 http://www.eff.org/files/PoliciesandProcedures_15Oct2010_OpeningComment.pdf

22 http://sgcanada.org/media/2011/04/Smart-Grid-Priorities-for-Canada-in-2011.pdf

Datenschutz und elektronisches Micropayment im Internet

– Übersetzung –

Hintergrund

Öffentliche Äußerungen prominenter Medienunternehmen deuten darauf hin, dass sich die Ära der kostenfreien Nutzung von Online-Medien ihrem Ende nähern könnte. Verschiedene Anbieter von Online-Diensten und insbesondere Online-Zeitungen weltweit beginnen den Zugriff auf ihre Dienste ausschließlich gegen eine Gebühr anzubieten.

Die diskutierten Geschäftsmodelle reichen von Abonnements, bei denen ein Zugriff auf Basis einer monatlichen Gebühr angeboten wird, bis zu „pay per view"-Geschäftsmodellen, bei denen ein kleiner Geldbetrag für den Zugriff auf eine Einzelinformation gezahlt wird (sog. „Micropayment", z. B. für einen einzelnen Artikel in einer Online-Zeitung oder einen Video-Clip).

Zusätzlich gestattet die letzte Generation von Mobiltelefonen die Installation von Zugriffsmöglichkeiten auf Online-Mediendienste über sog. „Apps". Verschiedene Anbieter von mobilen Endgeräten haben begonnen, eigene Verteilungsplattformen für solche „Apps" anzubieten, einschließlich damit verbundener Zahlungsdienste.

Gleichzeitig werden in sozialen Netzwerkdiensten sog. „Drittanwendungen" („Third-Party Applications") zunehmend populär. Viele dieser Drittanwendungen werden gegen Gebühr von einem anderen Anbieter als dem des sozialen Netzwerks angeboten. Facebook hat z. B. kürzlich die Einführung einer eigenen Währung „facebook coins" zum Bezahlen für Dienste innerhalb seines sozialen Netzwerks angekündigt.

Diese Entwicklungen können zu Beeinträchtigungen der Privatsphäre von Nutzern solcher Dienste führen, wenn die grundlegenden Prinzipien des Schutzes der Privatsphäre nicht beachtet werden. Tatsächlich haben die Anbieter solcher Micropayment-Systeme die Möglichkeit, Werbeeinnahmen durch die Auswertung der detaillierten personenbezogenen Transaktionsdaten zu generieren, die sie erlangen könnten.

Die Arbeitsgruppe hat bereits früher regelmäßig die Notwendigkeit der Wahrung der Anonymität im größtmöglichen Ausmaß als einen essentiellen Aspekt des

Schutzes der Privatsphäre im Internet betont[1]. Im Besonderen hat die Arbeitsgruppe die Notwendigkeit des Erhalts der Möglichkeit zum anonymen Zugriff auf digitale Medien, und besonders beim digitalen Fernsehen unterstrichen[2]. In jüngerer Zeit sind diese Prinzipien erneut in dem Konzept des „privacy by design" bestätigt worden[3].

Diese Prinzipien könnten gefährdet sein, wenn der Zugang zu Online-Medien und anderen Diensten gegen Gebühr angeboten wird, ohne dass anonyme Zahlungsmethoden zur Verfügung stehen. Wir könnten in eine Situation geraten, in der Nutzende sich allein zum Zweck der Bezahlung für einen Dienst identifizieren müssen.

Insbesondere besteht ein Risiko, dass „Micropayment"-Vorgänge (z. B. das Bezahlen für das Ansehen eines spezifischen Artikels in einer Online-Zeitung) zum Entstehen von Nutzungsdaten führen, die Spuren darüber enthalten, wer welchen Artikel in welchem Online-Medium zu welcher Zeit gelesen hat.

Gegenwärtig sind im Online-Bereich nur wenige Zahlungsmittel verfügbar, die denselben Grad von Anonymität wie Bargeld in der Offline-Welt haben. Die meisten der gängigen Zahlungsmethoden (z. B. Kreditkarten, Mobiltelefone, Zahlungsdiensteanbieter oder über Bankkonten) erlauben im Gegenteil keine anonyme Nutzung.

Während anonyme Guthabenkarten erhältlich sind, wird die Zahlung mit diesen Mitteln gegenwärtig nur von einer Minderheit von Online-Diensteanbietern angeboten.

Gleichzeitig ist in Deutschland ein Gesetzentwurf durch die deutsche Bundesregierung vorgelegt worden, der Anbieter von Online-Zahlungsdiensten zwingen würde, personalisierte Zahlungsmittel auch für Micropayment-Vorgänge anzubieten. Dies wird auf die Annahme gestützt, dass solche Dienste für Geldwäsche missbraucht werden könnten.

---

1 Vgl. Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet – „Budapest-Berlin Memorandum", angenommen auf der 20. Sitzung in Berlin, Deutschland am 18./19. November 1996; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf

2 Vgl. Arbeitspapier Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen, 42. Sitzung, Berlin, Deutschland, 4./5. September 2007; http://www.datenschutz-berlin.de/attachments/350/digit_de.pdf

3 Vgl. 32. Internationale Konferenz der Datenschutzbeauftragten, Jerusalem, Israel, 27./29. Oktober 2010: Resolution zu privacy by design; http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

Empfehlungen

Im Lichte des oben Gesagten gibt die Arbeitsgruppe die folgenden Empfehlungen:

Gesetzgeber sollten von einem gesetzlichen Verbot von anonymen Mitteln zum Micropayment Abstand nehmen. Es muss möglich bleiben, alltägliche Einkäufe auch im Online-Bereich zu tätigen, ohne sich einzig für das Bezahlen identifizieren zu müssen.

Gesetzgeber sollten das Angebot anonymer oder wenigstens pseudonymer Bezahldienste – insbesondere für Micropayment-Vorgänge – in ihrer nationalen Gesetzgebung vorschreiben, wo dies nicht bereits der Fall ist. Dieser Gesichtspunkt sollte auch in dem laufenden Prozess der Evaluierung und möglichen Änderung nationaler und internationaler Instrumente zum Datenschutz in Betracht gezogen werden (z. B. der EU-Richtlinie 95/46, der Konvention 108 des Europarats oder der OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten).

Diensteanbieter sollten anonyme oder wenigstens pseudonyme Möglichkeiten zum Bezahlen ihrer Dienste anbieten. Sie sollten die Prinzipien des „privacy by design“ in ihren Angeboten von Anfang an berücksichtigen.

