Dokumente
zu Datenschutz
und Informationsfreiheit
2014

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
Friedrichstr. 219, 10969 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 2015

Inhaltsverzeichnis

Vorwort

Die „Dokumente zu Datenschutz und Informationsfreiheit“ wurden erstmals 1999 gemeinsam vom Berliner Datenschutzbeauftragten und vom Brandenburgischen Landesbeauftragten für Datenschutz und für das Recht auf Akteneinsicht herausgegeben. Diese jährliche Sammlung von Entschließungen der nationalen, europäischen und internationalen Datenschutzgremien wie auch der entsprechenden Konferenzen der Informationsbeauftragten hat sich seitdem als gedruckte Dokumentation bewährt, selbst wenn heute die meisten Dokumente auch online abrufbar sind. Suchmaschinen können zwar Trefferlisten generieren, aber keinen vergleichbar systematischen Überblick über die Zusammenarbeit der Beauftragten für Datenschutz und Informationsfreiheit geben.

Im Vorwort zum ersten Dokumentenband für das Jahr 1998 schrieben die Herausgeber, dass angesichts der – mittlerweile reduzierten – Zersplitterung der Kompetenzen unter den deutschen Datenschutzbehörden „ein effektiver Datenschutz nur dann gesichert“ sei, „wenn die beteiligten Gremien ihre Arbeit koordinieren; dies ist auch deswegen erforderlich, weil die geringe Ausstattung der Datenschutzbehörden eine Spezialisierung und eine dadurch mögliche Aufgabenverteilung ermöglichen.“ Diese Aussage ist nach wie vor ebenso zutreffend wie der 1999 gegebene Hinweis der Herausgeber, dass die Koordination der europäischen Datenschutzbehörden untereinander immer größere Bedeutung gewinnt. Die Datenschutzbehörden in Deutschland stehen vor dem Hintergrund der künftigen Europäischen Datenschutz-Grundverordnung vor der Aufgabe, ihre Positionen im föderalen System der Bundesrepublik abzustimmen und in die Meinungsbildung des künftigen Europäischen Datenschutzausschusses (der an die Stelle der Art. 29-Datenschutzgruppe treten wird) einzubringen. Zentralistische Strukturen sind weder auf nationaler noch auf europäischer Ebene eine rechtlich zulässige oder auch nur wünschenswerte Alternative. Denn die betroffenen Bürgerinnen und Bürger müssen sich an eine Datenschutzbehörde in ihrem Bundesland wenden können. Der europäische Gesetzgeber sollte das Datenschutzrecht auf einem hohen Niveau vereinheitlichen, seine Durchsetzung aber den unabhängigen Datenschutzbeauftragten vor Ort überlassen.

Datenschutz und Informationsfreiheit leben auch von den gemeinsamen Entschließungen und Stellungnahmen, die die zum Schutz dieser Grundrechte berufenen Beauftragten öffentlich formulieren. Dazu gehören darüber hinaus rechtspolitische Forderungen, denn der rasante technische Fortschritt erlaubt es nicht, sich mit der Durchsetzung geltenden Rechts zu begnügen.

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 87. Konferenz am 27./28. März 2014 in Hamburg

Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage zur Entschließung
Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten.

Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographische Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur

Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.

Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung

Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.

Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten

Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen

stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten

Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation

Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen

Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird. Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und

Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können.

Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

- alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,
- für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,
- eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
- die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken.

Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen. Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.

Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.

Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik

Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.

- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die

Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.

- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise

in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

– Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

– In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

– In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

– Es ist sicherzustellen, dass

  • die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

  • die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,

  • die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

2. Entschließung zwischen der 87. und 88. Konferenz (vom 25. April 2014)

Ende der Vorratsspeicherung in Europa!

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z. B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

3. Entschließungen der 88. Konferenz am 8./9. Oktober 2014 in Hamburg

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechen-

den Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen." In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen(siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigen-

ständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes – und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.

- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Lander weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeu-

gen schafft Begehrlichkeiten, die dort anfallenden Daten fur die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote fur Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

4. Entschließungen nach der 88. Konferenz

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern (vom 14. November 2014)

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage zur Entschließung
Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291 a, 291 b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65 c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalog in Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden.

Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die

Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich.

Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N – 4N)

2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemioloigschen Krebsregistrierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. *Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten*.

Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedes für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 04./05. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

Ferner sind hohe (Szenarien 1 – 2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken

weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI-TR 03116-1 entnommen sein. (Szenarien 1 – 4)

5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch + gemäß Abschnitten 3 und 4 der BSI-TR 03107-1 zu erfüllen. (Szenarien 1 – 4)

6. *(optional)* Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1 – 4)

7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1 – 4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsslung einzusetzen. (Szenarien 1 – 4)

9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)

10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2 – 4)

11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1 – 4)

12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein. (Szenarien 1W – 4W)

13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2 + 4)

14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291 a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet. (Szenarien 2W + 4W)

15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291 a Abs. 5 c SGB V bestimmt wurden. (Szenarien 2 – 4)

16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)

17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)

18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19. Ambulante Leistungserbringer müssen die „Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1 – 4)

20. Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen,

die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1 – 4)

21. Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1 – 4)

22. Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein. (Szenarien 1 – 4)

23. Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss *(defense in depth)*. (Szenarien 1W – 4W)

24. Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W – 4W)

25. Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W – 4W)

26. Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmög-

lichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

27. Da die übermittelten Daten einer folgenden Behandlung zugrundegelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1 + 4)

28. Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1 + 4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

29. Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2 – 4)

30. Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2 – 4)

31. Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

Keine PKW-Maut auf Kosten des Datenschutzes! (vom 14. November 2014)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für

Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern! (vom 16. Dezember 2014)

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKVVersorgungsstärkungsgesetz – GKV–VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

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

1. Beschluss vom 27. Januar 2014

Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

Anlage:
Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“

Einleitung

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. An der Beantwortung der Fragen muss der Vermieter ein berechtigtes Interesse haben oder es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss das Recht des Mietinteressenten auf informationelle Selbstbestimmung Beachtung finden.

Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft ist nicht als das richtige Mittel zur Datenerhebung anzusehen. Eine wirksame Einwilligung erfordert nach § 4 a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Dem Mietinteressenten wird dabei suggeriert, er habe bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht. Wird der Abschluss des Mietvertrags von der Erhebung bestimmter

Angaben beim Mietinteressenten abhängig gemacht, fehlt diese Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommt.

Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden: (a) dem Besichtigungstermin, (b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und (c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Die Zulässigkeit der Erhebung einer Selbstauskunft richtet sich im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht dann ein vorvertragliches Schuldverhältnis zum künftigen Vermieter, so dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Steht dem Vermieter für die Datenerhebung eine gesetzliche Grundlage nach § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG zur Verfügung, so kommt es auf die Anforderungen nach § 4 a Abs. 1 Satz 1 BDSG nicht an bzw. ein Rückgriff auf das Konstrukt der Einwilligung wäre auch falsch, denn für den Mietinteressenten würde wiederum der Eindruck entstehen, dass die Offenbarung der Informationen seinem Wahlrecht unterliegt. Bei der Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG kommt es dann im Rahmen der Erforderlichkeitsprüfung darauf an, ob von Seiten des Interessenten aus Offenbarungspflichten bestehen bzw. ob von Vermieterseite aus zulässige Fragen gestellt werden. Unzulässige Fragen müssen demnach nicht beantwortet werden (Blank, in: Schmidt-Futterer, Kommentar zum Mietrecht, 11. Auflage 2013, § 543, Rn. 204). Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen des Mietinteressenten am Ausschluss der Datenerhebung bestehen.

Die folgende Darstellung ist nicht im Sinne einer abschließenden Aufzählung zu verstehen:

a) Besichtigungstermin

Strebt der Mietinteressent nur eine Besichtigung der Räumlichkeiten an, so wäre es etwa nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen. Erfragt werden dürfen:

aa) Angaben zur Identifikation

Hierzu zählen Name, Vorname und Anschrift. Der Vermieter wäre auch befugt, im Falle der Besichtigung allein durch den Mietinteressenten die Angaben durch

Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.

bb) Angaben aus Wohnberechtigungsschein

Der künftige Vermieter darf nach § 27 Abs. 1 Wohnraumförderungsgesetz (WoFG) eine Wohnung, die im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde, nur einem Wohnungssuchenden zum Gebrauch überlassen, wenn dieser ihm vorher seine Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweist. Möchte der Mietinteressent eine solche Wohnung besichtigen, sind Angaben zum Vorliegen eines Wohnberechtigungsscheins sowie zur genehmigten Wohnfläche und Anzahl der Wohnräume erforderlich, da nur in diesem Fall ein Besichtigungstermin sinnvoll ist. Eine Kopie des Wohnberechtigungsscheins darf erst nach der Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen, erfolgen, da die in dem Formular aufgeführten Angaben zu den Namen und Vornamen der im Haushalt des Mietinteressenten befindlichen Personen im Besichtigungstermin nicht erforderlich sind.

cc) Angaben zu Haustieren

Fragen des Vermieters nach dem beabsichtigten Einbringen von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Entsprechende Fragen sind zulässig, soweit dies nicht Kleintiere betrifft (z.B. Zierfische, Mäuse, Hamster).

b) Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen

aa) Familienstand und Angaben zu den im Haushalt lebenden Personen

Angaben zum Familienstand des Mietinteressenten werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein aus dieser Zwecksetzung heraus ist kein berechtigtes Vermieterinteresse gegeben, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen. Soweit nur ein Ehegatte den Wohn-Mietvertrag unterzeichnen möchte und im Hinblick auf die äußere Gestaltung des Mietvertrags und die mündlichen Absprachen nicht davon ausgegangen werden kann, dass auch der andere Ehegatte Mietvertragspartei wird, greift keine gesamtschuldnerische Haftung ein. Schließlich ginge auch das Argument ins Leere, von Vermieterseite aus einer möglichen Gebrauchsüberlassung an Dritte zuvor zu kommen, denn nach § 553 Abs. 1 BGB hätte der Mieter im Regelfall ein berechtigtes Interesse daran, dem Ehegatten den Wohnraum zur Nutzung zu überlassen.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben dürfen zu diesen Personen nicht eingeholt werden, es sei denn, diese möchten Mietvertragspartner sein.

bb) Eröffnetes Insolvenzverfahren, Angabe einer Vermögensauskunft, Räumungstitel wegen Mietzinsrückständen

Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05).

Bei der Angabe einer Vermögensauskunft (§ 802c Abs. 3 ZPO) sind Mietzinsansprüche des Vermieters nicht in gleicher Weise gefährdet (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05). Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften besteht, hängt u. a. davon ab, nach welchem Zeitraum gefragt wird. Ferner ist zu berücksichtigen, dass gemäß § 882 f Satz 1 Nr. 4 ZPO eine Einsicht in das Schuldnerverzeichnis unter bestimmten Voraussetzungen möglich ist und zum Inhalt eines solchen Verzeichnisses auch Eintragungsanordnungen nach § 882 c ZPO zählen. Nach § 882 f Satz 1 Nr. 4 ZPO ist die Einsicht in das Schuldnerverzeichnis jedem gestattet, der darlegt, Angaben nach § 882 b ZPO zu benötigen, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Im Hinblick auf den erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung des Mietinteressenten ist bei der Anwendung von § 882 f Satz 1 Nr. 4 ZPO vor allem der Verhältnismäßigkeitsgrundsatz zu beachten. Ferner muss den wirtschaftlichen Nachteilen bedeutsames Gewicht zukommen (Utermark, in: Vorwerk/Wolf, Beck'scher Online-Kommentar ZPO, 2013, § 882 f, Rn 7). An die Zulässigkeit einer Datenerhebung beim Vollstreckungsgericht nach § 882 f Satz 1 Nr. 4 ZPO sind ähnlich hohe Anforderungen zu stellen, wie im Rahmen einer Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG beim Mietinteressenten.

Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnis mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht (AG Wolfsburg, Urteil v. 09.08.2000, Az.: 22 C 498/99). Fragen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchge-

führt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, werden als zulässig angesehen (LG Wuppertal, Urteil v. 17.11.1998, Az.: 16 S 149/98).

cc) Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit

Nach § 19 Abs. 1 und 3 AGG ist bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum eine unterschiedliche Behandlung im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zulässig. Es fehlt regelmäßig an der Erforderlichkeit der Datenerhebung, da die Anforderungen nach den §§ 19, 20 AGG kaum erfüllt sein werden. Hierfür müsste zur Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zunächst ein tragfähiges Vermietungskonzept vorliegen. Das Konzept muss auch zur Prüfung sachlicher Gründe (vgl. etwa § 20 Abs. 1 Nr. 4 AGG) Auskunft geben, die eine Ungleichbehandlung rechtfertigen und folglich zur Entschärfung von Konflikten beitragen können. Eine pauschale Abfrage der Angaben ist daher unzulässig.

dd) Vorstrafen und strafrechtliche Ermittlungsverfahren

Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Berücksichtigt werden muss zum einen, dass bestimmte Strafen nicht in ein polizeiliches Führungszeugnis aufzunehmen sind, § 32 Abs. 2 BZRG, und sich schon deshalb keine darüber hinaus gehenden Mitteilungspflichten gegenüber einem Vermieter ergeben können. Weiterhin hat die Rechtsprechung eine Offenbarung von Vorstrafen bisher nur im Zusammenhang mit der Begründung von Arbeitsverhältnissen als zulässig angesehen, wenn ein klarer Bezug zu einer entsprechenden Tätigkeit besteht, wie etwa das Fragen nach Vermögensdelikten bei einer Beschäftigung im Kassenbereich eines Kreditinstituts. Dabei steht die Frage nach der Geeignetheit eines Bewerbers im Mittelpunkt. Bei der Anbahnung von Mietverhältnissen besteht grundsätzlich keine vergleichbare Gefährdungslage, da hier die Frage nach der Bonität des Mietinteressenten von zentraler Bedeutung ist. Gegen die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren spricht schon die verfassungsrechtlich und auch in Art. 6 Abs. 2 EMRK verankerte Unschuldsvermutung.

ee) Heiratsabsichten, Schwangerschaften, Kinderwünsche

Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und Kinderwünschen zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig. Eine Aufnahme von Kindern und Ehegatten in der Wohnung wäre für

den Mietinteressenten schon nicht erlaubnispflichtig im Sinne von § 553 Abs. 1 Satz 1 BGB, denn diese Personen sind in Anwendung von Art. 6 Abs. 1 GG bereits keine Dritten (§ 553 Abs. 1 BGB), sondern nahe Familienangehörige. Der Mieter muss die Aufnahme von Familienangehörigen nur anzeigen. Einer Aufnahmeerlaubnis durch den Vermieter bedarf es nicht.

ff) Mitgliedschaften in Parteien und Mietvereinen

Es besteht keine Verpflichtung, über die Zugehörigkeit zu Parteien oder Mietervereinen Auskunft zu geben. Mit den Angaben wird zudem noch keine Aussage zur Bonität des Mietinteressenten bzw. zu dessen Zahlungsfähigkeit und Zahlungswilligkeit getroffen.

gg) Angaben zum Arbeitgeber, zum Beschäftigungsverhältnis und zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

hh) Einkommensverhältnisse

Die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens wäre jedoch auch die Angabe einer bestimmten Betragsgrenze durch den Mietinteressenten ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird. Im Hinblick auf die monatlichen Belastungen ist die Erfragung der Forderungsgründe (Unterhaltsverpflichtungen, Darlehensverbindlichkeiten etc.) unzulässig, da dies für die Beurteilung der Bonität nicht erforderlich ist.

Fragen nach den Einkommensverhältnissen sind unzulässig, wenn die Mietzahlungen vollständig von dritter Stelle für den Mieter übernommen und direkt an den Vermieter geleistet werden sollen, was bei Empfängern von Arbeitslosengeld II der Fall sein kann. Empfänger von Arbeitslosengeld II müssen für die Durchführung einer solchen Direktzahlung gegenüber dem Jobcenter eine entsprechende Erklärung abgeben, § 22 Abs. 7 Satz 1 SGB II. Direktzahlungen an den Vermieter werden nach § 22 Abs. 7 Satz 2 SGB II von Amts wegen vorgenommen, wenn eine zweckentsprechende Verwendung der gewährten Mittel durch den Empfänger von Arbeitslosengeld II nicht sichergestellt ist.

ii) Angaben zu bisherigen Vermietern

Fragen nach den Kontaktinformationen aktueller oder früherer Vermieter des Mietinteressenten (z.B. Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig. Solche Angaben wären für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich und würden eine dem Grundsatz der Direkterhebung (§ 4 Abs. 2 Satz 1 BDSG) widersprechende Datenerhebung bei Dritten über den Mietinteressenten ermöglichen.

c) Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten

Der künftige Vermieter möchte nun mit dem einzigen Mietinteressenten für eine konkrete Wohnung einen Mietvertrag schließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.

aa) Nachweise zu den Einkommensverhältnissen

Der künftige Vermieter kann bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen darauf hinweisen, dass für den Fall einer positiven Entscheidung für den Mietinteressenten quasi unmittelbar vor Unterzeichnung des Vertrags noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z. B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben. Als Nachweis ist auch eine Bescheinigung des Arbeitgebers ausreichend, dass die Angaben des Mietinteressenten bezüglich der Angabe einer bestimmten Nettobetragsgrenze, die überschritten wird, zutreffend sind.

bb) Vorlage der Selbstauskunft nach Anfrage bei einer Auskunftei

Der künftige Vermieter benötigt Informationen zu den wirtschaftlichen Verhältnissen des Mietinteressenten, um dessen Zahlungsfähigkeit bezüglich des Mietzinses beurteilen zu können. Selbstauskünfte, die Mietinteressenten bei Auskunfteien (z. B. SCHUFA) selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse, als für eine solche Beurteilung erforderlich sind. Schon aus diesem Grund wäre die Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig.

Da die Verwendung von Einwilligungserklärungen gegenüber dem Mietinteressenten in Formularen zur Selbstauskunft nicht als das richtige Mittel zur Daten-

erhebung anzusehen ist, wäre auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, nicht rechtmäßig. Zur Einholung von Bonitätsauskünften über den Mietinteressenten wäre der Vermieter nur dann befugt, wenn die Voraussetzungen einer gesetzlichen Vorschrift (§ 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG) erfüllt sind.[1]

2. Beschlüsse vom 25./26. Februar 2014

Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nichtöffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6 b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen

[1] Vgl. zur Einholung von Bonitätsauskünften über Mietinteressenten gegenüber Auskunfteien den Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 22. Oktober 2009 „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig".

als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in **eigener** Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

III. Gemeinsame Positionen

Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten (vom 20. Mai 2014)

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von **Fernsehangeboten** muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als **Telemedien** den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter

von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

- Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

- Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.

- Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.

- Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

IV. Europäische Konferenz der Datenschutzbeauftragten

Straßburg, 5. Juni 2014

Entschließung zur Überarbeitung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108)

Bei vergangenen Frühjahrskonferenzen haben die europäischen Datenschutzbehörden wiederholt ihre Absicht zum Ausdruck gebracht, aktiv an der Entwicklung des Datenschutzes innerhalb und außerhalb Europas mitzuwirken und hohe Standards in diesem Bereich zu fordern[1].

Im Bewusstsein der großen Herausforderungen und Risiken, die sich durch die technischen Entwicklungen und durch die zunehmende Tendenz von Regierungen ergeben, eine Massenüberwachung von Personen durchzuführen, unterstreicht die Konferenz die Notwendigkeit, die verschiedenen Rechtsrahmen zum Datenschutz auf der Grundlage bestehender Prinzipien zu modernisieren und zu stärken.

Die Globalisierung der Datenverarbeitung und des Datenaustauschs erfordert einen umfassenden Ansatz unter Berücksichtigung des europäischen und des internationalen Rechtsrahmens[2].

Vor diesem Hintergrund unterstützt die Konferenz die Bemühungen des Europarats, das Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) sowie sein Zusatzprotokoll zu modernisieren, die beide allgemeine Grundsätze bekräftigen.

Die Konferenz lobt den Europarat dafür, Länder, die nicht Vertragsstaaten des Übereinkommens 108 und seines Zusatzprotokolls sind, zum Beitritt zu ermutigen, aber unterstreicht, dass die Bereitschaft zur Öffnung nicht zu einer Senkung des durch diese Instrumente geschaffenen hohen Datenschutzstandards führen darf.

In diesem Zusammenhang stellt die Konferenz fest, dass jede Absenkung des derzeit durch das Übereinkommen 108 und seines Protokolls gewährten Schutzes einen Rückschritt darstellen würde.

---

[1] Erklärung zur führenden Rolle und Zukunft des Datenschutzes in Europa, verabschiedet am 23.–24. April 2009 in Edinburgh, Entschließung zur künftigen Entwicklung von Datenschutz und Privatsphäre, verabschiedet am 30. April 2010 in Prag.

[2] Entschließung über die Notwendigkeit eines umfassenden Rechtsrahmens für den Datenschutz, verabschiedet am 5. April 2011 in Brüssel.

Vor diesem Hintergrund fordert die Konferenz alle Mitgliedstaaten des Europarats und Vertragsstaaten des Übereinkommens 108 dazu auf, den derzeitigen durch das Übereinkommen gewährleisteten Schutz zu wahren und, wenn möglich, zu stärken und insbesondere die vom beratenden Ausschuss (T-PD) vorgeschlagenen Masnahmen umzusetzen:

- **Beibehaltung eines breiten Anwendungsbereichs**, der jede Verarbeitung personenbezogener Daten im öffentlichen und privaten Sektor in der Zuständigkeit der Vertragsstaaten umfasst, damit jede Person unabhängig von ihrer Nationalitat oder ihres Wohnorts das Recht auf den Schutz personenbezogener Daten hat;

- **Begrenzung der Ausnahmeregelungen** zu den Datenschutzgrundsätzen, wobei jede Ausnahme **gesetzlich festgelegt, verhaltnismäßig und in einer demokratischen Gesellschaft erforderlich sein muss**;

- **Eingruppierung genetischer und biometrischer Daten in die Kategorie „sensible Daten“**;

- **Einführung des Grundsatzes der Datenminimierung** im Zusammenhang mit der Einhaltung des Verhältnismäßigkeitsprinzips;

- **Gewährleistung, dass eine erforderliche Zustimmung zur Verarbeitung spezifisch, freiwillig und informiert ist und eine ausdrückliche Willensäußerung darstellt**;

- **Unterstreichung der Bedeutung der Transparenz**, die den für die Verarbeitung Verantwortlichen dazu verpflichtet, die Personen, deren Daten verarbeitet werden, zumindest über seine Identität und die Zwecke der Verarbeitung, aber auch uber die Datenempfänger und die Möglichkeiten zur Wahrnehmung ihrer Rechte zu unterrichten;

- **Verbesserung der Rechte von Personen**, insbesondere das Recht auf Zugang und Berichtigung sowie das Widerspruchsrecht;

- **Aufnahme** von Bestimmungen zur Regelung von **Entscheidungen, die rein auf der automatischen Datenverarbeitung beruhen**;

- **Aufnahme von Rechenschaftspflichten**, nach denen die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter bei allen Verarbeitungsschritten geeignete Maßnahmen ergreifen müssen, um die Einhaltung des Übereinkommens zu gewährleisten und nachzuweisen, und ab der Planungsphase der Verarbeitung den Datenschutz berücksichtigen müssen;

- **Einführung einer Pflicht zur Meldung von Sicherheitsverstößen**;

- **Beibehaltung des hohen Schutzstandards für personenbezogene Daten und Aufsicht über internationalen Datentransfer** im Interesse der Kohärenz und Einhaltung des Rechtsrahmens der Europäischen Union;

- **Gewährleistung einer Evaluierung vor und nach der Ratifikation oder dem Beitritt zum Übereinkommen** zur Prüfung der Existenz, Einhaltung und Effektivitat von Maßnahmen zur Umsetzung der Bestimmungen des Übereinkommens.

Des Weiteren sollten Vertragsstaaten die **Vertretung der Datenschutzbehörden im Beratenden Ausschuss** von Übereinkommen 108 sicherstellen.

Schließlich stellt die Konferenz fest, dass ein **effektiver Datenschutz die Schaffung unabhängiger Aufsichtsbehörden erfordert**. In diesem Zusammenhang ist die Konferenz der Ansicht, dass Datenschutzbehörden zumindest folgende Befugnisse haben müssen:

- Ermittlungs- und Eingriffsbefugnisse sowie das Recht, Entscheidungen zu treffen und Sanktionen zu verhängen;

- Möglichkeit, Stellungnahmen zu allen Angelegenheiten des Datenschutzes abzugeben und insbesondere über alle rechtlichen oder administrativen Vorschläge zum Datenschutz konsultiert zu werden;

- Möglichkeit zur effektiven Zusammenarbeit durch den Austausch aller nützlichen Informationen und die Koordinierung ihrer Aktivitäten in einem Netzwerk.

Mit dieser Entschließung begrüßt die Konferenz die Vorschläge des Beratenden Ausschusses und fordert den Europarat auf, diese in seine Arbeit einzubeziehen. Die Konferenz unterstreicht, dass die Überarbeitung des Rechtsrahmens für den Datenschutz eine Möglichkeit darstellt, echte Verbesserungen beim Datenschutz vorzunehmen und einen effektiveren Schutz für jeden zu gewährleisten.In diesem Zusammenhang unterstreicht sie die Absicht der Datenschutzbehörden, untereinander und mit dem Europarat zu diesen Zielen eng zusammenzuarbeiten.

V. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Stellungnahme 01/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung (WP 211)

Angenommen am 27. Februar 2014

TEIL I

0.0 Zusammenfassung

Da sich nicht viele geplante oder bestehende Grenzkontroll- oder Strafverfolgungsmaßnahmen[1] denken lassen, die einen Eingriff in die Privatsphäre einer Person darstellen, ohne dass dabei auch deren personenbezogene Daten verarbeitet werden, hat die Artikel-29-Datenschutzgruppe („Datenschutzgruppe") diese Stellungnahme erarbeitet, um noch einmal die Bedeutung der Begriffe der Notwendigkeit und Verhältnismäßigkeit herauszustellen. Obgleich diese Begriffe aus dem breiter gefassten Kontext der Privatsphäre heraus entstanden sind, ist es wichtig, ihr Verhältnis zum Datenschutz zu begreifen.

Auch wenn die Richtlinie 95/46/EG als Instrument aus der Zeit vor dem Vertrag von Lissabon für einen Großteil des RFSR-Bereichs nicht anwendbar ist, möchte die Datenschutzgruppe daran erinnern, dass die Grundsätze der Richtlinie im Bereich Datenschutz allgemein anwendbar sind. Außerdem erscheinen die Grundsätze in anderen Instrumenten wie dem Übereinkommen 108, die für den RFSR-Bereich gültig sind.

Ausgehend von der Rechtsprechung und den Erfahrungen der Mitglieder der Datenschutzgruppe enthält die Stellungnahme praktische Hinweise für Gesetzgeber und RFSR-Behörden, wenn diese an die Planung neuer oder die Überprüfung vorhandener Maßnahmen denken. Folgendes sollte Berücksichtigung finden:

[1] In diesem Kontext definiert die Datenschutzgruppe „Maßnahmen" als alle vorgeschlagenen oder bestehenden Maßnahmen, die auf die Lösung eines Problems im Bereich der Strafverfolgung abzielen. Dabei könnte es sich beispielsweise um eine europäische oder einzelstaatliche Rechtsvorschrift handeln, mit der eine bestimmte Frage oder verschiedene Fragen angesprochen werden soll(en), die von einer RFSR-Agentur zu behandeln ist (sind), bis hin zur Überwachung eines Verdächtigen durch eine Strafverfolgungsbehörde.

- die Rechtsgrundlage einer Maßnahme, insbesondere nach Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention;
- das konkrete Problem, das angegangen werden soll, wie z. B. der Schweregrad des Problems sowie gesellschaftliche und kulturelle Einstellungen;
- die Gründe der Maßnahme, die eng mit den Entscheidungen über die Datenspeicherdauer, Datenminimierung und Datenqualität verbunden sind;
- Bereitstellung ausreichender Belege für die Gründe, aus denen die Maßnahme gewählt wurde.

1.0 Einleitung (Ziel und Struktur)

1.1 In der vorliegenden Stellungnahme sollen die Begriffe der Notwendigkeit und der Verhältnismäßigkeit und ihre Anwendung auf vorgeschlagene oder bestehende Maßnahmen[2] zur Lösung von Problemen im Bereich der Strafverfolgung auf mehreren Ebenen – d. h. auf lokaler/regionaler, nationaler oder europäischer Ebene – klargestellt werden. Diese Stellungnahme richtet sich in erster Linie an die einzelstaatlichen und EU-Gesetzgeber sowie an die Behörden, die für die Lösung von Fragen im Raum der Freiheit, der Sicherheit und des Rechts („RFSR“[3]) zuständig sind. Genauer gesagt handelt es sich um Behörden innerhalb des Geltungsbereichs der vorgeschlagenen Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und um jene Behörden, die in Titel V des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) genannt sind.

1.2 Auf europäischer Ebene haben sich die Begriffe der Notwendigkeit/Erforderlichkeit und der Verhältnismäßigkeit aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) im Zusammenhang mit Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) entwickelt, in dem das Recht auf Achtung des Privat- und Familienlebens verankert ist. Obwohl der Datenschutz an und für sich ein eigenständiges Konzept und nunmehr ein gesondertes und autonomes Grundrecht gemäß Artikel 8 der Charta der Grundrechte der Euro-

[2] In diesem Kontext definiert die Datenschutzgruppe „Maßnahmen“ als alle vorgeschlagenen oder bestehenden Maßnahmen, die auf die Lösung eines Problems im Bereich der Strafverfolgung abzielen. Dabei könnte es sich beispielsweise um eine europäische oder einzelstaatliche Rechtsvorschrift handeln, mit der eine bestimmte Frage oder verschiedene Fragen angesprochen werden soll(en), die von einer RFSR-Agentur zu behandeln ist (sind), bis hin zur Überwachung eines Verdächtigen durch eine Strafverfolgungsbehörde.

[3] Eine Liste von Behörden, die sich mit Fragen im Raum der Freiheit, der Sicherheit und des Rechts befassen, findet sich hier: http://europa.eu/legislation_summaries/justice_freedom_security/index_de.htm

päischen Union („Charta“) darstellt, die gemäß Artikel 7 AEUV den Verträgen rechtlich gleichrangig ist, möchte die Datenschutzgruppe auf den Ansatz des EGMR nach Artikel 8 der Konvention aufmerksam machen, da dessen enge Beziehung und Wechselwirkung zum Datenschutz von Bedeutung ist, vor allem im Kontext des RFSR.

Ausgehend von dieser Überlegung betrachtet die Datenschutzgruppe zunächst, wie der EGMR die Begriffe der Notwendigkeit/Erforderlichkeit und der Verhältnismäßigkeit bei der Behandlung von Artikel 8 EMRK definiert hat, bevor sie sich dem Ansatz des Europäischen Gerichtshofs (EuGH) bei der Auslegung der Artikel 7 und 8 der Charta zuwendet. Als eine Art praktische Anleitung betrachten wir schließlich die Elemente, die bei Maßnahmen im Raum der Freiheit, der Sicherheit und des Rechts zu berücksichtigen sind, und legen einige Lehren dar, die aus dem Ansatz des EGMR sowie aus den bereits vorhandenen diesbezüglichen Erfahrungen der Datenschutzgruppe (und ihrer Mitglieder) gezogen wurden.

Nach Auffassung der Datenschutzgruppe wird diese Stellungnahme dem Gesetzgeber und den RFSR-Behörden besser verstehen helfen, welchen Elementen Rechnung zu tragen ist, damit künftig geplante RFSR-Maßnahmen nicht nur einfach einen „Mehrwert“ haben oder „nützlich“ sind, sondern stattdessen auch notwendig und verhältnismäßig sind. Selbstverständlich wird es ihnen auch dabei helfen, die Grundsätze des Datenschutzes einzuhalten.

Hilfreich ist diese Stellungnahme wahrscheinlich auch für einige nationale Datenschutzbehörden, wenn sie diese Begriffe in einem RFSR-Kontext überprüfen sollen.

1.3 Die Datenschutzgruppe beabsichtigt, dieses Dokument auf der Basis weiterer Rechtsprechung und entsprechender Erfahrungen der nationalen Datenschutzbehörden in diesem Bereich zu überprüfen und erforderlichenfalls zu aktualisieren.

TEIL II

2.0 EU und europäischer Rechtsrahmen

2.1 Wie eine Untersuchung der bisherigen, derzeitigen und künftigen Datenschutzvorschriften zeigt, ist der Schutz personenbezogener Daten aus dem Recht auf Privatleben gemäß Artikel 8 der EMRK von 1950 heraus entstanden. Im Zuge neuer Technologien und immer größerer Überwachungsmög-

lichkeiten sowohl im öffentlichen als auch im privaten Sektor stellte sich heraus, dass Personen zusätzlich zu den gemäß Artikel 8 EMRK anerkannten „Defensivrechten" eines weiteren Schutzes vor Dritten (insbesondere vor dem Staat) bedürfen, indem ihnen das Recht auf Kontrolle der eigenen personenbezogenen Daten zugesichert wird.

Erstmals als gesondertes Recht anerkannt wurde der Schutz personenbezogener Daten im Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), das auch in der Richtlinie 95/46/EG als wichtiger Impulsgeber diente.

Die Erwähnung des Rechts auf „Achtung des Persönlichkeitsbereichs" in Artikel 1 des Übereinkommens 108 sowie des Rechts auf Privatsphäre in der Präambel und in Artikel 1 der Richtlinie 95/46/EG lassen erkennen, dass das Recht auf Datenschutz und das Recht auf Privatsphäre miteinander verknüpft sind.

Das Recht auf Schutz personenbezogener Daten wurde in der späteren Charta der Grundrechte der Europäischen Union („Charta") als gesondertes Recht weiterentwickelt, in der sowohl das Recht auf Achtung des Privat- und Familienlebens in Artikel 7 als auch ein ausdrückliches Recht auf den Schutz personenbezogener Daten in Artikel 8 verankert sind.

In Artikel 52 der Charta ist die Tragweite dieser Rechte aufgeführt. Gemäß Artikel 52 Absatz 1 müssen Einschränkungen der Ausübung beider Rechte gesetzlich vorgesehen sein. Sie müssen den Grundsatz der Verhältnismäßigkeit wahren und dürfen nur vorgenommen werden, wenn sie notwendig sind und den von der Europäischen Union anerkannten Zielsetzungen tatsächlich entsprechen oder wenn damit Rechte und Freiheiten geschützt werden sollen.

Laut Artikel 52 Absatz 3 der Charta haben Rechte, die sowohl in der Charta als auch in der EMRK enthalten sind, wie z. B. das Recht auf Privat- und Familienleben, die gleiche Bedeutung und Tragweite wie in der EMRK.

Wie sehr die Rechte zusammenhängen, lässt sich auch an der jüngeren Rechtsprechung des EuGH ablesen. Bei der Prüfung auf Notwendigkeit und Verhältnismäßigkeit in Rechtssachen, die die Privatsphäre/den Datenschutz betreffen, bevorzugt er eine Gesamtbetrachtung der Artikel 7 und 8 der Charta.[4]

[4] EuGH, C-291/12, Schwarz / Stadt Bochum, Urteil des Gerichtshofs vom 17. Oktober 2013.

2.2 Daran zeigt sich, dass sowohl nach der EMRK als auch nach der Charta eine eindeutige Verbindung zwischen dem Recht auf Datenschutz und dem Recht auf Privat- und Familienleben besteht. Da die RFSR-Behörden staatliche Behörden sind, unterliegen sie der EMRK, und nach den Bestimmungen von Artikel 52 Absatz 3 der Charta muss der Begriff der Privatsphäre in einem RFSR-Kontext die gleiche Bedeutung und Tragweite haben wie nach der EMRK.

Das heißt, dass Bedeutung, Tragweite und Anwendung von Begriffen wie Notwendigkeit und Verhältnismäßigkeit im RFSR-Bereich ebenfalls nicht geringer sein dürfen als ihnen gemäß Artikel 8 EMRK zukommt.

TEIL III

3.0 Auffassungen des EGMR zur Notwendigkeit und Verhältnismäßigkeit sowie zum Recht auf Privat- und Familienleben

3.1 Ausgehend von der in Abschnitt 2 erläuterten Verknüpfung zwischen Privatsphäre und Datenschutz sowie davon, dass der EGMR die Begriffe der Notwendigkeit und der Verhältnismäßigkeit in seiner Auslegung von Artikel 8 EMRK entwickelt hat, müssen wir zum Verständnis seines Ansatzes zunächst seine Rechtsprechung betrachten.