Nutzer von Online-Diensten, insbesondere von Online-Mediendiensten, sollten darauf hingewiesen werden, dass ihre Wahl einer Zahlungsmethode einen direkten Einfluss auf den Grad des Schutzes der Privatsphäre haben kann, der bei der Nutzung dieser Dienste garantiert werden kann. Sie sollten sich ausführlich über verschiedene verfügbare Zahlungsmethoden bei Diensteanbietern einzelner Plattformen informieren und anonyme oder wenigstens pseudonyme Bezahlungsmethoden fordern und wählen, wo immer dies möglich ist.

B. Dokumente zur Informationsfreiheit

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließungen der 22. Konferenz am 23. Mai 2011 in Bremen

Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger!

Neue Technologien rufen bei Bürgerinnen und Bürgern nicht nur positive Reaktionen hervor, sondern stoßen häufig auf Skepsis oder lösen Ängste aus. Grund hierfür ist nicht selten eine unzureichende Informationslage bis hin zur Zurückhaltung von Informationen für Verbraucherinnen und Verbraucher. Wer das Potential neuer Technologien ausschöpfen möchte, muss mit offenen Karten spielen. Das bedeutet, dass nicht nur Vorteile, sondern auch Risiken offengelegt werden müssen, um einen demokratischen Diskurs und jedem Menschen eine informierte Willensbildung zu ermöglichen.

Ein aktuelles Beispiel ist der Einsatz von Nanotechnologie: Dabei geht es um künstlich hergestellte winzige Partikel (Nanomaterial), die heute schon in Baustoffen, Textilien sowie Kosmetika und zukünftig immer mehr in verbrauchernahen Produkten wie etwa Lebensmitteln eingesetzt werden. Nanotechnologie soll Produkte zum Beispiel robuster machen. In einem Bericht aus dem Jahre 2009 (nano.DE-Report 2009) geht das Bundesministerium für Wissenschaft und Forschung davon aus, dass nanotechnologisches Know-how in den Bereichen Gesundheit, Informations- und Kommunikations- sowie Energie- und Umwelttechnik immensen Einfluss auf die Wertschöpfung nehmen wird. Ein Weltmarktvolumen von 15 Prozent der globalen Güterproduktion wird prophezeit.

Wenigen ist dies bekannt, denn es besteht derzeit keine Pflicht, Produkte, die Nanomaterial enthalten, zu kennzeichnen. Erst 2013 wird eine solche Pflicht für Kosmetika bestehen. Für Lebensmittel wird die Kennzeichnungspflicht noch diskutiert. Zugleich – stellt die Nano-Kommission der Bundesregierung in ihrem Aktionsplan Nanotechnologie 2015 fest – fehlen vielfach grundlegende Kenntnisse über die Risiken bei der Exposition mit Nanomaterialien.

Die Informationsfreiheitsbeauftragten in Deutschland fordern die Bundesregierung auf, sich bei den Diskussionen und Verhandlungen auf europäischer Ebene dafür einzusetzen, dass Bürgerinnen und Bürgern ein direkter Zugang zu Infor-

mationen über Nanotechnologie in Produkten ermöglicht wird. Deshalb ist es notwendig, dass auch Bürgerinnen und Bürger Zugang insbesondere zu dem auf europäischer Ebene diskutierten Nanoproduktregister erhalten. Beim Einsatz neuer Technologien muss verstärkt auf Aufklärung, Transparenz und Einbindung der Menschen gesetzt werden.

Informationsfreiheit – Lücken schließen!

Der Gedanke der Transparenz staatlichen Handelns ist beim Bund und den meisten Ländern seit einigen Jahren angekommen, wie die Informationsfreiheitsgesetze von Brandenburg (1998), der meisten anderen Länder und auch das Informationsfreiheitsgesetz des Bundes (2005) zeigen.

Vor diesem Hintergrund begrüßt die Konferenz der Informationsfreiheitsbeauftragten die Absicht der neuen Landesregierung von Baden-Württemberg, auch dort ein Informationsfreiheitsgesetz auf den Weg zu bringen. Dabei sollte allerdings, wie in Rheinland-Pfalz vorgesehen, dem Landesbeauftragten für den Datenschutz die Aufgabe der oder des Beauftragten für die Informationsfreiheit übertragen werden. Diese unabhängige Funktion eines oder einer Informationsfreiheitsbeauftragten fehlt gegenwärtig auch noch in Thüringen. Bayern, Hessen, Niedersachsen und Sachsen lehnen dagegen beharrlich jede gesetzliche Regelung für einen Anspruch der Bürgerinnen und Bürger auf Zugang zu behördlichen Informationen ab.

Dies führt zu absurden Ergebnissen: So haben die Bürgerinnen und Bürger gegenüber den Jobcentern mit gemeinsamer Trägerschaft durch Bundesagentur für Arbeit und Kommune auch in den vier Ländern ohne Informationsfreiheitsgesetze einen Anspruch auf der Grundlage des Bundesgesetzes. Dagegen besteht gegenüber den Jobcentern der Optionskommunen in ausschließlich kommunaler Trägerschaft in diesen Ländern kein Anspruch auf Informationszugang.

Unbefriedigend ist auch, dass die Bürgerinnen und Bürger bei Ersuchen auf Zugang zu Verbraucher- und Umweltinformationen nicht durchgängig die gesetzlich garantierte Möglichkeit haben, sich an die Informationsfreiheitsbeauftragten zu wenden. Eine Ombudsfunktion ist zwar in den meisten Informationsfreiheitsgesetzen vorgesehen, fehlt aber für Umwelt- und Verbraucherinformationen auf Bundesebene und in vielen Ländern.

Deshalb appelliert die Konferenz an die Gesetzgeber in Bund und Ländern, diese Regelungsdefizite zu beseitigen und „flächendeckend“ allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informationsfreiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln.

2. Entschließung der 23. Konferenz am 28. November 2011 in Berlin

Informationsfreiheit ins Grundgesetz und in die Landesverfassungen

Demokratie und Rechtsstaat können sich nur dort wirklich entfalten, wo auch die Entscheidungsgrundlagen staatlichen Handelns offen gelegt werden. Bund und Länder müssen ihre Bemühungen weiter verstärken, für mehr Transparenz staatlichen Handelns zu sorgen. Eine verfassungsrechtliche Verankerung der Informationsfreiheit ist geboten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland tritt dafür ein, den Anspruch auf freien Zugang zu amtlichen Informationen in das Grundgesetz und die Landesverfassungen – soweit noch nicht geschehen – aufzunehmen. Staatliche Stellen müssen die ihnen vorliegenden Informationen grundsätzlich öffentlich zugänglich machen.