3.2 Artikel 8 Absatz 1 EMRK lautet:

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."

Das Recht ist jedoch nicht absolut, und in Artikel 8 Absatz 2 sind die Gründe aufgeführt, unter denen der Staat in das Recht einer Person auf Privatsphäre eingreifen darf:

„Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist 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."

3.3 Der EGMR hat drei Kriterien aufgestellt, die zu erfüllen sind, damit ein Eingriff dem Artikel 8 Absatz 2 genügt. Ein Eingriff muss somit

- gesetzlich vorgesehen sein,
- eines der in Artikel 8 Absatz 2 genannten berechtigten Ziele verfolgen und
- in einer demokratischen Gesellschaft notwendig sein.

Ein Eingriff in die Rechte einer Person nach Artikel 8 muss daher alle drei Prüfkriterien erfüllen, damit er als gerechtfertigt gilt. Im Folgenden hat die Datenschutzgruppe die einschlägige Rechtsprechung des EGMR entweder zusammengefasst oder angeführt, damit ersichtlich wird, was der Gerichtshof zu den einzelnen Kriterien geäußert hat.

3.4 Kriterium 1: Gesetzlich vorgesehen

In der Rechtssache *MM / Vereinigtes Königreich*[5] legte der EGMR die Kriterien dafür fest, wann ein Akt oder eine Tätigkeit „gesetzlich vorgesehen" ist. Eine Handlung muss eine Grundlage im einzelstaatlichen Recht haben, mit dem Rechtsstaatsprinzip vereinbar sein und die Rechtsvorschriften müssen angemessen zugänglich und berechenbar, d. h. so genau formuliert sein, dass die betreffende Person ihr Verhalten daran ausrichten kann.[6]

Damit diese Anforderungen erfüllt werden, müssen die Rechtsvorschriften laut EGMR

„einen angemessenen Rechtsschutz vor Willkür bieten und dementsprechend den Ermessensspielraum, den die zuständigen Behörden haben, und die Art und Weise, wie dieser genutzt werden darf, hinreichend klar festlegen."[7]

Eine Handlung gilt also als gesetzlich vorgesehen, wenn sie eine Rechtsbasis hat (entweder im Gesetzesrecht oder im Richterrecht (Common Law)) und darin eindeutig geregelt ist, wie die Handlung erfolgt. Zudem sollten diese Regeln gegebenenfalls auch eindeutige Festlegungen zum Ermessensspielraum der Strafverfolgungsbehörde sowie Orientierungshilfen für dessen Nutzung beinhalten und angemessene rechtliche Garantien bieten.

3.6 Kriterium 2: Ein berechtigtes Ziel verfolgen

Dieses Kriterium erklärt sich hinreichend von selbst, ist jedoch eng mit der Anforderung verbunden, dass ein Eingriff „in einer demokratischen Gesellschaft notwendig" sein muss. Um ein berechtigtes Ziel zu verfolgen, muss

[5] *MM gegen Vereinigtes Königreich*, BNr. 24029/07 (EGMR 13. November 2012).

[6] *Huvig gegen Frankreich*, BNr. 11105/84 (EGMR 24. April 1990).

[7] *MM gegen Vereinigtes Königreich*, BNr. 24029/07 (EGMR 13. November 2012).

eine Tätigkeit zur Verfolgung eines der in Artikel 8 Absatz 2 genannten Ziele ausgeführt werden, z. B. zur Aufrechterhaltung der Ordnung und zur Verhütung von Straftaten oder deren Aufdeckung, zum Schutz der Rechte und Freiheiten anderer usw.

3.7 Kriterium 3: In einer demokratischen Gesellschaft notwendig

Hier besteht eine enge Verbindung mit dem vorherigen Kriterium. Eine RFSR-Maßnahme muss auch „in einer demokratischen Gesellschaft notwendig" sein, wenn sie zu einem Eingriff führt, der zur Verfolgung des berechtigten Zieles erfolgt.

3.8 Der EGMR hat in einer ganzen Reihe von Fällen die Bedeutung der Aussage „in einer demokratischen Gesellschaft notwendig" untersucht. So führte der Gerichtshof in der Rechtssache *Handyside / Vereinigtes Königreich*[8] aus, dass „notwendig" nicht mit „unverzichtbar" gleichzusetzen ist; ebenso wenig besitzt das Wort die Flexibilität von Ausdrücken wie „zulässig", „regulär", „nützlich", „vertretbar" oder „wünschenswert".[9] Auch befand der EGMR: *„In diesem Zusammenhang impliziert ‚Notwendigkeit' das Vorhandensein eines zwingenden gesellschaftlichen Bedürfnisses".*[10]

3.9 Dies ist von Bedeutung, heißt es doch, dass „Notwendigkeit" nicht zu weit ausgelegt werden sollte, da sich Grundrechte sonst leichter umgehen ließen. Zum anderen sollte der Ausdruck nicht zu wörtlich ausgelegt werden, da dadurch die Schwelle zu hoch wäre und ansonsten legitime Tätigkeiten, die einen Eingriff in die Grundrechte rechtfertigen können, übermäßig erschwert würden.

3.10 In derselben Sache betrachtete der Gerichtshof das Recht auf freie Meinungsäußerung, auf die Existenz und Fortentwicklung einer „demokratischen Gesellschaft". Er befand: *„Ausgehend davon „muss jede auferlegte ‚Formalität', ‚Bedingung', ‚Einschränkung' oder ‚Strafe' in einem angemessenen Verhältnis zu dem verfolgten berechtigten Ziel stehen."*[11]

3.11 Außerdem erläuterte der EGMR, dass seine Aufgabe dann darin besteht zu entscheiden, *„ob die von der Polizei angeführten Gründe für die Rechtfertigung der tatsächlichen ‚Eingriffsmaßnahmen' stichhaltig und ausreichend sind".*[12]

---

[8] *Handyside gegen Vereinigtes Königreich*, BNr. 5493/72 (EGMR 7. Dezember 1976).

[9] *Handyside gegen Vereinigtes Königreich*, BNr. 5493/72 (EGMR 7. Dezember 1976) Rn. 48.

[10] *The Sunday Times gegen Vereinigtes Königreich*, BNr. 6538/74 (EGMR 6. November 1980) Rn. 59.

[11] *Handyside gegen Vereinigtes Königreich*, BNr. 5493/72 (EGMR 7. Dezember 1976) Rn. 49.

[12] *Handyside gegen Vereinigtes Königreich*, BNr. 5493/72 (EGMR 7. Dezember 1976) Rn. 50.

3.12 Mittlerweile haben sich mehrere Rechtssachen vor dem EGMR auf einen oder mehrere der Prüfaspekte bezogen, die der EGMR anwendet, wenn er feststellen soll, ob eine Maßnahme „in einer demokratischen Gesellschaft notwendig" ist.[13]

Zwingendes gesellschaftliches Bedürfnis – Entspricht der Eingriff einem zwingenden gesellschaftlichen Bedürfnis?

Verhältnismäßigkeit – Steht der von der Maßnahme verursachte Eingriff in einem angemessenen Verhältnis zu dem verfolgten berechtigten Ziel?

Stichhaltige und ausreichende Gründe – Waren die zur Rechtfertigung des Eingriffs angeführten Gründe stichhaltig und ausreichend?

Auch hier möchte die Datenschutzgruppe im Folgenden einige Erläuterungen dazu anführen, wie der EGMR die einzelnen Prüfaspekte behandelt.

3.13 Prüfaspekt 1: Zwingendes gesellschaftliches Bedürfnis

Weiter oben wurde bereits erläutert, dass eine RFSR-Behörde ein berechtigtes Ziel gemäß Artikel 8 Absatz 2 haben könnte, z. B. die Verhütung, Aufdeckung und Untersuchung einer Straftat. Obwohl der Ausdruck „zwingendes gesellschaftliches Bedürfnis" schwer zu fassen ist, wird es dabei im Rahmen des breiteren Spektrums des verfolgten berechtigten Zieles immer um die Angabe des konkreten gesellschaftlichen Bedürfnisses gehen, dem im Interesse der öffentlichen Sicherheit entsprochen werden soll.

3.14 Im Wesentlichen versucht der EGMR festzustellen, ob die RFSR-Behörde beispielsweise den Grund dafür angegeben hat, warum sie in das Recht einer Person auf Privatsphäre eingreifen muss. Der Ausdruck „***zwingendes*** gesellschaftliches Bedürfnis" impliziert jedoch einen höheren Schwere-, Dringlichkeits- oder Unmittelbarkeitsgrad im Zusammenhang mit dem Bedürfnis, dem sich die Maßnahme zuwendet. Deshalb sind bei der Bestimmung des zwingenden gesellschaftlichen Bedürfnisses eine Reihe von Faktoren zu berücksichtigen, so zum Beispiel das öffentliche Interesse oder die Art des zu lösenden Problems. Diese Faktoren beeinflussen natürlich alle personenbezogenen Daten, die zur Lösung dieses Problems/dieses zwingenden gesellschaftlichen Bedürfnisses verarbeitet werden.

[13] Siehe beispielsweise *S & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008) Rn. 101; *Khelili gegen Schweiz*, BNr. 16188/07 (EGMR 18. Oktober 2011); *Klass u. a. gegen Deutschland*, BNr. 5029/71 (6. September 1978); *Leander gegen Schweden*, BNr. 9248/81 (EGMR 26. März 1987); *Huvig gegen Frankreich*, BNr. 11105/84 (EGMR 24. April 1990); *Z gegen Finnland*, BNr. 22009/93 (EGMR 25. Februar 1997); *K & T gegen Finnland*, BNr. 25702/94 (12. Juli 2001).

3.15 Ein besonderer Fall, der vom EGMR geprüft wurde, war die Rechtssache *Dudgeon gegen Vereinigtes Königreich*[14]. Der Beschwerdeführer brachte vor, dass die in Nordirland geltenden Rechtsvorschriften, die gleichgeschlechtliche Handlungen unter Strafe stellen, unabhängig davon, wo sie stattfinden, wie alt die Beteiligten sind oder ob sie ihre Einwilligung gegeben haben bzw. einwilligungsfähig sind, seine Rechte gemäß Artikel 8 EMRK verletzen.

3.16 Obwohl der EGMR einräumte, dass eine gewisse Regelung sämtlicher sexueller Handlungen notwendig ist, war zu bestimmen, ob die Rechtsvorschriften in Nordirland, die weit über die Regelung ähnlicher Handlungen in anderen Vertragsstaaten der EMRK hinausgehen, dennoch „notwendig" sind.[15]

3.17 Mit Verweis auf die berechtigten Ziele, die als Grund für die Rechtsvorschriften angegeben wurden, sowie darauf, dass sich die Einstellung der Gesellschaft gegenüber Homosexualität seit dem Erlass der Rechtsvorschriften wesentlich geändert hat, erklärte der EGMR:

„Unter diesen Umständen kann nicht daran festgehalten werden, dass ein ‚zwingendes gesellschaftliches Bedürfnis' besteht, solche Handlungen zu kriminalisieren, zumal es an einer ausreichenden Rechtfertigung im Sinne des Schutzes vor den Risiken für schutzbedürftige Gruppen der Gesellschaft oder vor den Folgen für die Öffentlichkeit fehlt."[16]

Obgleich also die nordirische Polizei ein berechtigtes Ziel verfolgte, konnte sie bei der Beurteilung, ob die ergriffenen Maßnahmen „in einer demokratischen Gesellschaft notwendig" waren, dem Prüfaspekt „zwingendes gesellschaftliches Bedürfnis" nicht standhalten, da sie dem EGMR nicht zufriedenstellend nachzuweisen vermochte, dass ein derartiges Bedürfnis vorlag[17]. Zwar hatte es Einwände aus bestimmten Bereichen der Gesellschaft gegeben, doch deuteten die toleranteren Ansichten der Gesellschaft insgesamt darauf hin, dass keine Notwendigkeit mehr dafür besteht, dass die Rechtsvorschriften so weit gehen, wie es in Bezug auf gleichgeschlechtliche Handlungen zwischen männlichen Homosexuellen der Fall ist. Darüber hinaus lagen keine ausreichenden Beweise dafür vor, dass diese Maßnahmen gerechtfertigt waren, um Schaden von diesen schutzbedürftigen Gruppen der Gesellschaft abzuwenden, oder dass sie bei Nichtanwendung negative Folgen für die Öffentlichkeit gehabt hätten.

---

[14] *Dudgeon gegen Vereinigtes Königreich*, BNr. 7525/76 (EGMR 22. Oktober 1981).

[15] *Dudgeon gegen Vereinigtes Königreich*, BNr. 7525/76 (EGMR 22. Oktober 1981) *„die öffentliche Ordnung und Sitte zu bewahren [und] den Bürger vor Dingen zu schützen, die anstößig oder verletzend sind … hinreichenden Schutz gegen Ausbeutung und verderbliche Beeinflussung anderer zu gewährleisten, insbesondere für Personen, die in besonderem Maße schutzbedürftig sind, weil sie jung, schwach an Körper oder Geist sind, unerfahren sind oder sich im Zustand besonderer physischer, rechtlicher oder wirtschaftlicher Abhängigkeit befinden*".

[16] *Dudgeon gegen Vereinigtes Königreich*, BNr. 7525/76 (EGMR 22. Oktober 1981) Rn. 60.

[17] Siehe dazu auch *Khelil gegen Schweiz*, BNr. 16188/07 (EGMR 18. Oktober 2011).

3.18 Dem Wesen nach ist ein zwingendes gesellschaftliches Bedürfnis fließend und mit einem Element der Subjektivität behaftet. Entscheidend für seine Erfüllung sind daher der Kontext und der entsprechende Nachweis. Der Schweregrad eines zwingenden gesellschaftlichen Bedürfnisses oder der damit verbundene Schaden, Nachteil bzw. negative Effekt für die Gesellschaft kann einen Einfluss darauf haben, wie „zwingend" das zwingende gesellschaftliche Bedürfnis ist.

Beispielsweise lässt sich argumentieren, dass sexuelle Gewaltkriminalität in der öffentlichen Wahrnehmung schwerer wiegt bzw. zwingender ist als Einbruchdiebstahl. Daher ließe sich nachvollziehen, dass stärkere Eingriffe in die Privatsphäre oder die Datenschutzrechte einer Person gerechtfertigt wären, um diese Art der Kriminalität zu bekämpfen. Es ließe sich jedoch gleichermaßen anführen, dass Einbruchdiebstahl aufgrund seiner Häufigkeit, der Art der Ausführung dieser Straftat und der Anzahl der davon betroffenen Menschen in einem oder mehreren Mitgliedstaaten als ebenso schwerwiegend, wenn nicht noch schwerwiegender gelten könnte. Maßgeblich bei der Bestimmung des Schweregrades sind jedoch der Kontext und die Belege für die Begründung von Eingriffen zur Bekämpfung dieser Straftaten.

3.19 Ausgehend von den vorstehenden Ausführungen und nach Durchsicht eines Großteils der Rechtsprechung des EGMR in diesem Bereich ist festzustellen, dass sich der EGMR bei der Bewertung des „zwingenden gesellschaftlichen Bedürfnisses" offenbar von folgenden möglichen Faktoren leiten lässt (die Liste ist nicht erschöpfend):

- Soll mit der Maßnahme auf ein Problem eingegangen werden, das ansonsten schädliche oder andere nachteilige Auswirkungen auf die Gesellschaft oder eine Gruppe der Gesellschaft haben könnte?
- Ist belegt, dass die Maßnahme diese schädlichen Auswirkungen abmildern kann?
- Welche Auffassungen (z. B. gesellschaftlicher, historischer oder politischer Art) vertritt die Gesellschaft allgemein zu dem betreffenden Problem?
- Wurden etwaige konkrete Meinungen/Einwände der Gesellschaft zu einer bzw. gegen eine Maßnahme oder eine Problemstellung hinreichend berücksichtigt?

3.20 Prüfaspekt 2: Verhältnismäßigkeit

Der zweite Prüfaspekt (Verhältnismäßigkeit) des EGMR verlangt im Wesentlichen, dass eine Maßnahme, die in ein in der EMRK verankertes Recht eingreift, nicht weiter gehen sollte als zur Erfüllung des verfolgten berechtigten Zieles notwendig.

3.21 Zwei beachtenswerte Beschwerdeverfahren des EGMR im Zusammenhang mit der Frage der Verhältnismäßigkeit im Bereich des Datenschutzrechts waren *Z gegen Finnland*[18] und *S. & Marper gegen Vereinigtes Königreich*[19]. In der Rechtssache *S & Marper* brachten die Beschwerdeführer vor, dass die Speicherung ihrer DNA-Profile und Fingerabdrücke durch die Polizei einen nicht gerechtfertigten Eingriff in ihre Rechte gemäß Artikel 8 darstellt. In der Rechtssache *Z* ging es darum, dass die personenbezogenen Angaben der Beschwerdeführerin (einschließlich ihres Gesundheitszustands) öffentlich bekanntgemacht wurden.

3.22 In beiden Fällen räumte der EGMR ein, dass die fraglichen Handlungen das berechtigte Ziel der Verhütung oder Aufdeckung von Straftaten verfolgten. Anschließend wandte sich der EGMR der Frage zu, ob die Handlungen „in einer demokratischen Gesellschaft notwendig" waren.

3.23 In Anbetracht dessen befand der EGMR, dass die angeführten Gründe nicht stichhaltig und ausreichend waren, um das Interesse des Beschwerdeführers an der Vertraulichkeit der Daten außer Kraft zu setzen.

3.24 In der Rechtssache *S. & Marper* kritisierte der EGMR die *„pauschale und unterschiedslose Befugnis"*[20] zur Einholung und Aufbewahrung von DNA-Proben. Er stellte fest, dass die *„Art oder Schwere der Straftat"*[21] oder *„das Alter des verdächtigten Straftäters"*[22] nicht berücksichtigt wurden, und merkte an, dass die Aufbewahrung unabhängig von der Art und Schwere der Straftat unbefristet erfolgte. Ebenfalls hervorgehoben wurde das Fehlen von Schutzvorkehrungen, vor allem die *„beschränkten Möglichkeiten für einen Freigesprochenen, die Daten entfernen zu lassen"*[23] sowie das Fehlen einer unabhängigen Überprüfung der Berechtigung für die Aufbewahrung der Proben.

3.25 Die vom EGMR in beiden Fällen betrachteten Faktoren lassen die breite Palette von Faktoren erkennen, die bei der Beurteilung der Verhältnismäßigkeit einer Maßnahme relevant sein können. Besonders die Rechtssache *S. & Marper* zeigt, dass eine pauschale Maßnahme, selbst wenn sie nachgewiesenermaßen ein berechtigtes Ziel verfolgt, wohl nicht als verhältnismäßig betrachtet werden kann, wenn es darum geht, ob sie „in einer demokratischen Gesellschaft notwendig" ist.[24]

[18] *Z. gegen Finnland*, BNr. 22009/93 (EGMR 25. Februar 1997).

[19] *S. & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008).

[20] *S. & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008) Rn. 119.

[21] *S. & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008) Rn. 35.

[22] *S. & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008) Rn. 119.

[23] *S. & Marper gegen Vereinigtes Königreich*, BNr. 30562/04 und 30566/04 (EGMR 4. Dezember 2008) Rn. 119.

[24] Siehe dazu auch *Campbell gegen Vereinigtes Königreich*, BNr. 3578/05 (EGMR 27. März 2008).

3.26 Ausgehend von den vorstehenden Ausführungen und nach Durchsicht eines Großteils der Rechtsprechung des EGMR in diesem Bereich ist festzustellen, dass sich der EGMR bei der Bewertung der „Verhältnismäßigkeit" offenbar von folgenden möglichen Faktoren leiten lässt (die Liste ist nicht erschöpfend):

- **Vorhandene und geplante Maßnahmen**

  Es sei darauf hingewiesen, dass dieser Faktor auch auf den Begriff der Notwendigkeit im engeren Sinne zutrifft. Bei der Betrachtung, ob eine geplante Maßnahme (entweder durch Ersatz oder durch Ergänzung vorhandener Maßnahmen) notwendig ist, besteht eine Möglichkeit darin, zunächst die Effektivität der vorhandenen Maßnahmen gegenüber der geplanten Maßnahme zu prüfen. Dabei kann jede vorhandene/geplante Maßnahme einzeln oder können die vorhandenen Maßnahmen ganzheitlich betrachtet werden. Erfüllt die geplante Maßnahme das Notwendigkeitskriterium, muss sie auch der Prüfung standhalten, ob es sich noch um eine verhältnismäßige Reaktion handelt. Dazu sind das berechtigte Ziel, das die geplante Maßnahme verfolgt, und das ermittelte zwingende gesellschaftliche Bedürfnis gegen die mit dem Recht des Einzelnen auf Privatsphäre verbundenen Rechte und Freiheiten aufzuwiegen.

  Wie auch immer diese Bewertung durchgeführt wird, sie sollte eine nachweisgeführte Erklärung beinhalten, warum die vorhandenen Maßnahmen für die Erfüllung dieses Bedürfnisses nicht mehr ausreichen. Es muss eindeutig nachweisbar sein, wie die geplante Maßnahme das zwingende gesellschaftliche Bedürfnis anpacken soll. Dazu können belegte Beispiele angeführt werden, wo die Maßnahme schon einmal unter gleichen oder ähnlichen Umständen eingesetzt wurde und sich als wirksam erwiesen hat. Wenn die neue Maßnahme zum Teil damit begründet wird, dass Defizite bei der Wirksamkeit der vorhandenen Maßnahmen beseitigt werden sollen, dann ist auch dies genau zu erläutern und zu belegen.

  An dieser Stelle sollte erläutert werden, welche anderen Maßnahmen in Betracht kamen und ob diese den Erkenntnissen zufolge einen stärkeren oder einen geringeren Eingriff in die Privatsphäre darstellen. Wurden Maßnahmen abgewiesen, die den Erkenntnissen zufolge weniger stark in die Privatsphäre eingreifen, dann sind stichhaltige Gründe dafür anzuführen, warum nicht diese Maßnahmen für die Durchführung ausgewählt wurden.[25]

[25] Hilfreich dabei ist ein Blick in die Arbeiten der Datenschutzgruppe zu Datenschutz-Folgeabschätzungen.

- **Geltungsbereich – Ist der Geltungsbereich der geplanten Maßnahme ausreichend begrenzt?**

Dazu kann die Anzahl der von der Maßnahme betroffenen Personen oder die Menge der erfassten Informationen oder der Aufbewahrungszeitraum dieser Informationen gehören. Der Geltungsbereich kann sich je nach Art der betreffenden Maßnahme auf alle, einige oder keinen dieser Punkte beziehen.

- **Schutzvorkehrungen – Welche Maßnahmen bestehen zum Schutz der Grundrechte?**

Der Begriff „Schutzvorkehrungen" in diesem Zusammenhang ist ebenfalls weit gefasst und kann zum Beispiel Schritte zur Begrenzung des Geltungsbereichs einer Maßnahme oder Vorbehalte für ihre Anwendung umfassen. Zum anderen kann auch eine andere objektive Entscheidung vor dem Einsatz einer Maßnahme zur Auflage gemacht werden. Schutzvorkehrungen können auch verfügbare Rechtsbehelfe für Personen gegen eine bestimmte Maßnahme bzw. deren Wirkungen sowie den Umfang dieser Rechtsbehelfe beinhalten.

- **Charakter des Eingriffs**

Dazu könnte die Art der erfassten Informationen, der Kontext, in dem die Maßnahme durchgeführt werden soll, oder die Art der Handlungen, die der Maßnahme unterliegen sollen, gehören. In der Rechtssache *Dudgeon* stellte der EGMR auf die besonders sensible Art der Handlung ab, die betroffen war, sowie auf die Umstände, unter denen die Maßnahme angewandt wurde. Obgleich die Sensibilität der betroffenen Handlung oder Information von Bedeutung ist, ist es ebenso notwendig zu betrachten, ob eine Maßnahme in Situationen erfolgt, bei denen Personen in erhöhtem Maße davon ausgehen, dass ihre Privatsphäre geschützt ist. Beispielsweise sind die Erwägungen zur Privatsphäre bei im öffentlichen Straßenland installierten Überwachungskameras völlig anders als bei der Installation derartiger Kameras auf Toiletten oder auf Krankenhausstationen.

- **Stärke des zwingenden gesellschaftlichen Bedürfnisses und Schweregrad des Schadens oder Nachteils für die Öffentlichkeit bzw. der Auswirkungen auf die Öffentlichkeit**

Der Charakter des zwingenden gesellschaftlichen Bedürfnisses, auf das reagiert werden soll, ist ebenso wie der Charakter des Eingriffs einschließlich der Art der betroffenen Handlungen oder erfassten Informationen ein wesentlicher Erwägungspunkt. Je schwerwiegender das Problem und/oder je größer oder schwerer der mögliche Schaden oder Nachteil für die Gesellschaft, desto mehr kann ein Eingriff gerechtfertigt sein.

Dem Vertragsstaat der EMRK steht immer ein Beurteilungsspielraum bei der Ermittlung des zwingenden gesellschaftlichen Bedürfnisses und des Umfangs des Eingriffs bei der Verfolgung eines berechtigten Ziels zu. Der EGMR hat deutlich gemacht, dass die Bewertung dieses Spielraums stets der gerichtlichen Prüfung unterliegt, vor allem die vorhandenen Schutzvorkehrungen.[26]

Ein berechtigtes allgemeines Ziel im Rahmen von Artikel 8 Absatz 2 könnte die Aufrechterhaltung der Ordnung und die Verhütung von Straftaten sein. Es ließe sich argumentieren, dass in der Regel die Verhütung oder Aufdeckung von Straftaten an sich ein zwingendes gesellschaftliches Bedürfnis darstellt und somit jede zu diesem Zweck durchgeführte Handlung stets auf ein zwingendes gesellschaftliches Bedürfnis abzielt. Aber selbst wenn dem so wäre, müsste bei der Bewertung der Verhältnismäßigkeit die konkrete Straftat angegeben werden können, die eine Maßnahme verhüten/aufdecken soll. Zugleich sind der Schaden, der Nachteil oder die Gefahr zu betrachten, denen die Öffentlichkeit ausgesetzt wäre, würde dieses Problem nicht behandelt.

3.27 Prüfaspekt 3: Stichhaltige und ausreichende Gründe

Der dritte Prüfaspekt des EGMR macht deutlich, dass ein Eingriff durch stichhaltige und ausreichende Gründe, verbunden mit den Anforderungen der vorigen zwei Prüfaspekte, gerechtfertigt sein muss. Die Schlussfolgerung, dass stichhaltige und ausreichende Gründe zur Rechtfertigung eines Eingriffs vorliegen, ist nur dann einfacher, wenn sorgfältig geprüft wird, ob ein zwingendes gesellschaftliches Bedürfnis besteht und die vorgeschlagene/ergriffene Maßnahme die Verhältnismäßigkeit am besten wahrt. Neben oder anstatt der eigenen Analyse können RFSR-Behörden/Gesetzgeber jedoch auf Recherchen, Erhebungen oder andere Informationen zurückgreifen, die die Begründung stützen.

3.28 Ein Beispiel dafür, in welchem Umfang ausreichende und stichhaltige Gründe dargelegt werden müssen, zeigt die Rechtssache *K. und T. gegen Finnland*[27]. In diesem Fall gingen die Beschwerdeführer gegen die Entscheidung der finnischen Behörden vor, zwei Kinder aus ihrer Obhut zu nehmen und sie in Pflege zu geben, und beanstandeten die damit zusammenhängenden Einschränkungen für den Umgang. Nach Auffassung des EGMR hatten die Behörden, obwohl sie sich mit zwei Kindern derselben Familie befassten, nur für ein Kind ausreichende und stichhaltige Gründe für ihre Maßnahmen angeführt, nicht jedoch für das andere.

[26] *Klass und andere gegen Deutschland*, BNr. 5029/71, (EGMR 6. September 1978).

[27] *K. und T. gegen Finnland*, BNr. 25702/94, (EGMR 12. Juli 2001).

3.29 Aussagen des EuGH zu Notwendigkeit und Verhältnismäßigkeit sowie zum Recht auf Privat- und Familienleben

3.30 Neben der bisher dargelegten eingehenden Analyse der Rechtsprechung des EGMR zu Artikel 8 der EMRK möchte die Datenschutzgruppe auch auf Bemühungen des EuGH aus jüngerer Zeit aufmerksam machen, die Prüfaspekte Notwendigkeit und Verhältnismäßigkeit auf die Artikel 7 und 8 der Charta anzuwenden. In der Rechtssache Schwarz[28] entwickelte der EuGH eine Methode, um festzustellen, ob die Ausübung der aus den Artikeln 7 und 8 der Charta abgeleiteten Rechte unangemessenerweise eingeschränkt wurde. Der EuGH beginnt seine Prüfung mit Artikel 52 Absatz 1. Demnach, so bekräftigt er, müssen Einschränkungen der Grundrechte

- *gesetzlich vorgesehen sein,*
- *den Wesensgehalt dieser Rechte achten*
- *und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sein*
- *und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen* (Randnr. 34 des Urteils).

3.31 Mit näherem Blick auf die Frage der Verhältnismäßigkeit und Notwendigkeit erklärte der EuGH, er müsse *„prüfen, ob die Einschränkungen dieser Rechte gemessen an den … Zielen [der relevanten Rechtsvorschriften] verhältnismäßig sind. Zu untersuchen ist daher, ob die … eingesetzten Mittel zur Erreichung dieser Ziele geeignet sind und nicht über das dazu Erforderliche hinausgehen“* (siehe Randnr. 40 des Urteils).

Außerdem erklärte der Gerichtshof in Randnr. 46 der Urteils: *„Was sodann die Prüfung der Erforderlichkeit einer solchen Verarbeitung betrifft, hat der Gesetzgeber insbesondere zu prüfen, ob Maßnahmen denkbar sind, die weniger stark in die durch die Art. 7 und 8 der Charta anerkannten Rechte eingreifen und trotzdem den Zielen der in Rede stehenden Unionsregelung wirksam dienen“.*

3.32 Erst unlängst stellte der Generalanwalt des EuGH, Pedro Cruz Villalón, seine Schlussanträge in den verbundenen irischen und österreichischen Rechts-

[28] *Schwarz / Stadt Bochum*, EuGH, C-291/12, (EuGH 17. Oktober 2013), noch nicht veröffentlicht. *Herr Schwarz klagte gegen die Behörden der Stadt Bochum, die sich weigerten, ihm einen Reisepass auszustellen, solange er nicht bereit war, sich zwei Fingerabdrücke zur Speicherung auf diesem Reisepass abnehmen zu lassen. Diese Verpflichtung geht zurück auf die Verordnung (EG) Nr. 2252/2004 vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten.*

sachen C-293/12 und C-594/12 (Dezember 2012). Darin stellte er klar, dass die Richtlinie über die Vorratsdatenspeicherung 2006/24/EG zwar ein berechtigtes Ziel verfolge, sie aber dennoch nicht erforderlich sei, da sie *„mit dem Grundsatz der Verhältnismäßigkeit unvereinbar sei, soweit sie den Mitgliedstaaten vorschreibe, sicherzustellen, dass die Daten für die Dauer von bis zu zwei Jahren auf Vorrat gespeichert würden.“*[29] Deshalb sei die Richtlinie über die Vorratsdatenspeicherung nicht erforderlich, da für die Vorratsspeicherung von zwei Jahren keine stichhaltigen und ausreichenden Gründe angegeben werden. Das habe zu einem unverhältnismäßigen Eingriff in das Privatleben von Kunden geführt, deren Daten ohne Verdacht für die Höchstdauer von zwei Jahren gespeichert werden.

3.33 Zusammenfassung

Es sei nachdrücklich darauf hingewiesen, dass nach eindeutiger Auffassung des EGMR die Schwelle der Notwendigkeit nur dann überschritten wird, wenn alle drei Kriterien erfüllt sind.

Daher muss jedes einzelne Kriterium – „gesetzlich vorgeschrieben“, „berechtigtes Ziel“ und „in einer demokratischen Gesellschaft notwendig“ (inklusive der drei Prüfaspekte) – geprüft werden und erfüllt sein, damit sichergestellt ist, dass eine RFSR-Maßnahme einen notwendigen Eingriff in das Recht des Einzelnen auf Privat- und Familienleben darstellt.

Aus der Rechtsprechung folgt ebenfalls, dass zwischen Privatsphäre und Datenschutz eine Beziehung besteht, die eine gemeinsame Behandlung beider Bestimmungen erforderlich macht. Diese Beziehung wird von der Datenschutzgruppe in den Teilen IV und V weiter beleuchtet.

TEIL IV

4.0 Herstellung der Verknüpfung zwischen Privatsphäre und Datenschutz

Wie bereits an anderer Stelle erläutert, soll gemäß Artikel 52 Absatz 3 der Charta jede Auslegung von Artikel 7 der Charta die gleiche Bedeutung haben wie Artikel 8 EMRK. Der Schutz personenbezogener Daten ist auch als Grundrecht in Artikel 8 der Charta verankert, und konkrete Bestimmungen zu seiner Umsetzung sind in Artikel 16 des Vertrags von Lissabon aufgeführt. Eine spezifische Regelung des Rechts enthalten die geltende

[29] Schlussanträge des Generalanwalts, Pressemitteilung http://europa.eu/rapid/press-release_CJE-13-157_de.htm

Datenschutzrichtlinie 95/46/EG sowie der Rahmenbeschluss über den Datenschutz (2008/977/JI). Obwohl die Richtlinie 95/46/EG nicht unbedingt alle RFSR-Behörden in allen Mitgliedstaaten erfasst, sind ihre (aus dem Übereinkommen 108 abgeleiteten) Grundsätze im Allgemeinen dennoch anwendbar. Da sich nicht viele RFSR-Maßnahmen denken lassen, die einen Eingriff in die Privatsphäre darstellen, ohne dass personenbezogene Daten verarbeitet werden, sind bei der Planung, Umsetzung und Überprüfung einer RFSR-Maßnahme beide Rechte und beide Regelungen zu ihrem Schutz zu berücksichtigen.

4.1 Bei der Betrachtung einer RFSR-Maßnahme ist mehreren Faktoren Rechnung zu tragen, um sicherzustellen, dass sie sowohl mit den Vorschriften zur Privatsphäre als auch mit den Vorschriften zum Datenschutz im Einklang steht. Wie bei allen Grundrechten unterliegen Einschränkungen des Rechts auf Privatsphäre und des Rechts auf Datenschutz den Anforderungen von Artikel 52 Absatz 1 der Charta: „Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen."

Der Begriff „erforderlich" bzw. „notwendig" erscheint auch in Sekundärrechtsvorschriften, z. B. in Artikel 3 des Rahmenbeschlusses. Vorbehaltlich der verschiedenen Bedingungen für die Anwendung der Richtlinie im RFSR-Kontext sei darauf hingewiesen, dass der Begriff „erforderlich" bzw. „notwendig" darin häufig verwendet wird, wobei seine Verwendung in den Artikeln 6 und 7 mit Grundsätzen in Bezug auf die Zulässigkeit der Verarbeitung von Daten vielleicht am wichtigsten ist. Von besonderer Relevanz im Zusammenhang mit der Notwendigkeit in einem RFSR-Kontext ist Artikel 7 Buchstabe e. Darin heißt es, dass die Verarbeitung nur unter folgender Voraussetzung zulässig ist: *„die Verarbeitung ist **erforderlich** für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde"*.

In dieser Hinsicht bietet der Begriff „erforderlich" in der Richtlinie eine wichtige Schutzvorkehrung in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten, und im Zusammenhang mit Artikel 13 sollte er als Schutzvorkehrung betrachtet werden, die eine Datenverarbeitung für die in diesem Artikel aufgeführten Zwecke *beschränkt*.

4.2 In Bezug auf die Verarbeitung von Daten im RFSR-Kontext äußerte sich der EuGH ausdrücklich zum Begriff der Erforderlichkeit und zu seiner einheitlichen Anwendung sowie den Auswirkungen auf den Datenschutz: *„Ange-*

sichts des Zieles der Gewährleistung eines gleichwertigen Schutzniveaus in allen Mitgliedstaaten kann … der Begriff der Erforderlichkeit im Sinne von Art. 7 Buchst. e der Richtlinie 95/46 … in den einzelnen Mitgliedstaaten keinen variablen Inhalt haben."[30]

Obwohl sich beim EuGH nur ein kleinerer Teil der Rechtsprechung mit dieser Beziehung befasst, stimmen die Entscheidungen des Gerichtshofs weitgehend mit dem Ansatz des EGMR überein. Der vom EGMR verfolgte Ansatz gegenüber dem Begriff der Notwendigkeit dürfte daher als schlüssiges Konzept für seine Anwendung im Zusammenhang mit dem Datenschutz gelten.