II. Live-Übertragung der Sitzungen der Bezirksverordnetenversammlung (BVV) via Internet

I. Sachverhalt

Im Zusammenhang mit der Anfrage des Geschäftsordnungsausschusses der BVV Treptow-Köpenick an die Datenschutzbeauftragte des Bezirksamtes kam die Frage auf, warum gegen die Live-Übertragung der Sitzungen der BVV Bedenken bestehen, während die Plenarsitzungen des Berliner Abgeordnetenhauses übertragen werden.

II. Rechtliche Bewertung

Die Unterschiede in der Bewertung der Übertragungen sind grundsätzlich den kommunal- und verfassungsrechtlichen Unterschieden zwischen der Bezirksverordnetenversammlung und dem Abgeordnetenhaus geschuldet.

1. Live-Übertragungen aus dem Abgeordnetenhaus

Die Zulässigkeit der Live-Berichterstattung aus dem Parlament wird aus Art. 42 Abs. 3 VvB gefolgert, wonach Verhandlungen des Abgeordnetenhauses öffentlich sind.

Das Abgeordnetenhaus ist das Landesparlament des Landes Berlin gem. Art. 38 Abs. 1 VvB. In Anlehnung an Art. 42 Abs. 1 Satz 1 GG werden aus dem Öffentlichkeitsgebot die Sitzungsöffentlichkeit und die Berichterstattungsöffentlichkeit abgeleitet.[1] Unter Beachtung des Wandels der Mediennutzung wird davon ausgegangen, dass erst durch den Zugang der Massenmedien zu den Sitzungen die für die Kontrolle der Abgeordneten und der Regierung notwendige Öffentlichkeit hergestellt wird.[2] Die Öffentlichkeit der Sitzungen stellt somit die Transparenz des legislativen Handelns sicher. Sie dient darüber hinaus im Hinblick auf die Artikulations- und Öffentlichkeitsfunktion des Parlaments der politischen Willensbildung, und schließlich hat sie Bedeutung für die Wahlentscheidung des einzelnen Bürgers, sodass sie insgesamt sehr eng mit den Aufgaben und Funktionen der Volksvertretung zusammenhängt.[3] Aus dieser für den demokratischen Parlamen-

[1] *Morlok* in Dreier GG, Band II, Art. 42 Rn. 27.

[2] *Versteyl* in v. Münch/Kunig GG Bd. 2 Art. 42 Rn. 8.

[3] *Magiera* in Sachs GG Art. 42 Rn. 1.

tarismus zentralen Zweckbestimmung entsteht nach allgemeiner Ansicht die Pflicht, sowohl der Presse als auch den anderen Massenmedien Zugang zu den Parlamentsverhandlungen zu gewähren, wobei hiervon teilweise auch das Recht zur Direktübertragung abgeleitet wird.[4]

2. Unterschiede zwischen dem Landesparlament und der BVV

Die BVV ist kein Parlament im staatsrechtlichen Sinne. Auch wenn augenscheinlich etliche Gemeinsamkeiten bestehen, unterscheiden sich die beiden Organe erheblich voneinander.

a) Unterschiedlicher Aufgabenkatalog

Die BVV ist als Kollegialorgan der bezirklichen Selbstverwaltung Teil der Exekutive gem. Art. 72 Abs. 1 VvB, § 2 Bezirksverwaltungsgesetz (BezVG). Anders als im Rahmen der Verhandlungen des Abgeordnetenhauses geht es in der BVV nicht vorrangig um die Vorbereitung parlamentarischer Beschlüsse, die zum überwiegenden Teil auf abstrakte Maßnahmen wie der Vorbereitung und Verabschiedung abstrakt-genereller Regelungen abzielen. Insofern gilt es zu erörtern, inwiefern sich die Aufgaben der BVV von denen eines Parlamentes unterscheiden, um die Frage zu klären, ob sich hieraus zwingende Argumente für die abweichende Beurteilung der Zulässigkeit der Sitzungsübertragungen ergeben.

Die Zuständigkeiten der BVV ergeben sich aus den Art. 69, 72, 73, 74, 76 VvB und aus dem Bezirksverwaltungsgesetz:

Die **Grundlinienkompetenz** und das Initiativrecht ermöglichen es der BVV, Empfehlungen und Ersuchen an das Bezirksamt zu richten. Es handelt sich dabei jedoch nicht um eine umfangreiche Befugnis zum Erlass verbindlicher Verwaltungsvorschriften oder um ein allgemein-politisches Mandat. Die Literatur misst den Vorschriften Art. 72 Abs. 1 VvB und § 12 Abs. 1 Satz 2 BezVG dahingehend lediglich deklaratorischen Charakter bei.[5]

Die BVV überprüft die Führung der Geschäfte des Bezirksamtes (BA) im Rahmen der **Kontrollkompetenz** gem. Art. 72 VvB i. V. m. § 12 Abs. 1 Satz 2 BezVG.[6]

Die BVV übt **Entscheidungsbefugnisse** gem. § 12 Abs. 2 BezVG aus, sofern es um den Bezirkshaushaltsplan, die Zustimmung zu Rechtsverordnungen

4 *Magiera* in Sachs GG Art. 42 Rn. 3; *Versteyl* in v. Münch/Kunig GG Bd. 2 Art. 42 Rn. 8.

5 Ottenberg BezVG § 12 Rn. 1; Driehaus VvB, Art. 72 Rn. 1; Zivier, Verfassung und Verwaltung von Berlin. 90.4.2.

6 Zivier, Verfassung und Verwaltung von Berlin. 90.4.4.

zur Festsetzung von Bebauungs- und Flächennutzungsplänen und anderen baurechtlichen Akte. geht, sie beschließt Betriebssatzungen der Eigenbetriebe und übt auch ein allgemeines Entscheidungsrecht § 12 Abs. 3 BezVG aus.[7]

Gem. § 16 Abs. 1 BezVG wählt die BVV u.a. die Mitglieder des Bezirksamtes und die Bürgerdeputierten, sie stellt außerdem die Vorschlagslisten für Schöffen zusammen. Gem. §§ 7, 9 BezVG bestimmt sie einen Vorstand und bildet Ausschüsse. Weitere **Wahlbefugnisse** können sich aus Spezialgesetzen ergeben.[8]

Grundsätzlich kann die BVV **Meinungsäußerungen oder Resolutionen** tätigen, sofern hierdurch nicht der Kompetenzbereich eines anderen Staatsorgans tangiert wird.[9]

Der überwiegende Teil der Zuständigkeiten erfordert in den Sitzungen und den Redebeiträgen abstrakte Auseinandersetzungen mit Sachthemen, sodass sich Wertungen zu der Öffentlichkeitsfunktion des Parlamentes in bestimmten Punkten übertragen lassen:

Sofern die BVV die **Grundlinien** der Verwaltungspolitik festsetzt und Empfehlungen an das BA richtet, werden die Redebeiträge in den Sitzungen ganz überwiegend allgemein gehaltene, abstrakte Äußerungen enthalten. Daher ergibt sich aus der Tatsache, dass kommunalpolitische Themen aus dem örtlichen Wirkungskreis des Bezirks behandelt werden, nicht zwingend ein Wertungsunterschied zu den Sachverhalten, die im Abgeordnetenhaus diskutiert werden. Diese Wertung gilt ebenfalls dann, wenn die BVV **Meinungsäußerungen** oder Resolutionen hervorbringt, auch hierbei wird es sich stets um abstrakte Anmerkungen handeln. Aus diesen Aufgaben der BVV ist die unterschiedliche Bewertung der Übertragung der Sitzungen daher nicht zu erklären.

Im Rahmen der **Entscheidungsbefugnisse** gem. § 12 BezVG befindet die BVV nicht über formell-materielle Gesetze; als Teil der Exekutive macht sie lediglich von Ermächtigungen des parlamentarischen Gesetzgebers Gebrauch und erlässt in diesem Rahmen sog. nur-materielle Gesetze in der Form der Satzung oder der Rechtsverordnung (bzw. sie erteilt ihre Zustimmung zu den Verordnungen des BA). Rechtsverordnung und Satzungen sind aber abstrakt-generelle Regelungen und daher hinsichtlich ihrer Formulierung mit formell-materiellen Gesetzen vergleichbar. Sofern demensprechend

[7] Zivier, Verfassung und Verwaltung von Berlin. 90.4.5.

[8] Zivier, Verfassung und Verwaltung von Berlin. 90.4.6.

[9] Zivier, Verfassung und Verwaltung von Berlin. 90.4.7.

vor der Beschlussfassung in der Sitzung ein untergesetzlicher Rechtsakt vorbereitet und diskutiert wird, unterscheiden sich die Äußerungen in ihrer Qualität oder Intensität nicht von solchen, wie sie im Zusammenhang mit der Beschlussfassung im Abgeordnetenhaus getätigt werden. Sollte im konkreten Fall ein Satzungsbeschluss insbesondere ein Bebauungsplan den betroffenen Personenkreis in besonderer Weise eingrenzen und sollten in diesem Zusammenhang personenbezogene Daten von Privatpersonen offenbart werden, so wird der Vorsitzende grundsätzlich die Nichtöffentlichkeit der Sitzung herstellen. Allein aus der Tatsache, dass bestimmte Themen nicht in der öffentlichen Sitzung erörtert werden, ergibt sich jedoch noch kein grundlegender Unterschied zu den Parlamenten, denn auch dort besteht gem. Art. 42 Abs. 1 Satz 2 GG bzw. Art. 42 Abs. 2 VvB die Möglichkeit, die Öffentlichkeit aus der Sitzung auszuschließen. Betrachtet man daher nur den öffentlichen Teil der BVV-Sitzungen, ergeben sich hinsichtlich der Entscheidungskompetenz der BVV keine grundlegenden, die stark abweichende Beurteilung der Sitzungsübertragungen rechtfertigenden Unterschiede zu der Berichterstattung aus dem Abgeordnetenhaus.

Hinsichtlich der Wahlbefugnisse gilt es zu differenzieren: Sofern die **Bezirksamtsmitglieder gewählt** werden, so geschieht dies entsprechend den Wahlvorschlägen der Fraktionen. Die Bezirksamtsmitglieder selbst erfüllen politische Selbstverwaltungsaufgaben und bedürfen des politischen Vertrauens. Sollten im Rahmen der Nominierung die persönlichen Verhältnisse einzelner Anwärter erörtert werden, so ist zu berücksichtigen, dass diese sich für ein politisches, öffentliches Amt bewerben. Auch wenn diesbezüglich konkrete Personalien erörtert werden, so unterscheidet sich die Wahl der Bezirksamtsmitglieder daher nicht in qualitativer Weise von den in den Parlamenten zu erörternden Personalfragen, sodass auch diese Aufgabe keine andere Bewertung rechtfertigt.

Diese Beurteilung gilt erst recht, wenn besondere **politische Positionen** in der BVV selbst gem. § 7 Abs. 1 BezVG besetzt werden, sodass die Wahl des Vorstehers, seines Vertreters und der übrigen Vorstandsmitglieder keinen sachlichen Unterschied in der Bewertung bedeuten kann.

Sofern aus der Mitte der BVV Ausschüsse gem. § 15 GO BVV und der Ältestenrat gem. § 9 BezVG gebildet werden, gilt diese Beurteilung ebenfalls entsprechend.

Anders ist die Sachlage zu bewerten, wenn **Ehrenämter** wie der Patientenfürsprecher gem. § 26 LKG, Bürgerdeputierte gem. Art. 73 Abs. 2 Satz 2 VvB oder andere Ehrenämter besetzt werde sollen. Im Unterschied zu den parlamentarischen Personalfragen werden hierbei Bürger für besondere Positionen und Aufgaben ausgewählt. Diese Wahlbefugnisse finden keine direkte

Entsprechung in den Befugnissen und Aufgaben des Abgeordnetenhauses. Am ehesten lässt sich diese Befugnis mit dem Auswahlverfahren bei der Einberufung bestimmter Sonderausschüsse oder der Enquete-Kommission gem. Art. 44 Abs. 3 VvB, §§ 20 Abs. 2, 23. der GO des Abgeordnetenhauses vergleichen, bei denen auch Sachverständige als Mitglieder bestimmt werden können. Demnach ist es auch im parlamentarischen Betrieb nicht gänzlich untypisch, bestimmte Positionen mit Bürgern zu besetzen, sodass sich aus der entsprechenden Wahlbefugnis der BVV eine andere Bewertung der Sitzungsübertragungen nicht erklären lässt.

Sofern für die Bekleidung der Position nicht in besonderer Weise die persönlichen und sachlichen Verhältnisse erörtert werden müssen, steht der Erörterung solcher Personalfragen in öffentlicher Sitzung nichts entgegen, schließlich bekleiden auch die Ehrenamtlichen freiwillig ein öffentliches Amt.