TEIL V

5.0 Sicherstellung, das RFSR-Maßnahmen im Einklang mit den Vorschriften zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten stehen

Privatsphäre und Datenschutz sind zwei eigenständige Begriffe, die jedoch oft miteinander in Wechselbeziehung stehen. Bei der Umsetzung einer RFSR-Maßnahme, die beide berührt, müssen also auch beide berücksichtigt werden.

Der EGMR hat – wie weiter oben dargestellt – sein Herangehen an den Aspekt der Privatsphäre bei derartigen Maßnahmen deutlich gemacht. Auch der EuGH hat erste Urteile gefällt, bei denen in Rechtssachen zu Privatsphäre und Datenschutz eine entsprechende Prüfung der Erforderlichkeit und Verhältnismäßigkeit erfolgte. Die Datenschutzgruppe wird nunmehr auf einige weitere konkrete Beispiele eingehen, bei denen es um die Erforderlichkeit bzw. Notwendigkeit und Verhältnismäßigkeit in den Datenschutzrechtsvorschriften geht. Dabei sind die Beispiele anhand der folgenden vier Grundprinzipien des Datenschutzes gegliedert, wie sie in der Richtlinie aufgeführt sind: Verarbeitung der Daten nach Treu und Glauben und auf rechtmäßige Weise, Zweckbindung und Datenminimierung sowie Aufbewahrung der Daten. Die Datenschutzgruppe bezieht sich auf die Richtlinie, obgleich diese als Instrument aus der Zeit vor dem Vertrag von Lissabon für einen Großteil des RFSR-Bereichs nicht anwendbar ist. Dennoch möchte die Datenschutz-

[30] Rechtssache C-524/06 Huber / Deutschland, EuGH (16. Dezember 2008) http://curia.europa.eu/juris/document/document.jsf?text=&docid=76077&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=30432

gruppe daran erinnern, dass die Grundsätze der Richtlinie im Bereich Datenschutz allgemein gelten, da sie auch in anderen Instrumenten wie dem Übereinkommen 108 und dem Rahmenbeschluss über den Datenschutz erscheinen, die für den RFSR-Bereich gültig sind.

5.1 Verarbeitung der Daten nach Treu und Glauben und auf rechtmäßige Weise

Der erste Grundsatz der Richtlinie wird in Artikel 6 Absatz 1 Buchstabe a wie folgt ausgedrückt:

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden.

5.2 Eine RFSR-Behörde muss einen gesetzlichen Rahmen (Richterrecht oder Gesetzesrecht) haben, der sicherstellt, dass die von ihr ausgeübten Befugnisse legitim sind. In einem Rechtskreis, in dem gesetztes Recht gilt, kommt es besonders darauf an, dass die RFSR-Behörde über eine Rechtsgrundlage für die Ausübung bestimmter Befugnisse zur Verfolgung des berechtigten Ziels verfügt. Zur Gewährleistung der vollständigen Einhaltung des Begriffs „auf rechtmäßige Weise" beim Datenschutz empfiehlt es sich, die drei Prüfaspekte des EGMR zum Kriterium „in einer demokratischen Gesellschaft notwendig" auch in Bezug auf die Datenschutzvorschriften anzuwenden.

5.3 Beispielsweise wurde in der Rechtssache Dudgeon gegen Vereinigtes Königreich[31] nicht bestritten, dass die Polizei dem Gesetz entsprechend gehandelt oder ein berechtigtes Ziel verfolgt hat. Sie hat es jedoch versäumt nachzuweisen, dass die von ihr unternommenen Schritte zum Eingriff in das Privatleben von Herrn Dudgeon „in einer demokratischen Gesellschaft notwendig" waren. Einen ähnlichen Ansatz verfolgte die Datenschutzgruppe, als sie ihre Stellungnahme zu den Vorschlägen der Europäischen Kommission über intelligente Grenzen abgab. Hier hatte die Kommission vier zentrale Ziele ins Visier genommen, die eine Verarbeitung der Daten von Millionen von Bürgern verlangen würden. Die Datenschutzgruppe gelangte jedoch zu dem Schluss, dass unzureichend nachgewiesen wurde, wie die in den Kommissionsvorschlägen genannten Ziele erreicht werden können. Aus Datenschutzsicht hatte die Kommission nicht mit hinreichender Klarheit den Zweck der Verarbeitung der Daten dargelegt, was bedeutete, dass auch die Grundsätze Datenminimierung/ Datenspeicherung nicht beachtet wurden.

[31] *Dudgeon gegen Vereinigtes Königreich*, BNr. 7525/76 (EGMR 23. September 1981).

Aus der breiter gefassten Perspektive des Schutzes der Privatsphäre betrachtet stellten die Vorschläge keine verhältnismäßige Reaktion auf das ermittelte zwingende gesellschaftliche Bedürfnis und letztendlich das verfolgte berechtigte Ziel dar. Somit wären die Maßnahmen aus beiden Blickwinkeln heraus nicht rechtmäßig gewesen.

5.4 Im Vereinigten Königreich wurde die Datenschutzrichtlinie so umgesetzt, dass auch alle Strafverfolgungsorgane ihren Bestimmungen unterliegen. Somit ergriff die britische Datenschutzbehörde formelle Durchsetzungsmaßnahmen gegen eine Polizeidienststelle, da diese sämtliche Straßen innerhalb und außerhalb einer kleinen Landgemeinde in der englischen Grafschaft Hertfordshire mit einer automatischen Fahrzeugkennzeichenerfassung ausgestattet hatte. In diesem Fall stand die Verarbeitung personenbezogener Daten allgemein im Einklang mit den Anforderungen des nationalen Datenschutzrechts. Die Dienststelle hielt die entsprechenden nationalen Vorschriften für die Speicherung ein, verarbeitete die erfassten personenbezogenen Daten für polizeiliche Maßnahmen und verarbeitete keine irrelevanten oder unrichtigen Daten für diesen Zweck.

Dennoch müssen personenbezogene Daten auch „auf rechtmäßige Weise“ unter Einhaltung anderer Rechte und rechtlicher Verpflichtungen, einschließlich des Rechts auf Privatsphäre, verarbeitet werden. Der Argumentation der EGMR folgend, stellte die britische Datenschutzbehörde bei genauerer Prüfung fest, dass die Dienststelle es versäumt hatte, ein ausreichend zwingendes gesellschaftliches Bedürfnis anzugeben, das den Grad des Eingriffs in das Privatleben so vieler (unschuldiger) Personen rechtfertigen würde. Ebenso wenig wurde hinreichend nachgewiesen, wie die Einführung der automatischen Kennzeichenerfassung in diesem Ausmaß in einer Gegend mit niedriger Kriminalität einen signifikanten Beitrag zur Lösung der von der Polizeidienststelle angegebenen Probleme leisten würde. Daher befand die britische Datenschutzbehörde, dass die Maßnahme einen ungerechtfertigten Eingriff in die Rechte der Personen auf Privatsphäre gemäß Charta/EMRK darstellt. Die Verarbeitung der Daten war somit im datenschutzrechtlichen Sinne unrechtmäßig.

5.5 Damit gewährleistet ist, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden, muss eine RFSR-Maßnahme also rechtskonform und Bestandteil eines gemäß Artikel 8 EGMR verfolgten legitimen Zieles sein. Zudem muss sie auch in einer demokratischen Gesellschaft notwendig sein. Wiederum anhand der vom EGMR festgelegten Prüfaspekte sollte die Maßnahme nicht nur dem Recht auf Privatsphäre, sondern auch dem Grundsatz der Verarbeitung von Daten nach Treu und Glauben und auf rechtmäßige Weise nachkommen.

5.6 Zweckbindung und Datenminimierung als Grundsätze

Obwohl es sich bei Zweckbindung und Datenminimierung um eigenständige Grundsätze handelt, stehen sie oft in Wechselbeziehung. Deshalb befasst sich die Datenschutzgruppe hier mit beiden. In der Richtlinie sind diese Grundsätze in Artikel 6 Absatz 1 Buchstabe b bzw. c niedergelegt, wonach vorzusehen ist, dass personenbezogene Daten

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.

5.7 Beim Grundsatz der Zweckbindung[32] geht es darum zu verstehen, **warum** bestimmte personengebundene Daten verarbeitet werden. Es ist also so genau wie möglich anzugeben, zu welchem Zweck bei einer geplanten Maßnahme personengebundene Daten erhoben und verarbeitet werden sollen. Im Zuge dessen sollte auch eine bessere Einhaltung des Grundsatzes der Datenminimierung erfolgen. Damit soll sichergestellt werden, dass für den angegebenen Zweck nur die minimal notwendige Menge an personengebundenen Daten verarbeitet wird. Diese Datenschutzgrundsätze stehen in engem Zusammenhang mit dem Begriff der Verhältnismäßigkeit im Rahmen des Schutzes der Privatsphäre. Aber auch hier wird die Einhaltung dieser Grundsätze zur Einhaltung des Erforderlichkeitsgebots insgesamt beitragen. Generalanwalt Poiares Maduro (2008) machte dies in seinen Schlussanträgen deutlich: *„Der Begriff der Erforderlichkeit … ist als Teil der Verhältnismäßigkeitsprüfung fest verankert. Er bedeutet, dass eine Behörde, die eine Maßnahme erlässt, die in ein durch das Gemeinschaftsrecht geschütztes Recht eingreift, um ein legitimes Ziel zu erreichen, nachweisen muss, dass die Maßnahme das zur Erreichung dieses Ziels am wenigsten einschneidende Mittel ist"*.[33]

5.8 In ihrer Stellungnahme zu dem von der Europäischen Kommission vorgeschlagenen Paket „intelligente Grenzkontrollsysteme" bekräftigte die Datenschutzgruppe ihr Argument, dass eine unzureichend festgelegte Zweckbin-

[32] Stellungnahme der Datenschutzgruppe zur Zweckbindung: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[33] Rechtssache C-524/06, Randnr. 27.

dung – verbunden mit dem fehlenden Nachweis, dass die geplante Maßnahme ein zwingendes gesellschaftliches Bedürfnis angehen würde – nicht datenschutzgerecht wäre. Insbesondere zum Einreise-/Ausreisesystem (EES), das die Verarbeitung der Daten von Millionen von Bürgern umfasst, stellte die Datenschutzgruppe fest: „[Mit dem EES] … *würden zwar Personen ermittelt, die die zulässige Aufenthaltsdauer überzogen haben (Overstayers), doch blieben damit die eigentlichen Ursachen unberührt, und für sich genommen hat das EES keine Möglichkeit, die Zahl der ‚Overstayers' zu senken, außer vielleicht, dass es als mildes Abschreckungsmittel wirkt.* "[34]

5.9 Ein weiteres Beispiel, bei dem diese Bedenken geäußert wurden, war die Richtlinie zur Vorratsdatenspeicherung. Die Datenschutzgruppe vertrat die Auffassung, dass die pauschale Speicherung der Daten sämtlicher Personen durch EU-Telekommunikationsanbieter für die Dauer von zwei Jahren, so dass RFSR-Behörden darauf zugreifen können, einen unverhältnismäßigen Eingriff in das Recht des Einzelnen auf Privatsphäre darstellt. Sie führte außerdem an, dass es der Richtlinie zur Vorratsdatenspeicherung an hinreichender Klarheit mangelt und sie den Grundsatz der Zweckbindung verletzen würde. Darüber hinaus schlug die Datenschutzgruppe alternative Maßnahmen mit größerer Verhältnismäßigkeit vor, wie z. B. „Quick-Freeze"-Verfahren, um die Ziele des Vorschlags mit weniger Eingriffen in die Privatsphäre zu erreichen, und gelangte zu dem Schluss, dass der Vorschlag Neubewertungs- und Auslaufklauseln enthalten sollte.[35]

5.10 Zwei weitere Beispiele für den Umgang mit Zweckbindung und Verhältnismäßigkeit bilden Fälle, die von Datenschutzbehörden auf nationaler Ebene behandelt wurden, und zwar von der maltesischen und von der italienischen Datenschutzbehörde. Beide Fälle machen deutlich, warum die obligatorische Angabe konkreter Gründe für die Verarbeitung personengebundener Daten so wichtig ist – vor allem, wenn die RFSR-Maßnahme die Verarbeitung der personengebundenen Daten von Nichtverdächtigen verlangt.

Die maltesische Polizei beantragte den pauschalen und direkten Zugriff auf Geolocation-Daten der Telekommunikation, um eine Serie von Brandanschlägen auf der Insel aufzuklären. Während die Datenschutzbehörde und anschließend das Gericht dem Zugriff zustimmten, entschied das Berufungsgericht in Malta, dass die Maßnahmen nicht verhältnismäßig waren. Das

[34] Stellungnahme 206 der Datenschutzgruppe zu intelligenten Grenzkontrollsystemen, 05/2013.

[35] Stellungnahme 64 der Datenschutzgruppe, 5/2002, zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.–11. September 2002) über die obligatorische systematische Vorratsspeicherung von Daten des Telekommunikationsverkehrs; und Stellungnahme 4/5 der Datenschutzgruppe zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endgültig vom 21.9.2005).

Gericht befand, dass das Datenersuchen zu vage und breit gefasst war und zur Verarbeitung der Daten unschuldiger Bürger geführt hätte. Daher wäre dies ein unverhältnismäßiger Eingriff in das Recht auf Privatleben gewesen. Der Antrag wurde für unrechtmäßig befunden, da er nicht hinreichend abgegrenzt und somit unverhältnismäßig und nicht erforderlich war.

5.11 In Italien schlug die Polizei mehrere Maßnahmen gegen Fußballrowdytum vor. Die italienische Datenschutzbehörde entschied, dass in Anbetracht wiederholter Ausschreitungen in Fußballstadien Italiens Überwachungskameras in all diesen Stadien zugelassen werden sollten. Im selben Fall gelangte die Behörde aber zu dem Schluss, dass nicht genügend Gründe und Beweise vorgelegt wurden, um einen individualisierten Eintrittskartenverkauf für Spiele einzuführen, durch den eine riesige Datenbank von Personen entstehen würde, die Fußballspiele besuchen. Die geplante Maßnahme sei für ein Vorgehen gegen die Ausschreitungen unverhältnismäßig. In einem ähnlich gelagerten Fall in der Tschechischen Republik wurden diese Maßnahmen dagegen als verhältnismäßig angesehen, da entsprechende Schutzvorkehrungen umgesetzt werden, um den Erfassungsbereich der individualisierten Kartenverkäufe zu begrenzen. Die tschechische Datenschutzbehörde stellte sicher, dass nur bestimmte Spiele, die (nachweislich) als besonders problematisch gelten, mit der Pflicht zum individualisierten Kartenverkauf belegt werden.

5.12 Aus dem Blickwinkel der Privatsphäre betrachtet ließe sich anführen, das die Datenschutzgruppe nicht von der Erforderlichkeit des Kommissionsvorschlags zu intelligenten Grenzkontrollsystemen überzeugt war, weil a) vorhandene Maßnahmen unzureichend berücksichtigt wurden und weil es sich b) insbesondere im Hinblick auf das EES um eine unverhältnismäßige Reaktion auf die dargelegten zwingenden gesellschaftlichen Bedürfnisse handelte, da auf diese nicht in angemessener Weise eingegangen wurde. Aus Datenschutzsicht bedeutete die unzureichende Abgrenzung der Zweckbestimmung des Vorschlags zu den intelligenten Grenzkontrollsystemen, dass die Verarbeitung der Daten weder dem Zweck entspricht noch erheblich ist, sondern über den Zweck hinausgeht und die Daten somit länger gespeichert bleiben als notwendig.

Um den vom EGMR zum Kriterium „in einer demokratischen Gesellschaft notwendig“ aufgestellten Prüfaspekt „Verhältnismäßigkeit“ zu erfüllen, muss eine Maßnahme eine verhältnismäßige Reaktion auf das dargelegte zwingende gesellschaftliche Bedürfnis sein, wobei sicherzustellen ist, dass ausreichende Beweise dafür vorgebracht werden. Aus Datenschutzsicht liegt jedoch der Fokus darauf, in welchem Umfang die Verarbeitung der personengebundenen Daten eines Einzelnen als Bestandteil der RFSR-Maßnah-

me erfolgen sollte. Damit beide Voraussetzungen erfüllt werden, sollten die Angaben so konkret wie möglich sein. Auf diese Weise wird jede Verarbeitung personengebundener Daten, die Bestandteil der Maßnahme ist, klar verständlich und abgegrenzt, und es wird das Risiko minimiert, dass mehr Daten als für den Zweck notwendig verarbeitet werden. Vorausgesetzt, die Maßnahme wird auch hinreichend begründet, dürfte die Einhaltung der Artikel 7 und 8 der Charta, von Artikel 8 EMRK, der Richtlinie 95/46/EG und des Rahmenbeschlusses über den Datenschutz erreicht sein.

5.13 Datenspeicherdauer

In der Richtlinie kommt der Datenschutzgrundsatz der Speicherung in Artikel 6 Absatz 1 Buchstabe e zum Ausdruck, wonach vorzusehen ist, dass personenbezogene Daten *„nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden“.*

Nahezu genauso wie der Grundsatz der Datenminimierung verlangt, dass nur die geringstmögliche Menge an Daten erhoben und verarbeitet wird, um den Zweck der Datenverarbeitung zu erreichen, sind die Daten nach dem Grundsatz der Datenspeicherdauer für die geringstmögliche Dauer zu speichern.

5.14 Aus der Rechtsprechung des EGMR geht eindeutig hervor, dass eine länger als notwendige Datenspeicherung nicht die drei Prüfaspekte zum Kriterium „in einer demokratischen Gesellschaft notwendig“ erfüllt (siehe S. Marper gegen Vereinigtes Königreich[36]). Die Speicherung personengebundener Daten ist nicht nur datenschutzrechtlich relevant, sondern stellt auch einen Eingriff in das Privatleben des Einzelnen dar.

5.15 Das Fehlen von ausreichenden und erheblichen Gründen, Unverhältnismäßigkeit und eine fehlende eindeutige Verbindung zu dem zwingenden gesellschaftlichen Bedürfnis der Speicherung personengebundener Daten – besonders von Personen, die nicht verdächtig sind – waren in den letzten Jahren immer wieder Gegenstand von Bedenkensäußerungen der Datenschutzgruppe und anderer. Das gilt besonders für Themenbereiche wie Fluggastdaten-

[36] S. und Michael Marper gegen Vereinigtes Königreich (Nr. 30562/04 und 30566/04).

sätze (Passenger Name Records, PNR)[37] und das Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP).

5.16 Die konkrete Frage der Neubewertung, wie lange die Datenspeicherung erforderlich ist, wurde im jährlichen Kontrollbericht 2012 von Europol aufgegriffen. Darin heißt es: *„Die Verarbeitung personengebundener Daten einer Gruppe von 96 nicht gewalttätigen Anarchisten, die nach Aussage des Zulieferers als nicht gefährlich eingestuft werden, entspricht nicht und entsprach niemals der Errichtungsanordnung. … Die Speicherung von Daten für 5 Jahre ohne jegliche Prüfung ihrer Relevanz und die Begründung der Weiterverarbeitung mit der Aufarbeitung eines Datenrückstaus stellt keine gültige Bewertung der Erforderlichkeit der Speicherung dieser Daten dar".* Daher ist es für die Wahrung des Rechts einer Person auf Privatleben und die Einhaltung des Datenschutzrechts von maßgeblicher Bedeutung, dass eine Befristung der Datenspeicherung von Anfang an in eine Maßnahme eingebaut wird und eine regelmäßige Neubewertung erfolgt.

5.17 In ähnlicher Weise entschieden die deutsche und die niederländische Datenschutzbehörde sowie entsprechende Gerichte, dass im Falle der automatischen Kennzeichenerfassung sicherzustellen ist, dass das Kennzeichen bei negativem Abgleichergebnis sofort gelöscht werden muss, damit die Maßnahme in einem hinreichenden Verhältnis zur Erzielung des ausgewiesenen Zwecks/zwingenden gesellschaftlichen Bedürfnisses steht.

5.18 Daher stehen die Grundsätze Datenminimierung und Datenspeicherdauer oft in Wechselbeziehung miteinander und im engen Zusammenhang mit dem Grundsatz der Zweckbindung. Aus Datenschutzsicht führt eine ungenaue Zweckbestimmung in der Regel zu einer Verletzung der Grundsätze der Datenminimierung und der Datenspeicherdauer. Aus dem Blickwinkel des Privatsphärenschutzes bedeutet die ungenaue Abgrenzung des Zwecks für die Verarbeitung personenbezogener Daten, dass das zwingende gesellschaftliche Bedürfnis unzureichend definiert ist. Damit könnte die RFSR-Behörde ihre Befugnisse in einer Weise ausüben, die in keinem angemessenen Verhältnis zu dem verfolgten berechtigten Ziel steht.

[37] Stellungnahme 7/2010 zur Mitteilung der Europäischen Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer – Stellungnahme 178 der Datenschutzgruppe, 2/2007, zur Unterrichtung von Fluggästen über die Übermittlung von PNR-Daten an Behörden der USA, angenommen am 15. Februar 2007, überprüft und aktualisiert am 24. Juni 2008; Gemeinsame Stellungnahme zu dem von der Kommission am 6. November 2007 vorgelegten Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken; Stellungnahme Nr. 5/2007 zu dem im Juli 2007 geschlossenen Folgeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security; Stellungnahme 2/2007 zur Unterrichtung von Fluggästen über die Übermittlung von PNR-Daten an Behörden der USA; Stellungnahme 8/2004 zur Unterrichtung von Fluggästen über die Übermittlung von PNR-Daten bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika.

TEIL VI

6.0 Lehren und praktische Empfehlungen

Aus den vorstehenden Ausführungen geht klar hervor, dass sowohl aus dem Schutz der Privatsphäre als auch aus dem Datenschutz Lehren gezogen werden müssen, damit eine RFSR-Maßnahme vorschriftsgemäß ist.

6.1 Der Ansatz des EGMR sollte nicht als einzige Möglichkeit zur Erfüllung aller Anforderungen, sondern als Richtschnur oder Prozess auf dem Weg dorthin angesehen werden. Nachfolgend eine Zusammenfassung dieses Prozesses und einige Punkte, die zu berücksichtigen sind, wenn RFSR-Maßnahmen vorgeschlagen, umgesetzt oder neubewertet werden.

Ist die geplante Maßnahme **gesetzlich vorgesehen**?

Die RFSR-Maßnahme muss eine gesetzliche Basis haben, damit sie umgesetzt oder eingeführt werden kann.

Verfolgt die Maßnahme ein **berechtigtes Ziel**?

Die Maßnahme muss eines der in Artikel 8 Absatz 2 EMRK aufgeführten Ziele verfolgen.

Ist die geplante Maßnahme **in einer demokratischen Gesellschaft notwendig**?

Zwingendes gesellschaftliches Bedürfnis

Ermitteln Sie das zwingende gesellschaftliche Bedürfnis (das konkrete Problem oder den konkreten Straftatbestand), auf den eingegangen werden muss.

Bestimmen Sie den Schweregrad des Problems sowie Nachweise für diese Auffassung. Betrachten Sie das Wesen des Straftatbestands, in dem ermittelt wird. Je nach Schwere der Straftat, ihrer Auswirkungen auf die Gesellschaft, dem Kontext, in dem sie begangen wird, usw. können Probleme eine unterschiedliche „Gewichtung" erhalten.

Zeit – Prüfen Sie, ob Maßnahmen ausgehend vom verstrichenen Zeitraum zwischen der Straftat und der Ergreifung der Maßnahme erforderlich und verhältnismäßig sind, z. B. wenn es sich um eine Straftat handelt, die der Täter als Kind begangen hat. Berücksichtigen Sie das Inkrafttreten des Gesetzes und der Maßnahmen im aktuellen Kontext. Überprüfen Sie zudem regelmäßig die Notwendigkeit und Verhältnismäßigkeit von Maßnahmen, um sicherzustellen, dass die Gründe für die Ergreifung der Maßnahmen zur Lösung eines bestimmten Problems noch stichhaltig sind.

Einstellungen, Kultur und Ermessensspielraum – Es ist klar, dass die Mitgliedstaaten bei RFSR-Maßnahmen über einen Ermessensspielraum verfügen. Dieser unterliegt jedoch stets der gerichtlichen Kontrolle. Unter dem Blickwinkel des Privatsphärenschutzes müssen stichhaltige und ausreichende Gründe zur Rechtfertigung einer Maßnahme und ihrer Verhältnismäßigkeit in Bezug auf das zwingende gesellschaftliche Bedürfnis angegeben werden, um sicherzustellen, dass der Ermessensspielraum richtig angewendet wird. Aus Datenschutzsicht besteht für die Berücksichtigung solcher kultureller Fragen eine gewisse Flexibilität. Beispielsweise stimmten die deutschen Behörden im Zusammenhang mit der Richtlinie über die Vorratsdatenspeicherung einer Speicherdauer von 3 Monaten anstatt von 2 Jahren wie in anderen Mitgliedstaaten zu.

Verhältnismäßigkeit

Setzen Sie eindeutige Ziele mit entsprechender Zweckbestimmung. Wenn das zu erreichende Ziel klar ist, lassen sich die Kategorien oder Arten der benötigten Daten, die Art der notwendigen Verarbeitung und die Qualität der benötigten Daten leichter festlegen.

Beispielsweise sollte mit einer richtigen Zweckbindung erreicht werden, dass so wenige Personen wie möglich von der Datenverarbeitung betroffen sind. Im RFSR-Kontext könnte es sich um die Zahl der einer Straftat verdächtigen Personen handeln. Es sollte also eine klare Unterscheidung zwischen einzelnen Kategorien von Betroffenen vorgenommen werden, und gegebenenfalls sollte die Art der zu verarbeitenden Daten für bestimmte Personen fallweise festgelegt werden. Ein weiteres Beispiel wäre die Aufbewahrung von DNA-Proben. Dazu bedarf es konkreter Vorstellungen von der entsprechenden Straftat und vom Nutzen, den die Verarbeitung von DNA-Daten bei der Aufklärung dieser Straftat spielen kann. Jede Stufe des Prozesses der Erhebung, Verarbeitung und Speicherung der DNA-Daten ist zu berücksichtigen, damit jedes Element der Datenverarbeitung vollständig gerechtfertigt ist. Mit einem derartigen Ansatz bei der Zweckbindung können die Vorschriften für Privatsphären- und Datenschutz besser eingehalten werden.

Allerdings werden nicht alle personengebundenen Daten, auf die eine Behörde Zugriff benötigt, von ihr verarbeitet. Sie braucht vielleicht auch Zugang zu Daten, die ursprünglich von anderen Stellen zu ganz anderen Zwecken erfasst wurden. Wie bei der neuen Eurodac-Verordnung kommt es im Zusammenhang mit der Erforderlichkeit und Verhältnismäßigkeit in diesen Fällen darauf an, dass Schutzvorkehrungen zur Begrenzung des Zugriffs vorhanden sind.

Überprüfen Sie vorhandene Maßnahmen und Alternativen. Bei der Planung einer Maßnahme kommt es darauf an, zunächst die Maßnahmen zu prüfen, die bereits zur Bewältigung des Problems vorhanden sind. Eine unzureichende Umsetzung und Prüfung bereits bestehender Mechanismen und ihre mangelhafte Gegenüberstellung mit einer neu vorgeschlagenen Maßnahme kann dazu führen, dass nicht genug Gründe und Beweise dafür vorliegen, dass die geplante Maßnahme tatsächlich die notwendige und verhältnismäßige Antwort auf ein zwingendes gesellschaftliches Bedürfnis darstellt. Ebenso wichtig sind derartige Überlegungen im Zusammenhang mit der Erweiterung des Zugriffs auf personengebundene Daten durch RFSR-Behörden bei Initiativen und Projekten wie PNR-Daten-Abkommen, Gesetzen zur Verkehrsüberwachung, Standortdaten sowie Vorschriften über den Zugang zu Finanztransaktionen.

Stehen Maßnahmen zur Verfügung, die einen geringeren Eingriff in die Privatsphäre darstellen, aber ebenso wirksam sind (unter Berücksichtigung angemessener Kosten), dann gelten nur diese Maßnahmen als erforderlich.

Stellen Sie sicher, dass Daten den Zwecken entsprechen, für die sie erhoben werden, dafür erheblich sind und nicht darüber hinausgehen. Ein riesiges Reservoir von Daten, auf die jederzeit direkt zugegriffen werden kann, ist verständlicherweise etwas, das aus Sicht einer RFSR-Behörde stets nützlich und mehrwertbehaftet ist. Gleichermaßen Rechnung zu tragen ist jedoch dem Recht des Einzelnen auf ein Privatleben und dem Recht, dass seine Daten nicht ohne gegebenen Anlass verarbeitet werden. Daher ist ein ausgewogenes Verhältnis zu finden.

Jede geplante Maßnahme ist gesondert zu prüfen, um ihre Auswirkungen zu beurteilen. Eine pauschale Anwendung einer geplanten Maßnahme dürfte schwerlich die Voraussetzung der Erforderlichkeit und Verhältnismäßigkeit erfüllen.

Legen Sie fest, wie lange die Daten aufbewahrt werden – Die Festlegung der Aufbewahrungsdauer von Daten in einem RFSR-Kontext ist schwierig, da die Sorge besteht, dass eine Löschung zum Verlust nützlicher Daten bei künftigen Ermittlungen führt. Aber ebenso wie bei der Erfassung der einzelnen Arten von Daten muss auch jede einzelne geplante Maßnahme gesondert überprüft werden, um ihre Auswirkung zu beurteilen. Eine pauschale Aufbewahrungsregelung für geplante Maßnahmen dürfte schwerlich die Voraussetzung der Erforderlichkeit und Verhältnismäßigkeit erfüllen.

Die Aufbewahrungsdauer sollte sorgsam zu den ursprünglichen Zwecken in Beziehung gebracht werden, zu denen die Datenerhebung erfolgte. Dabei

ist die Person zu betrachten, von der die Daten erhoben wurden, sowie der Grund dafür. Beispielsweise kann die Aufbewahrungsdauer der Daten von Nichtverdächtigten viel kürzer sein als bei Verdächtigten oder Personen, die auf andere Weise in die Straftat verwickelt sind.

Anwendung eines ganzheitlichen Ansatzes. Vor allem nach dem 11. September haben die europäischen Gesetzgeber immer neue Maßnahmen erlassen, die das Recht auf Schutz der Privatsphäre und das Recht auf Datenschutz im RFSR einschränken. Diese Entwicklung macht es besonders wichtig, bei der Beurteilung des Eingriffs eines neuen Gesetzesvorschlags in die Privatsphäre und den Datenschutz eine ganzheitliche Betrachtungsweise anzuwenden. Um sagen zu können, ob ein neuer Gesetzesvorschlag noch verhältnismäßig ist, muss bewertet werden, wie die neue Maßnahme bestehende Maßnahmen ergänzt und ob die Einschränkung der Grundrechte auf Datenschutz und Privatsphäre durch alle zusammengenommen noch im richtigen Verhältnis steht.

Stichhaltige und ausreichende Gründe

Evidenzbasierte Vorschläge. Ein Großteil der in den letzten Jahren geäußerten Kritik der Datenschutzgruppe an geplanten Maßnahmen zur Lösung von RFSR-Problemen bezog sich auf die unzureichenden Gründe und Beweise, die vorgelegt wurden, um nachzuweisen, dass die geplante Maßnahme die einzige verhältnismäßige Maßnahme ist, mit der auf das ermittelte zwingende gesellschaftliche Bedürfnis reagiert werden kann. Eine schlüssige Begründung der geplanten Maßnahmen muss bei Bedarf einer gründlichen Prüfung standhalten. Daher müssen geplante Maßnahmen auf evidenzbasierten Recherchen, Statistiken, Prognosen usw. beruhen. All dies wird dazu beitragen, dass der Prüfaspekt „stichhaltige und ausreichende Gründe“ erfüllt wird.

TEIL VII

7.0 Fazit

Als Schlussfolgerung empfiehlt die Datenschutzgruppe die vorstehend dargelegte Vorgehensweise, wenn RFSR-Maßnahmen vorgeschlagen, umgesetzt oder überprüft werden, die einen Eingriff in die Privatsphäre darstellen und bei denen personenbezogene Daten verarbeitet werden. Die in dieser Stellungnahme empfohlenen Überlegungen sollten als Möglichkeiten zur

Einhaltung der Vorschriften betrachtet werden und als Schutzvorkehrungen dienen, damit künftige geplante RFSR-Maßnahmen wirklich notwendig und verhältnismäßig sowie umfassend datenschutzgerecht sind.

Brüssel, 27. Februar 2014

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken (WP 215)

Angenommen am 10. April 2014

Zusammenfassung

Seit dem Sommer 2013 wird in verschiedenen internationalen Medien in großem Maßstab vor allem basierend auf von Edward Snowden bereitgestellten Dokumenten über die Überwachungstätigkeiten von Nachrichtendiensten in den USA und in der Europäischen Union berichtet. Die Enthüllungen haben eine weltweite Debatte über die Auswirkungen einer solch flächendeckenden Überwachung auf die Privatsphäre der Bürger entfacht. Die Art und Weise, in der sich Nachrichtendienste unserer täglichen Kommunikationsdaten sowie der Inhalte dieser Kommunikation bedienen, führt eindringlich vor Augen, dass der Überwachung Grenzen gesetzt werden müssen.

Das Recht auf Privatsphäre und auf Schutz der personenbezogenen Daten ist ein Grundrecht, das im Internationalen Pakt über bürgerliche und politische Rechte, in der Europäischen Menschenrechtskonvention und in der Charta der Grundrechte der Europäischen Union verankert ist. Die Einhaltung des Rechtsstaatsprinzips setzt deshalb zwingend voraus, dass dieses Recht in höchstmöglichem Maße geschützt wird.

Anhand ihrer Analyse kommt die Datenschutzgruppe zu dem Schluss, dass geheime, massive und willkürliche Überwachungsprogramme mit unseren grundlegenden Gesetzen unvereinbar sind und nicht mit der Bekämpfung des Terrorismus oder anderen größeren Bedrohungen der nationalen Sicherheit gerechtfertigt werden können. Die Beschränkung der Grundrechte aller Bürger ist nur hinnehmbar, wenn diese Maßnahme in einer demokratischen Gesellschaft unbedingt notwendig und verhältnismäßig ist.

Die Datenschutzgruppe empfiehlt daher verschiedene Maßnahmen zur Gewährleistung und Einhaltung der Rechtsstaatlichkeit.

Erstens fordert die Datenschutzgruppe mehr Transparenz in Bezug auf die Funktionsweise der Überwachungsprogramme. Transparenz trägt zur Wiederherstellung und Verbesserung des Vertrauensverhältnisses zwischen den Bürgern, Regierungen und privaten Einrichtungen bei. Dazu gehört, dass Einzelpersonen darüber in Kenntnis gesetzt werden, wenn Nachrichtendiensten Zugang zu Daten gewährt

wurde. Um die Bürger besser über die Auswirkungen der Nutzung elektronischer Online- und Offline-Kommunikationsdienste und die Möglichkeiten, sich selbst besser zu schützen, zu informieren, möchte die Datenschutzgruppe im zweiten Halbjahr 2014 eine Konferenz zum Thema Überwachung mit allen relevanten Akteuren abhalten.

Darüber hinaus spricht sich die Datenschutzgruppe nachdrücklich für eine wirksamere Beaufsichtigung der Überwachungstätigkeiten aus. Da die wirksame und unabhängige Aufsicht über die Nachrichtendienste, einschließlich der Verarbeitung personenbezogener Daten, eine Voraussetzung ist, um den Missbrauch dieser Programme zu verhindern, vertritt die Datenschutzgruppe die Ansicht, dass die Datenschutzbehörden unbedingt darin einbezogen werden müssen.

Des Weiteren empfiehlt die Datenschutzgruppe die Durchsetzung der bestehenden Verpflichtungen der EU-Mitgliedstaaten und der Vertragsparteien der Europäischen Menschenrechtskonvention (EMRK) zum Schutz des Rechts auf Achtung der Privatsphäre und der personenbezogenen Daten. Ferner erinnert die Datenschutzgruppe daran, dass den EU-Rechtsvorschriften unterliegende Datenverarbeiter die anwendbaren EU-Datenschutzvorschriften einhalten müssen. Sie verweist zudem darauf, dass Datenschutzbehörden die Datenübermittlung aussetzen können und gegebenenfalls entsprechend ihrer einzelstaatlichen Zuständigkeit Sanktionen verhängen sollten.