Anders muss die Bewertung jedoch ausfallen, wenn die BVV die Vorschlagslisten für **Schöffen** zusammenstellt. Hierbei kann unter Umständen in besonders intensiver Weise auf die persönlichen Verhältnisse der betroffenen Personen einzugehen sein. Da die Schöffen gem. § 36 Abs. 2 GVG alle Gruppen der Bevölkerung repräsentieren sollen, wird dabei auch auf die soziale Stellung einzugehen sein. Es ist nicht auszuschließen, dass hierbei auch Vermögens- und gesundheitliche Verhältnisse oder zurückliegende Ermittlungsverfahren erörtert werden. Zudem beziehen sich diese Unterredungen auch auf Personen, die sich nicht zuvor für ein Schöffenamt beworben haben, sodass sie zuvor keine Gelegenheit haben, zu den einzelnen Punkten Stellung zu nehmen.[10] Diese Wahlbefugnis findet keine Entsprechung im Aufgabengebiet des Abgeordnetenhauses, sie ist allerdings aufgrund der zu erörternden sensiblen personenbezogenen Daten der Betroffenen stets in nicht öffentlicher Sitzung auszuüben, wie es auch in § 32 Abs. 4 der GO BVV vorgesehen ist.

Entsprechend fällt auch die Beurteilung hinsichtlich der von der BVV durchzuführenden Abberufungen der von ihr eingesetzten und gewählten Personen aus: Da stets persönliche Verhältnisse erörtert werden, sind diese Tagesordnungspunkte ausschließlich in nicht öffentlicher Verhandlung zu klären.

Abschließend lässt sich daher aus den Wahlbefugnissen der BVV – sofern sie im öffentlichen Teil der Sitzung erörtert werden – kein Hinweis für den Grund der unterschiedlichen Beurteilung der Sitzungsübertragungen ableiten.

---

10 vgl. zu den datenschutzrechtlichen Aspekten der Schöffenvorschlagsliste TB 32 4.1.9 des ULD Schleswig-Holstein und TB 27 4.3.6, sowie den Beitrag des ULD unter https://www.datenschutzzentrum.de/material/themen/divers/schoeffenwahl.htm. (zuletzt abgerufen am 28.07.2011).

Konkrete Bezüge zu individuellen Personen können auch im Rahmen der **Kontrollbefugnisse** der BVV zu erörtern sein. Insbesondere bei der Untersuchung der Durchführung einzelner Geschäfte der Bezirksämter können häufig auch die individuellen Verhältnisse oder Geschäftsinteressen einzelner Bürger betroffen sein. § 12 Abs. 3 BezVG zeigt dies im Hinblick auf das Aufhebungs- und Selbstentscheidungsrecht besonders deutlich, wenn auch die BVV von diesem Recht in der Praxis äußerst selten Gebrauch macht.[11] Wie bereits bei anderen oben angesprochenen Punkten ist in solchen Fällen nicht öffentlich zu tagen.[12]

Auch wenn daher mit der Kontrollkompetenz der BVV ein Tätigkeitsfeld existiert, das überwiegend von der Erörterung konkreter Verhältnisse geprägt ist, lässt sich hieraus nicht ein solch eklatanter Unterschied zu den Aufgaben des Abgeordnetenhauses formulieren, als dass dies allein eine unterschiedliche Bewertung der Frage nach der Rechtmäßigkeit einer Sitzungsübertragung rechtfertige.

Aus dem Vergleich der unterschiedlichen Aufgaben der Bezirksverordnetenversammlung und dem Abgeordnetenhaus ergeben sich demnach keine zwingenden Argumente gegen die Zulässigkeit einer Übertragung der Sitzungen.

b) Unterschiedliche Bedeutung der Öffentlichkeit

Es gilt allerdings zu berücksichtigen, dass das Parlament entsprechend der vom BVerfG formulierten Wesentlichkeitstheorie die zentralen Fragen der Ausübung der Grundrechte sowie die Rahmenbedingungen der Teilhaberechte und staatlichen Schutzpflichten und die elementaren Grundsatzfragen durch formell-materielles Gesetz zu regeln hat und die „wesentlichen Entscheidungen“ somit nicht an die Verwaltung delegieren darf.[13] Im Lichte dieser Aufgabe erklärt sich auch die zentrale Bedeutung der Öffentlichkeitsfunktion des Parlaments: Jegliches Gesetzesvorhaben ist von der Initiative bis zum Beschluss für die Bevölkerung nachvollziehbar. Es soll sowohl der öffentliche Diskurs durch die Erörterung im Parlament im Sinne der Willensbildungsfunktion geprägt werden als auch andersherum im Sinne der Artikulationsfunktion die öffentliche Diskussion ihren Niederschlag in den parlamentarischen Auseinandersetzungen finden. Dieser zentrale Punkt kann nicht ohne Weiteres auch für die Funktion der BVV herangezogen werden, denn im Rahmen der untergesetzlichen Normgebung erreicht die Bedeutung der Sitzungsöffentlichkeit der BVV nicht dieselbe zentrale Bedeutung wie die Öffentlichkeit des Abgeordnetenhauses.

---

11 Ottenberg, § 12 Rn. 19 f.

12 Ottenberg, § 17 Rn. 8.

13 vgl. BVerfG 33, 125 (Facharztbeschluss); *Dreier* in Dreier GG, Band II, Art. 20 Rn. 110, 103.

Andererseits lässt sich das Gebot der Transparenz der Verwaltungsarbeit mittelbar aus dem zentralen Prinzip der Volkssouveränität gem. Art. 20 Abs. 2 Satz 1 GG ableiten. Aus diesem Grund haben die Sitzungen der BVV gem. § 8 Abs. 6 Satz 1 BezVG grundsätzlich öffentlich stattzufinden. Die BVV ist als originäre Vertretung der Einwohner des Bezirks angehalten, den Bürgern eine öffentliche Debatte über die Themen des örtlichen Wirkungskreises zu ermöglichen.[14] Insbesondere die Diskussion über den Bezirkshaushaltsplan soll im Fokus der (Bezirks-) Öffentlichkeit stattfinden. Dementsprechend relativiert sich die unterschiedliche Bedeutung der Öffentlichkeitsfunktion im Lichte der Wesentlichkeitstheorie durch das Erfordernis, die Aufgabenerfüllung der BVV für den Bürger transparent zu gestalten, zumal der Sinn der rechtlichen Selbstverwaltung gerade in der Volks-, Orts- und Sachnähe gesehen wird.[15]

Unter diesen Gesichtspunkten rechtfertigt sich allein aus dem Verweis auf die zentrale Bedeutung des Parlaments als unmittelbare Volksvertretung und Träger der wesentlichen Entscheidungen keine unterschiedliche Bewertung der Sitzungsübertragungen.

c) Unterschiedliches Diskussionsklima

Insbesondere ergibt sich auch keine andere Beurteilung aus der Annahme, dass in den Sitzungen der BVV die Verhältnisse einzelner Personen oder Personengruppen besonders heftig oder kontrovers diskutiert und dabei personenbezogene Daten offenbart werden. Als Organ der öffentlichen Verwaltung ist die BVV gem. § 2 Abs. 1 BlnDSG vom persönlichen Anwendungsbereich des BlnDSG umfasst. Demensprechend richtet sich die Zulässigkeit der Datenverarbeitung grundsätzlich nach § 4 Abs. 1 BlnDSG. Sollte es im Rahmen der oben erörterten Aufgabenerfüllung erforderlich sein, auf die persönlichen oder sachlichen Verhältnisse eines Bürgers derart einzugehen, dass hierbei konkrete Einzelangaben über bestimmte oder bestimmbare Personen in den Sitzungen offenbart werden, richtet sich die Beurteilung einer solchen Übermittlung – im Sinne einer Bekanntgabe an Dritte – nach §§ 6 Abs. 1 Satz 1 Nr. 1, 9 Abs. 1 BlnDSG i. V. m. Art. 72 ff VvB, §§ 12 ff. BezVG. Im Rahmen der Bestimmung der Erforderlichkeit gem. § 9 Abs. 1 BlnDSG sind umfangreiche Verhältnismäßigkeitserwägungen anzustellen. Hierbei sind insbesondere datenschutzrechtliche Grundsätze wie sie bspw. in §§ 5 ff. BlnDSG kodifiziert sind, zu beachten. Gem. § 5 BlnDSG hat die verarbeitende Stelle, hier also die BVV, sicherzustellen, dass organisatorische Maßnahmen getroffen werden, um den Schutzzweck des Datenschutzgesetzes zu realisieren. Konkret ergibt sich hieraus die Pflicht der BVV, diejenigen Tagesordnungspunkte in nicht-öffentlicher Sitzung zu erörtern, in deren Zusammenhang

14 Ottenberg, § 1 Rn. 17.

15 Machalet, Die Berliner Bezirksverwaltung S. 49 m.w.N.

personenbezogene Daten erörtert werden müssen, sodass sich die Verordneten bereits bei der Aussprache über die Tagesordnung der nächsten Sitzung darüber Gedanken machen müssen, ob es einer Ausnahme vom Grundsatz der Öffentlichkeit bei einem der konkret anstehenden Themenkomplexe bedarf. Aus dieser Pflicht zur datenschutzkonformen Aufgabenerfüllung ergibt sich somit der Schluss, dass es im Grunde keine Situation geben darf, in der personenbezogene Daten eines Bürgers ohne dessen Einwilligung im öffentlichen Teil der Sitzung explizit erörtert werden.

d) Unterschiede zwischen Bezirksverordneten und Abgeordneten

Auch wenn die Verordneten gem. Art. 70 VvB nach denselben Grundsätzen wie die Abgeordneten gewählt werden, üben sie ein ehrenamtliches Mandat aus. Es gelten demnach die Bestimmungen des 2. Abschnitts des BezVG. Als Organwalter haben die Bezirksverordneten daher nicht die den Parlamentariern vorbehaltene Immunität und Indemnität gem. Art. 51 VvB. Die Indemnität bezweckt, den parlamentarischen Diskurs frei von Beeinträchtigungen zu halten und so die Freiheit der Diskussionen und Abstimmungen zu gewährleisten und schließlich die Funktionsfähigkeit des Parlaments zu schützen.[16] Für die Sitzungen der BVV existiert keine entsprechende Regelung, auch § 36 StGB ist nicht anwendbar. Aus diesem Unterschied ergibt sich dennoch kein Grund für die kategorische Ablehnung der Live-Übertragung einer BVV-Sitzung, denn auch bisher gab es eine Sitzungsöffentlichkeit, und die Arbeit des Kollegialorgans ist durch das Fehlen persönlicher Strafausschließungsgründe nicht erkennbar beeinträchtigt worden.

III. Fazit

Selbst unter Berücksichtigung der unterschiedlichen Aufgabenfelder der Legislative und der Exekutive und der weiteren Unterschiede zwischen den Mitgliedern der BVV und des Abgeordnetenhauses ergibt sich daher keine zwingend unterschiedliche Beurteilung einer möglichen Sitzungsübertragung, sofern die Bezirksverordnetenversammlung sorgfältig zwischen solchen Inhalten differenziert, die im öffentlichen, und solchen, die im nicht öffentlichen Teil der Sitzung erörtert werden.

Daran schließt sich die Frage an, ob eine Live-Übertragung unter Beachtung der gegebenen Vorschriften an sich zulässig wäre und wie sie ausgestaltet sein müsste.

---

[16] *Schulze-Fielitz* in Dreier GG, Band II, Art. 46 Rn. 8; Driehaus VvB Art. 51 Rn. 2.

IV. Zulässigkeit der Live-Übertragung

Anders als das Abgeordnetenhaus unterliegt die BVV als Teil der Exekutive dem Anwendungsbereich des Berliner Datenschutzgesetzes (vgl. §§ 1, 2 BlnDSG).

Die geplante Übermittlung personenbezogener Daten ist gem. § 6 Abs.1 Satz 1 BlnDSG nur zulässig, wenn das BlnDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

Die Direktübertragung der öffentlichen BVV-Sitzung stellt eine Übermittlung im Sinne einer Bekanntgabe an Dritte dar, wobei die potentiellen Empfänger des Internetstreams eine unbestimmte Anzahl an Personen sind, die sich räumlich überall auf der Welt befinden können. Das BlnDSG ist anwendbar, da die BVV als Teil der Berliner Verwaltung eine öffentliche Stelle i. S. d. § 2 Abs. 1 BlnDSG ist. Die Beiträge der Redner stellen Einzelangaben über ihre eigene Person dar. Sofern inhaltlich andere Personen betroffen sind, handelt es sich auch diesbezüglich um personenbezogene Daten. Desweiteren stellen auch die Bilder der Webcam personenbezogene Daten dar. Neben den Verordneten selbst können auch geladene Gäste, Bezirksamtsmitglieder oder Besucher der Sitzung betroffen sein.