Weder die Grundsätze des „sicheren Hafens“ noch Standardvertragsklauseln oder unternehmensinterne Datenschutzregelungen können als Rechtsgrundlage herangezogen werden, um die Übermittlung personenbezogener Daten an eine Drittstaatsbehörde zum Zwecke massiver und willkürlicher Überwachung zu rechtfertigen. Die in diesen Instrumenten enthaltenen Ausnahmeregelungen haben nämlich einen beschränkten Anwendungsbereich und sollten eng ausgelegt werden. Unter keinen Umständen sollten sie so umgesetzt werden, dass das durch die EU-Vorschriften und -Instrumente für die Datenübermittlung garantierte Schutzniveau beeinträchtigt wird.

Die Datenschutzgruppe fordert die EU-Organe auf, die Verhandlungen über das Datenschutz-Reformpaket zum Abschluss zu bringen. Sie begrüßt insbesondere den Vorschlag des Europäischen Parlaments für einen neuen Artikel 43a, der die Verpflichtung auferlegt, Personen zu informieren, wenn einer Behörde innerhalb der letzten zwölf Monate Zugriff auf Daten gewährt wurde. Durch Transparenz bei diesen Vorgehensweisen wird das Vertrauen enorm gestärkt.

Darüber hinaus ist die Datenschutzgruppe der Ansicht, dass der Anwendungsbereich der Ausnahmen aus Gründen der nationalen Sicherheit präzisiert werden sollte, um Rechtssicherheit hinsichtlich des Geltungsbereichs des EU-Rechts zu schaffen. Bislang hat der europäische Gesetzgeber weder eine klare Definition

des Begriffs „nationale Sicherheit“ vorgenommen, noch gibt es diesbezüglich eine schlüssige Rechtsprechung der europäischen Gerichte.

Abschließend empfiehlt die Datenschutzgruppe die unverzügliche Einleitung von Verhandlungen über ein internationales Abkommen, um Personen bei der Durchführung nachrichtendienstlicher Tätigkeiten angemessene Datenschutzgarantien zu gewähren. Die Datenschutzgruppe unterstützt zudem die Entwicklung eines weltweiten Instruments, das durchsetzbare hohe Grundsätze für den Schutz der Privatsphäre und den Datenschutz vorschreibt.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGNER 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 c und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung und insbesondere Artikel 12 und 14,

HAT DIESE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

Seit dem Sommer 2013 wird in verschiedenen internationalen Medien viel über die elektronischen Überwachungstätigkeiten von Nachrichtendiensten in den USA, in der Europäischen Union (EU) und in der übrigen Welt berichtet, wobei diese Berichte in erster Linie auf den von Edward Snowden zur Verfügung gestellten Dokumenten basieren. Die Enthüllungen haben eine weltweite Debatte über die Auswirkungen einer solch flächendeckenden elektronischen Überwachung auf die Privatsphäre der Bürger entfacht. So wurde auch die Frage aufgeworfen, inwieweit es Nachrichtendiensten gesetzlich erlaubt sein sollte, unseren Alltag betreffende Informationen zu sammeln und zu verwenden. Diese Stellungnahme enthält die Ergebnisse der Rechtsanalyse durch die Datenschutzbehörden in der EU, die in der Artikel-29-Datenschutzgruppe (die Datenschutzgruppe) vereint sind, in Bezug auf die Auswirkungen elektronischer Überwachungsprogramme auf den Schutz des Grundrechts auf Datenschutz und Schutz der Privatsphäre.

Die Hauptaufgabe von Datenschutzbehörden besteht darin, das Grundrecht jedes Einzelnen auf Datenschutz zu schützen und sicherzustellen, dass die entsprechenden gesetzlichen Vorgaben von den Datenverarbeitern eingehalten werden. Allerdings haben viele Datenschutzbehörden nur begrenzte oder sogar gar keine Aufsichtsbefugnisse über Nachrichtendienste. Für deren Beaufsichtigung, einschließlich der Verarbeitung personenbezogener Daten, haben die Mitgliedstaaten andere Regelungen getroffen. Die Datenschutzgruppe hat daher eine Bestandsaufnahme der in der EU für die Überwachung der Nachrichtendienste vorhandenen verschiedenen Regelungen vorgenommen, die Bestandteil dieser Stellungnahme ist.

Nicht berücksichtigt ist in dieser Stellungnahme das kabelgebundene Abfangen personenbezogener Daten. Der Datenschutzgruppe liegen zum gegenwärtigen Zeitpunkt nicht genügend Informationen zu diesen Behauptungen vor, um die anwendbare Rechtsgrundlage – und sei es auch nur hypothetisch – bewerten zu können.

2. Metadaten

Um das Ausmaß der mutmaßlichen Verletzung von Datenschutzvorschriften beurteilen zu können, muss zunächst abgeklärt werden, worum es eigentlich geht. Regierungsvertreter sprechen oftmals von der Sammlung von Metadaten und implizieren damit, dass diese weniger bedenklich ist als die Sammlung von Inhalten. Diese Annahme ist jedoch falsch. Unter Metadaten fallen sämtliche Daten einer stattfindenden Kommunikation, ausgenommen der Inhalt der Konversation. Dazu zählen beispielsweise die Telefonnummer bzw. die IP-Adresse der anrufenden oder eine E-Mail versendenden Person, Informationen zum Zeitpunkt, Ort, Thema, Empfänger usw. Die Analyse kann sensible Daten von Personen zu Tage bringen, weil z. B. Auskunftsnummern medizinischer oder religiöser Zentren angewählt wurden. Wie der Europäische Gerichtshof für Menschenrechte bereits im Fall Malone[1] festgestellt hat, ist die Verarbeitung von Metadaten, wobei es in diesem Fall um die Registrierung von Kommunikationsverbindungsdaten („metering“) ging, ein integraler Bestandteil der Telefonkommunikation. Daher komme die Weitergabe dieser Informationen an die Polizei ohne die Einwilligung des Telefonteilnehmers einer Verletzung eines durch Artikel 8 gewährleisteten Rechts gleich. Der Gerichtshof hat seitdem an dieser Auffassung festgehalten.

Festzustellen ist auch, dass Metadaten oftmals leichter Informationen preisgeben als der eigentliche Inhalt der Kommunikation.[2] Aufgrund ihrer Strukturiertheit

[1] Urteil des EGMR vom 2. August 1984, Malone/Vereinigtes Königreich.

[2] ACLU/Clapper, Fall Nr. 13-3994 (WHP) – Schriftliche Erklärung von Prof. Edward W. Felten vor dem US-Bezirksgericht des Southern District New York.

lassen sie sich mühelos sammeln und analysieren. Moderne Computerprogramme gestatten die Analyse großer Datensätze und die Identifizierung darin enthaltener Muster und Beziehungen, einschließlich privater Details, Gewohnheiten und Verhaltensweisen. Die eigentlichen Gespräche sind nicht gleichermaßen analysierbar, da sie in beliebiger Form und Sprache geführt werden.

Gemäß Artikel 2 Buchstabe a der Richtlinie 95/46/EG 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". Eine ähnliche Begriffsbestimmung erfolgt in Artikel 2 Buchstabe a der Konvention Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Daher werden Metadaten in Europa im Gegensatz zu anderen Ländern als personenbezogene Daten betrachtet und sind zu schützen.[3]

In einem kürzlich ergangenen Urteil zur Vorratsdatenspeicherung bestätigte der Gerichtshof der Europäischen Union, dass „aus der Gesamtheit dieser [Telekommunikations-]Daten […] sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden [können]".[4] Und schließlich befand der Gerichtshof im selben Urteil, dass „die Pflicht, […] Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Art. 7 der Charta garantierten Rechte darstellt. Zudem stellt der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht dar. […] Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen […] das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist."[5]

3. Hauptpunkte

Die Enthüllungen von Edward Snowden stellten für viele einen heftigen Weckruf dar. Erstmals wurde offenbar, wie viele verschiedene Überwachungsprogramme die Nachrichtendienste zu laufen haben, mit denen Daten über praktisch jeden

[3] Es handelt sich dabei um eine seit langem bestehende Auslegung des Datenschutzrechts. In ihrer Stellungnahme 4/2007 zum Begriff „personenbezogener Daten" hat die Datenschutzgruppe bereits festgestellt, dass „auch wenn der Umfang der vorhandenen Kennzeichen auf Anhieb keinen Rückschluss auf eine bestimmte Person erlaubt, […] diese Person dennoch „bestimmbar" sein [könnte], weil diese Information in Verbindung mit anderen Informationen (unabhängig davon, ob diese vom für die Verarbeitung Verantwortlichen gespeichert werden oder nicht) eine Unterscheidung dieser Person von anderen Personen ermöglicht".

[4] Siehe Urteil des EuGH vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12, Randnr. 27.

[5] Siehe Urteil des EuGH vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12, Randnrn. 34, 35 und 37.

gesammelt werden können. Einzelfälle sind bereits früher bekannt geworden, doch nun liegen erstmals umfassende Belege für die allgemeine Durchdringung auf dem Tisch. Die Art und Weise, in der Nachrichtendienste die Daten unserer täglichen Kommunikation wie auch deren Inhalt nutzen, verdeutlicht, dass der Überwachung Grenzen gesetzt werden müssen.

Selbst jene, die ihr Online-Leben mit Bedacht führen, können sich gegenwärtig nicht vor massiven Überwachungsprogrammen schützen. Und angesichts der vielen rechtlichen, technischen und praktischen Herausforderungen können Datenschutzbehörden in aller Welt auch keinen zufriedenstellenden Schutz bieten. Es muss daher ein Wandel vollzogen werden.

In den folgenden Kapiteln analysiert die Artikel-29-Datenschutzgruppe die massive Datensammlung durch Nachrichtendienste im Lichte ihrer Überwachungsprogramme. Aus rechtlicher Sicht ist zwischen Überwachungsprogrammen von Nachrichtendiensten der Mitgliedstaaten und Überwachungsprogrammen der Nachrichtendienste von Drittländern, die Daten von EU-Bürgern verwenden, zu unterscheiden.

Von EU-Mitgliedstaaten durchgeführte Überwachungsprogramme unterliegen entsprechend den in die EU-Verträge aufgenommenen Ausnahmeregelungen aus Gründen der nationalen Sicherheit und den – nach diesem Beschluss der vertragschließenden Mitgliedstaaten – erlassenen EU-Verordnungen und -Richtlinien, einschließlich der EU-Datenschutzrichtlinie 95/46/EG, generell nicht den EU-Rechtsvorschriften. Das heißt allerdings nicht, dass solche Programme nur dem einzelstaatlichen Recht unterworfen sind. Die Analyse durch die Artikel-29-Datenschutzgruppe zeigt, dass auch wenn das EU-Recht im Allgemeinen und die Datenschutzrichtlinie im Besonderen nicht anwendbar sind, aus der Europäischen Menschenrechtskonvention und der Konvention Nr. 108 des Europarates zum Schutz personenbezogener Daten folgt, dass die Grundsätze des Datenschutzes[6] von den Nachrichtendiensten bei der rechtmäßigen Wahrnehmung ihrer Aufgaben gleichwohl zum Großteil einzuhalten sind. Diese Grundsätze sind in vielen Mitgliedstaaten Bestandteil der jeweiligen nationalen Verfassung. Überwachungsprogramme, die auf der unterschiedslosen und flächendeckenden Sammlung personenbezogener Daten basieren, können keinesfalls den in diesen Datenschutzgrundsätzen niedergelegten Anforderungen an die Erforderlichkeit und die Verhältnismäßigkeit genügen. Beschränkungen der Grundrechte sind der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR)[7]

[6] Zu den wichtigsten Datenschutzgrundsätzen gehören eine rechtmäßige Verarbeitung nach Treu und Glauben, Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit, sachliche Richtigkeit, Transparenz, Wahrung der Rechte des Einzelnen und angemessene Datensicherheit.

[7] Siehe Urteile des EGMR vom 17. Januar 1970 (Delcourt) und vom 6. September 1978 (Klass).

und des Gerichtshofs der Europäischen Union (EuGH)[8] zufolge eng auszulegen. Dazu gehört, dass alle Eingriffe im Hinblick auf das verfolgte Ziel erforderlich und verhältnismäßig sein müssen. Außerdem ist zu beachten, dass nicht automatisch davon auszugehen ist, dass das von einer nationalen Behörde vorgebrachte Argument der nationalen Sicherheit tatsächlich zutrifft und berechtigt ist. Dies muss erst nachgewiesen werden.

Die Datenschutzgruppe bekräftigt, dass es Sache der Regierungen der Mitgliedstaaten ist, sämtlichen nationalen und internationalen Verpflichtungen einschließlich dem Internationalen Pakt über bürgerliche und politische Rechte nachzukommen, denn andernfalls würden nicht nur die Grundrechte ihrer Bürger verletzt, sondern auch das Vertrauen der Gesellschaft in die Rechtsstaatlichkeit beschädigt.

Bei Überwachungsprogrammen, die von Drittstaaten durchgeführt werden, ist die Sachlage komplizierter. Werden Daten entweder direkt aus einer Quelle in der EU oder nach der Übermittlung in den jeweiligen Drittstaat (oder auch einen weiteren Drittstaat) erfasst, können die im Zuge der Überwachungsprogramme offengelegten Informationen weiterhin unter das EU-Recht fallen. Die bereits genannte Ausnahme aus Gründen der nationalen Sicherheit gilt nämlich nur für die nationale Sicherheit eines EU-Mitgliedstaats und nicht für die eines Drittstaats. Natürlich kann es zu Situationen kommen, in denen sich die nationalen Sicherheitsinteressen eines Drittstaats mit denen eines Mitgliedstaats überschneiden und gemeinsame Überwachungsmaßnahmen berechtigt sind. Auch dann müssen die an der Überwachung beteiligten Behörden nachweisen können, warum und inwiefern sich die nationalen Sicherheitsinteressen überschneiden und damit die Anwendung des EU-Rechts ausschließen.

Alle in der Richtlinie 95/46/EG aufgeführten Anforderungen an die internationale Übermittlung personenbezogener Daten müssen beachtet werden: Dies bedeutet vor allem, dass der Empfänger ein angemessenes Schutzniveau gewährleistet und die Übermittlungen mit dem ursprünglichen Zweck, aus dem die Daten erfasst wurden, in Einklang stehen. Die Übermittlungen müssen auch das Erfordernis einer angemessenen Rechtsgrundlage für eine rechtmäßige Verarbeitung nach Treu und Glauben erfüllen.

Keines der verfügbaren Instrumente, das als alternative Grundlage für die Übermittlung personenbezogener Daten an unsichere Staaten genutzt werden kann (Grundsätze des „sicheren Hafens", Standardvertragsklauseln und unternehmensinterne Datenschutzregelungen), erlauben Drittstaatsbehörden den Zugang

[8] Siehe Urteil des EuGH vom 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12, in dem der Gerichtshof feststellte, dass die Vorratsdatenspeicherung von Verkehrsdaten „ohne irgendeine Differenzierung, Einschränkung oder Ausnahme" […] „einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie (Richtlinie 2006/24, Anm. d. Ü.) Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt" (Randnrn. 57 und 65).

zu den auf ihrer Grundlage übermittelten personenbezogenen Daten zum Zwecke der massiven und willkürlichen Überwachung. Die in diesen Instrumenten enthaltenen Ausnahmeregelungen haben nämlich einen beschränkten Anwendungsbereich und sollten eng ausgelegt werden (d. h. sie sind nur in Sonderfällen und bei einzelnen Ermittlungen anwendbar). Da die Instrumente zur Sicherstellung der Angemessenheit insbesondere dem Schutz der aus der EU stammenden personenbezogenen Daten dienen sollen, sollten sie unter keinen Umständen so umgesetzt werden, dass das durch die EU-Vorschriften und -Instrumente für die Datenübermittlung garantierte Schutzniveau beeinträchtigt wird. Die Datenschutzgruppe betont außerdem, dass sich gemäß der Datenschutzrichtlinie die Bewertung des Datenschutzniveaus in Drittstaaten derzeit im Allgemeinen nicht auf die Verarbeitung von Daten für Strafverfolgungs- oder Überwachungszwecke erstreckt.

Unternehmen sollte zudem bewusst sein, dass sie gegen EU-Recht verstoßen könnten, wenn Nachrichtendienste von Drittstaaten Zugang zu den auf ihren Servern gespeicherten Daten von EU-Bürgern erlangen, oder sie einer Anweisung folgen, in großem Maßstab personenbezogene Daten herauszugeben. Diesbezüglich könnten Unternehmen bei der Entscheidung, ob sie einer Anweisung zur Herausgabe personenbezogener Daten in großem Maßstab nachkommen oder nicht, in eine Zwickmühle geraten: Entweder sie verstoßen gegen EU-Recht oder das Recht des jeweiligen Drittstaats. Strafverfolgungsmaßnahmen gegen diese Unternehmen sollten insbesondere in Fällen nicht ausgeschlossen werden, in denen für die Datenverarbeitung Verantwortliche willentlich und wissentlich mit Nachrichtendiensten zusammengearbeitet und ihnen Zugang zu ihren Daten verschafft haben. Unternehmen müssen für ein möglichst hohes Maß an Transparenz sorgen und sicherstellen, dass sich Betroffene im Klaren darüber sind, dass, sobald ihre personenbezogenen Daten auf der Grundlage der für diese Übermittlungen verfügbaren Instrumente an unsichere Drittstaaten übermittelt wurden, sie von Drittstaatsbehörden überwacht werden können oder diese Zugangsrechte haben können, sofern derartige Ausnahmen in den genannten Instrumenten vorgesehen sind. Am wichtigsten ist es allerdings, eine wirksame Lösung auf politischer Ebene zu finden. Durch ein Schutzbestimmungen enthaltendes internationales Abkommen könnte sichergestellt werden, dass Nachrichtendienste die Grundrechte achten.

Damit die Nachrichtendienste die Beschränkungen für Überwachungsprogramme auch tatsächlich einhalten, sind wirksame Aufsichtsmechanismen in den Gesetzen aller Mitgliedstaaten vorzusehen. Dazu sollten gänzlich unabhängige Kontrollen der Datenverarbeitungsvorgänge durch eine unabhängige Stelle sowie wirksame Durchsetzungsbefugnisse gehören. Neben einer stärkeren und effektiven parlamentarischen Kontrolle könnten diese Aufgaben je nach den von dem jeweiligen Mitgliedstaat erlassenen Aufsichtsregeln von einer Datenschutzbehörde oder einem anderen geeigneten unabhängigen Gremium wahrgenommen werden. Sollte die Aufsicht durch ein anderes Gremium erfolgen, empfiehlt die

Datenschutzgruppe regelmäßige Kontakte zwischen diesem Gremium und der nationalen Datenschutzbehörde, um eine kohärente und einheitliche Anwendung der Datenschutzgrundsätze sicherzustellen.