Ein expliziter Erlaubnistatbestand für ein solches Streaming liegt nicht vor. Die Übertragung kann nicht aus Art. 42 VvB hergeleitet werden. Diese Vorschrift ist lediglich auf die Sitzungen des Abgeordnetenhauses anwendbar. Gem. § 8 Abs. 6 Satz 1 BezVG tagt die BVV öffentlich. Eine Datenverarbeitung wird in der Vorschrift jedoch nicht explizit beschrieben, erlaubt oder vorausgesetzt. Als potentielle Erlaubnisnorm ist sie daher in jedem Fall zu unbestimmt i. S. d. § 6 Abs. 1 Satz 3 BlnDSG. Aus demselben Grund kann auch die Vorschrift des § 7 Abs. 2 Satz 1 BezVG, die das Hausrecht des Bezirksverordnetenvorstehers normiert, nicht als Erlaubnistatbestand fungieren.

Im Rahmen des BlnDSG käme möglicherweise § 6 Abs. 1 Satz 2 i. V. m. § 13 BlnDSG in Betracht. Voraussetzung wäre, dass § 6 Abs. 1 Satz 2 BlnDSG eine Erlaubnisnorm im Sinne des § 13 BlnDSG sein könnte. Vorliegend kann die Klärung dieser Frage jedoch dahinstehen, wenn die Übermittlung auch bei einer hypothetischen Anwendbarkeit des § 6 Abs. 1 Satz 2 BlnDSG nicht zulässig wäre: Die zu übermittelnden Daten sind ihrer Art nach nicht in ihrer Schutzwürdigkeit beschränkt. Bei den Redebeiträgen und dem entstehenden Bildmaterial handelt es sich unter Umständen um spontane Äußerungen zu verschiedenartigsten Themen. Es erscheint daher nicht angemessen, ein niedrigeres Schutzniveau anzusetzen und auf eine ausdrückliche bereichsspezifische Erlaubnisnorm zugunsten einer einfachen Abwägung zu verzichten. Auch die beabsichtigte Art der Verwendung der Daten kann nicht Argument für die ausnahmsweise Zulässigkeit sein, da eine Übermittlung weltweit und unter Umständen beliebig reproduzierbar stattfinden würde. Hinsichtlich der Offenkundigkeit kann nicht auf die Tatsa-

che abgestellt werden, dass die Sitzung der BVV selbst öffentlich ist, um auf diesem Wege „offenkundige Daten“ i. S. d. § 6 BlnDSG anzunehmen. Eine Übermittlung wäre demnach auch bei hypothetischer Anwendbarkeit des § 6 Abs. 1 Satz 2 BlnDSG nicht ohne Einwilligung zulässig.

Daher kommt eine zulässige Übermittlung nur dann in Betracht, wenn eine Einwilligung der Betroffenen vorläge.

V. Weiteres Vorgehen

1. Gesetzliche Regelung

Es wäre empfehlenswert, für die Zukunft eine gesetzliche Vorschrift für die Übermittlung der Sitzungen via Streamingdienste zu schaffen. Ob dies im Wege einer Ergänzung des § 32 der GO der BVV geschehen kann, indem man einen neuen Absatz einfügt, der die Übertragung des öffentlichen Teils der Sitzung der BVV ausdrücklich erlaubt, ist fraglich. Denn eine solche Erlaubnisnorm würde nicht ausreichen, um die Rechte Dritter einzuschränken: Die GO ist als Innenrecht der BVV nicht geeignet, Grundrechte zu beschränken, sofern die betreffende Norm nicht ausnahmsweise ein formell-materielles Gesetz konkretisiert.

Ohne eine solche ausreichende Rechtsgrundlage wird man auf die Einholung der Einwilligungen der Verordneten verweisen müssen. Prinzipiell muss die Einwilligung eines jeden Verordneten vorliegen, um die Übertragung zu legalisieren, sodass ein einstimmiger Beschluss hierfür notwendig wäre. Es wäre jedoch auch denkbar, einen Mehrheitsbeschluss ausreichen zu lassen, sofern der einzelne Verordnete die Möglichkeit hat, sich der Übertragung zu entziehen, indem beispielsweise die Kamera und das Mikrofon vor Beginn seines Redebeitrages abgestellt werden. Ein Verordneter sollte zudem die Möglichkeit haben, grundsätzlich für die Zukunft einen Widerspruch gegen die Übertragung zu vermerken. Auf eine solche Möglichkeit sollte im Rahmen eines neuen Absatzes in der GO verwiesen werden. Auch sollte dort festgelegt werden, dass die Übertragungen nur für den öffentlichen Teil der regulären Sitzungen vorgesehen sind, während bspw. die Bürgerfragestunde grundsätzlich nicht übertragen wird.

2. Tendenzen der neueren Rechtsprechung

Angesichts der neueren Entwicklung in der Rechtsprechung[17] sei darauf hingewiesen, dass sich diese Entscheidungen nur bedingt auf die vorliegende Situation

[17] vgl. OVG Saarlouis, Beschluss vom 30.8.2010, 3 B 203/10; Urteil des VG Saarlouis vom 25.03.2011, 3 K 501/10.

übertragen lassen: Die im Saarland zu entscheidende Streitigkeit bezog sich auf das Ersuchen eines privaten lokalen Rundfunkveranstalters an den Ratsvorsitzenden eines Stadtrates, eine Sendegenehmigung für die öffentlichen Sitzungen zu erhalten. Es handelte sich somit um eine Informationsbeschaffung gegenüber der öffentlichen Verwaltung und nicht wie vorliegend um eine Informationsverschaffung durch die Verwaltung. Das OVG kam in seiner Eilentscheidung zu dem Schluss, dass eine pauschale Ablehnung dieses Ersuchens mit dem Verweis auf die Gefährdung der Funktionsfähigkeit des Verwaltungsorgans „Stadtrat" in rechtswidriger Weise gegen Art. 5 Abs. 1 GG verstößt.

Anders als noch das BVerwG in seinem Beschluss vom 3. August 1990 (7 C 14/90) war das OVG der Ansicht, dass das Recht auf freie Berichterstattung durch ein grundsätzliches Sendeverbot gänzlich entleert würde, während dies bei einem Verbot von Tonmitschnitten für die Berichterstattung der Presse damals nicht gegolten habe. Im Rahmen der Abwägung zur Herstellung der praktischen Konkordanz zwischen dem Schutz der Funktionsfähigkeit des Organs und dem Informationsinteresse der Öffentlichkeit wies das OVG insbesondere daraufhin, dass das allgemeine Persönlichkeitsrecht der Stadträte aufgrund ihrer politischen Funktion weit in den Hintergrund trete. Auch sei der Verweis auf das Datenschutzrecht nicht zielführend oder entscheidend. Schließlich ergebe sich daher ein Anspruch des Rundfunkveranstalters auf ermessensfehlerfreie Abwägung, da zwar nicht ausgeschlossen werden könne, dass im Einzelfall die Funktionsfähigkeit des Stadtrates beeinträchtigt werden könnte, aber keinesfalls ein genereller Vorrang dieses Interesses vor dem Informationsinteresse der Öffentlichkeit gegeben sei.

Dieser neueren Entwicklung lässt sich jedenfalls entnehmen, dass ein Ersuchen eines Rundfunkveranstalters, die Sitzungen zu übertragen, nur unter größerem Begründungsaufwand im Einzelfall abgelehnt werden könnte. Des Weiteren hat die vorgenommene Abwägung des OVG gezeigt, dass die Organwalter in den Selbstverwaltungsgremien ähnlich den Abgeordneten der Parlamente in ihrer politischen öffentlichen Funktion tätig werden und ein Verweis auf die ehrenamtlich übernommene Aufgabe nicht geeignet ist, ein grundsätzlich höheres Schutzniveau für das allgemeine Persönlichkeitsrecht anzunehmen, als dies bei Berufspolitikern der Fall ist. Allerdings hat das OVG auch die Möglichkeit gesehen, dass Rundfunkveranstalter zum Schutz der Rechte einzelner Gremienmitglieder nur mit der Maßgabe zugelassen werden, dass sie die betreffenden Gremienmitglieder nicht in Bild oder Ton aufnehmen.

3. Praktische Hinweise

Sollte die Live-Übertragung im Internet auf Veranlassung der BVV zukünftig stattfinden, gilt es, folgende praktische Hinweise zu bedenken und ggf. umzusetzen:

Sachverständige und Bezirksamtsmitarbeiter, die der Sitzung beiwohnen, müssen um ihre Einwilligung gebeten werden. Der Hinweis auf die Übertragung sollte daher praktischerweise bereits in der Einladung zur Sitzung abgedruckt sein.

Entsprechend sind auch die Zuschauer der Sitzung auf die Übertragung hinzuweisen. Es sollte daher zumindest ein Aushang vor dem Sitzungssaal angebracht werden, sodass ein Zuschauer seine Einwilligung bei Betreten konkludent erklärt.

In technischer Hinsicht sollte die Kameraperspektive feststehend sein. Die Kamera sollte lediglich auf das Rednerpult gerichtet sein. Keinesfalls sollten Bilder aus dem Zuschauerraum übertragen werden, auch eine Übertragung der zuhörenden anderen Bezirksversammlungsmitglieder sollte unterbleiben. Den Verordneten sollte vor der ersten Übertragung das Bild der Übertragungen vorgeführt werden, sodass die Redner und Zuhörer einschätzen können, welcher sichtbare Bereich ins Internet gestreamt wird.

Es ist zu erwägen, ob nicht über die Einstellungen zur Bildauflösung und der Bildwechselfrequenz (fps; Anzahl der Bilder pro Sekunde) ein wirksamer technischer Datenschutz erreicht werden kann. Es erscheint nicht notwendig, einen hochauflösenden, flüssigen Film von der Sitzung zu übertragen, bei dem jede Nuance und jedes visuelle Detail erkennbar ist, wenn die Zwecke Transparenz, Bürgernähe und Herstellung der Öffentlichkeit auch durch ein verpixeltes Bild erreicht werden können.

Technisch kaum zu verhindern ist die Möglichkeit, dass die gestreamten Übertragungen gespeichert werden können. Den besten Schutz verspricht daher der Verzicht auf hochauflösende Bilder und Nahaufnahmen.

Es gilt außerdem zu bedenken, dass infolge der Nutzung eines kommerziellen Streamingdienstes die Möglichkeit besteht, dass die Daten auf Servern in Drittstaaten zwischengespeichert werden. Insbesondere, wenn der Anbieter auf p2p-Technik setzt, kommt es zu zahlreichen Zwischenspeicherungen des Streams auf den Rechnern der Nutzer, auch wenn diese nicht unmittelbar abspielbar sind. Auch darauf sollten die Verordneten vorab hingewiesen werden.

Eine Beschränkung der Erreichbarkeit des Streams mittels IP-Adressen-Filterung wäre zwar grundsätzlich möglich, aber dies wäre technisch dann nicht zu realisieren, wenn man die Infrastruktur eines kommerziellen Streaminganbieters nutzt. Es soll an dieser Stelle auch darauf hingewiesen werden, dass kommerzielle Anbieter sich die Nutzung des hochgeladenen Streams gerne selbst vorbehalten, wie sich aus dieser typischen Klausel des Anbieters ustream.tv ergibt, den die BVV Marzahn-Hellersdorf derzeit nutzt:

> […] by uploading, streaming, submitting, emailing, posting, publishing or otherwise transmitting any User Submission to Ustream on the Site or to the Services, you hereby grant Ustream a non-exclusive, worldwide, royalty-free, sublicensable, perpetual and irrevocable right and license to use, reproduce, modify, adapt, prepare derivative works based on, perform, display, publish, distribute, transmit, broadcast and otherwise exploit such User Submissions in any form, medium, device or technology now known or later developed, including without limitation on third party websites and platforms where the Services are syndicated. For example, Ustream will have the right to insert, place or include all types of advertisements within or around your User Submissions, including without limitation to running or streaming pre-rolls, mid-rolls, post-rolls, overlays, banners, campaign and companion ads and any other type of advertising units in connection with your User Submission.

Ähnliche Klauseln finden sich in den AGB aller größeren Streaminganbieter.

Der Vorsitzende hat bei laufender Übertragung besonders darauf zu achten, dass Zwischenrufe aus dem Zuschauerraum unterbleiben, die das Persönlichkeitsrecht eines Dritten oder eines Verordneten betreffen. Denn anders als bei der Ausübung der Tätigkeit im Rahmen des übernommenen Amtes ist der einzelne Verordnete in seinem allgemeinen Persönlichkeitsrecht dann geschützt, wenn er bspw. in seiner Person beleidigt wird.