Es sei darauf hingewiesen, dass Aufsichtsmechanismen nicht nur auf dem Papier bestehen dürfen, sondern konsequent anzuwenden sind. Die Enthüllungen von Edward Snowden haben gezeigt, dass es auf dem Papier zwar viele Kontrollmechanismen gibt, darunter eine gerichtliche Kontrolle geplanter Datenerhebungsprogramme, die wirksame Umsetzung der Schutzmaßnahmen jedoch zu wünschen übrig lässt. Werden die Schutzmaßnahmen gegen den unberechtigten Zugriff weder auf alle Überwachungsprogramme noch auf alle Personen angewendet, gewährleisten sie nicht die von der Datenschutzgruppe angestrebte umfassende Aufsicht.

4. Aufsicht über Nachrichtendienste

Während die Aufsichtsmodalitäten für die Sicherheits- und Nachrichtendienste von Drittstaaten in den letzten Jahren eingehend von Sachverständigen verschiedener Einrichtungen untersucht wurden, standen die nationalen Nachrichtendienste der einzelnen EU-Mitgliedstaaten weniger im Fokus eingehenderer Analysen. Um ein klareres Bild von den verschiedenen Modalitäten für die Aufsicht über nationale Nachrichtendienste in Europa zu gewinnen, hat die Datenschutzgruppe allen Datenschutzbehörden (darunter zwei Nicht-EU-Beobachtern) einen Fragebogen zugesandt, um Auskünfte über ihre diesbezügliche nationale Vorgehensweise einzuholen.[9]

Zwei Aspekte sollen eingehender beleuchtet werden:

1. das Vorhandensein eines gesetzlichen Rahmens für eine umfassende Aufsicht über nationale Sicherheits- und Nachrichtendienste;

2. die Funktion (oder die fehlende Funktion) der nationalen Datenschutzaufsichtsbehörde innerhalb dieses gesetzlichen Rahmens.

Die Datenschutzgruppe kommt damit auch der Aufforderung der Vizepräsidentin der Europäischen Kommission, Viviane Reding, nach, die künftige Funktion der Datenschutzbehörden zu prüfen.[10]

[9] Antworten auf den Fragebogen gingen von 27 nationalen Datenschutzbehörden der EU, der subnationalen Datenschutzbehörde Sachsens (Deutschland) und den Nicht-EU-Datenschutzbehörden der Schweiz und Serbiens ein.

[10] Schreiben von Vizepräsidentin Reding an den Vorsitzenden der Artikel-29-Datenschutzgruppe vom 30. August 2013.

4.1. Überblick über die einschlägigen nationalen Aufsichtsmechanismen

Die Überwachungstätigkeiten, um die es in dieser Stellungnahme und dem beigefügten Arbeitsdokument geht, werden überwiegend von Nachrichtendiensten im Rahmen der ihnen übertragenen Aufgaben zum Schutz der nationalen Sicherheit ausgeführt. Entsprechend den jeweiligen einzelstaatlichen Rechtstraditionen und -strukturen für nationale Sicherheitsmodalitäten gibt es ein breites Spektrum von Aufsichtssystemen. In 26 der 27 Mitgliedstaaten, die den Fragebogen beantworteten [11], bestehen und agieren die Nachrichtendienste auf der Grundlage von Gesetzen, in denen ihre Befugnisse, Struktur und Zuständigkeiten niedergelegt sind. In einem Mitgliedstaat, in dem es keine Nachrichtendienste gibt, werden die Sicherheitsaufgaben des Staats von der nationalen Polizei wahrgenommen.[12]

In der Mehrheit der Länder, die den Fragebogen beantwortet haben, gibt es ein bis drei Sicherheits- und Nachrichtendienste auf nationaler Ebene. Im Allgemeinen erfolgt eine Trennung der Aufgaben nach interner und externer (ausländischer) Bedrohung der nationalen Sicherheit, was auch zu getrennten Zuständigkeiten, nämlich der zivilen (Innen- oder Justizministerium) und der militärischen (Verteidigungsministerium) führt. In drei Mitgliedstaaten sind die verschiedenen Strukturen zu einem Schutzsystem verbunden, das direkt dem Regierungschef (z. B. dem Premierminister) untersteht.

Der Verarbeitung personenbezogener Daten liegt jeweils ein einzelstaatliches Gesetz zugrunde, und die Aufsicht basiert entweder auf einem allgemeinen Datenschutzgesetz oder auf einem oder mehreren gesonderten Gesetzen für die Verarbeitung personenbezogener Daten durch einen oder mehrere Nachrichtendienste.

4.2. Die Funktion der nationalen Datenschutzaufsichtsbehörde

Die Analyse der einschlägigen nationalen Rechtsvorschriften zeigt, dass das allgemeine Datenschutzgesetz in vielen Ländern nicht für die nachrichtendienstlichen Tätigkeiten gilt und die Datenschutzbehörde eine begrenzte bzw. in einigen Fällen sogar gar keine Aufsichtsfunktion hat. Häufig sind spezifische Datenschutzregeln im Gesetz vorgesehen, doch diese sehen nicht zwangsläufig die Aufsicht durch die Datenschutzbehörde vor.

In den beiden Nicht-EU-Mitgliedstaaten, die den Fragebogen freundlicherweise ebenfalls beantworteten[13], ist die Verarbeitung personenbezogener Daten durch

[11] Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern.

[12] Irland.

[13] Serbien (ein ziviler und zwei militärische Dienste), Schweiz (ein ziviler und ein militärischer Dienst).

die Nachrichtendienste im allgemeinen Datenschutzgesetz geregelt. Die Aufsicht hierüber führt die nationale Datenschutzbehörde gestützt auf Vorschriften, die ebenfalls im allgemeinen Datenschutzgesetz niedergelegt sind.

Soweit anwendbar sieht das allgemeine Datenschutzgesetz in der Regel eine Reihe von Ausnahmeregelungen (Abweichungen von einem oder mehreren Grundsätzen) bei der Verarbeitung personenbezogener Daten durch Nachrichtendienste vor. Diese Ausnahmen betreffen zumeist die grundlegenden Verpflichtungen von Datenverarbeitern und die Rechte der betroffenen Personen.[14] Sie können in der Beschränkung des Rechts, unterrichtet zu werden, und des Rechts auf Zugang durch die betroffene Person bestehen, die im Allgemeinen durch die Datenschutzbehörde vorzunehmen ist.

Was die Aufsicht über die Datenverarbeitung anbelangt, so werden in nur vier Mitgliedstaaten mit den allgemeinen einzelstaatlichen Datenschutzgesetzen (oder dem Gesetz zur Errichtung eines allgemeinen Datenschutzaufsichtsgremiums) grundsätzlich die gleichen Aufsichtsbefugnisse über Nachrichtendienste verliehen wie über jeden anderen für die Datenverarbeitung Verantwortlichen.[15] In dreizehn Mitgliedstaaten fallen die nationalen Sicherheits- und Nachrichtendienste unter die Aufsichtsbefugnis der Datenschutzbehörde, doch in einigen Fällen sind spezielle Vorschriften oder Verfahren für die Beaufsichtigung von Sicherheits- und Nachrichtendiensten anwendbar, darunter die Möglichkeit, Sanktionen zu verhängen.[16] In neun Mitgliedstaaten hat die Datenschutzbehörde keine Aufsichtsbefugnis über den Nachrichtendienst als Datenverarbeiter.[17]

Nur in Schweden und Slowenien ist die volle Aufsicht der Datenschutzbehörde über die Einhaltung der geltenden Datenschutzverpflichtungen gewährleistet. Sofern andere nationale Datenschutzbehörden Befugnisse gegenüber Nachrichtendiensten haben, bestehen diese darin, die Einhaltung des geltenden allgemeinen Datenschutzgesetzes zu überprüfen, Beschwerden zu bearbeiten und das Recht der betreffenden Person auf Zugang auszuüben. Des Weiteren dürfen sie auf eigene Initiative oder auf Antrag eines Dritten Untersuchungen und Vor-Ort-Kontrollen durchführen. In einigen Mitgliedstaaten unterliegen diese Befugnisse gewissen Beschränkungen, indem beispielsweise die Einhaltung spezieller Sicherheitsbestimmungen bei der Untersuchung auferlegt wird, um staatlichen Geheimhaltungspflichten Rechnung zu tragen.

[14] Beispielsweise Belgien, Bulgarien, Deutschland, Griechenland, Ungarn und Zypern. Für einige Mitgliedstaaten liegen keine Informationen über Ausnahmeregelungen vor.

[15] Bulgarien, Schweden, Slowenien, Ungarn.

[16] Belgien, Deutschland, Estland, Finnland, Frankreich, Irland, Italien, Lettland, Luxemburg, Österreich, Polen, Schweden, Zypern.

[17] Dänemark, Malta, Niederlande, Portugal, Rumänien, Slowakei, Spanien, Tschechische Republik, Vereinigtes Königreich.

4.3. Die Funktion anderer unabhängiger Aufsichtsmechanismen

Zwanzig Mitgliedstaaten erklärten, dass das Gesetz neben der Zuständigkeit der Datenschutzbehörden für die Datenverarbeitung die parlamentarische Aufsicht und/oder Kontrolle über die Tätigkeiten der Nachrichtendienste[18] und spezielle interne Kontrollsysteme vorsieht.[19] Die Auffassungen über die parlamentarische Kontrolle gehen in den Mitgliedstaaten allerdings offenkundig auseinander, denn nur wenige von ihnen verfügen tatsächlich über eine Stelle, die für die Aufsicht über den Datenschutz (und die Bewertung der Rechte der Betroffenen sowie die Einhaltung der Bestimmungen des allgemeinen Datenschutzgesetzes und der spezifischen Vorschriften) zuständig ist.[20]

Die bestehenden Aufsichtsmechanismen sind äußerst vielfältig und bestehen aus folgenden Elementen:

- Ein Parlamentsausschuss mit der umfassenden Aufgabe, Geheimdienst- und Sicherheitsbehörden im Allgemeinen oder einen bestimmten Nachrichtendienst zu beaufsichtigen.

- Die parlamentarische Aufsicht und/oder Kontrolle erfolgt neben anderen unabhängigen Aufsichtsgremien (bei denen es sich nicht um Datenschutzbehörden handelt). Derzeit erfolgt die parlamentarische Kontrolle entweder durch den Bürgerbeauftragten des Parlaments, eine parlamentarische Delegation oder einen parlamentarischen Ausschuss.

- Ein Parlamentsausschuss ist das einzige Aufsichtsgremium außerhalb der Exekutivstruktur. Die Aufgaben des Parlaments sind in diesem Fall entweder sehr allgemein oder so formuliert, dass kein Zugang zu offenen Fällen vorgesehen ist.

- Für die Aufsicht ist ausschließlich eine spezielle Behörde zuständig. Der Zuständigkeit können Datenschutzvorschriften zugrundeliegen, in einem Fall wurde allerdings gemeldet, dass für diese Behörde bis vor kurzem unverbindliche Regelungen („Soft Law“) galten.

[18] In Finnland beispielsweise besitzt neben der Datenschutzbehörde der Bürgerbeauftragte des Parlaments entsprechende Befugnisse; diese basieren allerdings auf dem speziellen Gesetz für Sicherheits- und Nachrichtendienste.

[19] Diese 20 Mitgliedstaaten sind: Bulgarien, Deutschland, Estland, Finnland, Frankreich, Griechenland, Italien, Lettland, Luxemburg, Österreich, Polen, Portugal, Rumänien, die Slowakei, Slowenien, Spanien, die Tschechische Republik, Ungarn, das Vereinigte Königreich und Zypern.

[20] In der Stellungnahme werden keine Informationen zur Kontrolle der Verwaltung (der Ministerien) und zur allgemeinen politischen Kontrolle berücksichtigt, die von mehreren beitragenden Ländern vorgelegt wurden.

- Neben der allgemeinen parlamentarischen Aufsicht erfolgt eine spezielle gerichtliche Kontrolle.

- Neben der Aufsicht durch die allgemeine Datenschutzbehörde erfolgt eine gemischte exekutive und parlamentarische Kontrolle; den Vorsitz der eingesetzten Kommission hat ein Richter inne, und die Mitglieder gehören verschiedenen ehemals oder derzeit im Parlament vertretenen politischen Partien an. Es sind Konsultationsverfahren mit der Datenschutzbehörde vorgesehen.

- Denkanstöße für die Verbesserung der Aufsicht geben auch Länder, in denen ein spezielles Gremium für die Beaufsichtigung der Einhaltung des Datenschutzes durch Nachrichtendienste eingesetzt wurde, so z. B. eine aus drei vom Generalstaatsanwalt ernannten Staatsanwälten bestehende Datenaufsichtskommission, die die Nachrichtendienste neben dem parlamentarischen Aufsichtsrat beaufsichtigt.

- Die Datenschutzbehörde kann mit der Prüfung befasst werden, ob die nationale Sicherheit im Einzelfall berührt ist, und muss – sofern dies festgestellt wird – den Fall zwei unabhängigen Beauftragten mit unabhängiger gerichtlicher Aufsichtsbefugnis über die nationalen Nachrichtendienste und die vom Außenminister erteilten Ermächtigungen für die Durchführung einer verdeckten Überwachung vorlegen. Zusätzlich gibt es ein spezielles Gericht für die Entschädigung betroffener Personen.

- Ein gesondertes Gesetz sieht die Zusammenarbeit zwischen dem speziellen Aufsichtsgremium und der allgemeinen Datenschutzbehörde vor: Ein unabhängiger Rechtsschutzbeauftragter muss die Genehmigung erteilen, wenn die Geheim- oder Nachrichtendienste bestimmte Operationen durchführen wollen (z. B. verdeckte Ermittlungen, Videoüberwachung bestimmter Personen). Der Rechtsschutzbeauftragte ist darüber hinaus verpflichtet, bei der Datenschutzbehörde Beschwerde einzulegen, sofern er der Ansicht ist, dass Rechte aus dem allgemeinen Datenschutzgesetz verletzt wurden.

Die Datenschutzbehörde ist mit gewissen Einschränkungen zur Aufsicht über die Nachrichtendienste befugt, während ein spezielles parlamentarisches Gremium dafür zuständig ist, die Überwachung der Kommunikation zu beaufsichtigen und Beschwerden zu bearbeiten. Die Mitglieder des entsprechenden Ausschusses werden vom parlamentarischen Kontrollausschuss ernannt. Der Vorsitzende muss über die Befähigung zur Ausübung einer richterlichen Tätigkeit verfügen.

5. Empfehlungen

A. Mehr Transparenz

1. Es ist mehr Transparenz in Bezug auf die Funktionsweise der Programme und die Tätigkeiten und Entscheidungen der Aufsichtsbehörden geboten.

Die Datenschutzgruppe ist der Ansicht, dass die Mitgliedstaaten in Bezug auf ihre Rolle bei der Erfassung nachrichtendienstlicher Daten und die Mitnutzung von Programmen größtmögliche Transparenz herstellen sollten, und zwar vorzugsweise gegenüber der Öffentlichkeit, gegebenenfalls jedoch zumindest gegenüber ihren nationalen Parlamenten und den zuständigen Aufsichtsbehörden. Datenschutzbehörden wird empfohlen, ihr Fachwissen im Interesse der Wiederherstellung des Gleichgewichts zwischen nationalen Sicherheitsinteressen und dem Grundrecht auf Achtung der Privatsphäre des Einzelnen auf nationaler Ebene einzubringen.

Es sollte in irgendeiner Form ganz allgemein über Überwachungsaktivitäten berichtet werden, nicht zuletzt um den Transparenzverpflichtungen nachzukommen, die den Mitgliedstaaten dem EGMR zufolge obliegen.[21] Jeder Eingriff in die Grundrechte muss vorhersehbar sein, weshalb diese Programme auf klaren, spezifischen und zugänglichen Rechtsvorschriften basieren müssen. Die nationalen Datenschutzbehörden sind aufgefordert, ihren jeweiligen Regierungen diesen Standpunkt zur Kenntnis zu bringen.

2. Mehr Transparenz seitens der für die Datenverarbeitung Verantwortlichen

Unternehmen müssen für ein möglichst hohes Maß an Transparenz sorgen und sicherstellen, dass sich Betroffene im Klaren darüber sind, dass sobald ihre personenbezogenen Daten auf der Grundlage der für diese Übermittlungen verfügbaren Instrumente an unsichere Drittstaaten übermittelt wurden, sie von Drittstaatsbehörden überwacht werden können oder diese Zugangsrechte haben können, sofern derartige Ausnahmen in diesen Instrumenten vorgesehen sind. Die Datenschutzgruppe ist sich bewusst, dass Datenverarbeiter angewiesen worden sein können, die Betroffenen nicht über die von einer Behörde ergangene Anordnung zu unterrichten. Sie begrüßt die jüngsten Bemühungen um eine bessere und genauere Unterrichtung der Betroffenen über eingegangene Anfragen und ermutigt die Unternehmen, die Informationspolitik weiter zu verbessern.

[21] Siehe auch Urteil des Europäischen Gerichtshofs für Menschenrechte vom 25. Juni 2013, Fall Nr. 48135/06 – Youth Initiative for Human Rights/Serbien, S. 6.

3. Stärkere Sensibilisierung der Öffentlichkeit

Betroffene müssen über die Auswirkungen der Nutzung von elektronischen Online- und Offline-Kommunikationsdiensten und die Möglichkeiten, sich selbst besser zu schützen, Bescheid wissen. Dafür sind Datenschutzbehörden, andere Behörden, Unternehmen und die Zivilgesellschaft gemeinsam verantwortlich. Daher möchte die Datenschutzgruppe im zweiten Halbjahr 2014 eine Konferenz mit allen Beteiligten abhalten, auf der ein möglicher
Ansatz diskutiert werden soll.

B. Wirkungsvollere Aufsicht

1. Pflege eines kohärenten Rechtssystems für die Nachrichtendienste, einschließlich datenschutzrechtlicher Vorschriften

Die Enthüllungen von Edward Snowden haben vor Augen geführt, dass die Nachrichtendienste der EU-Mitgliedstaaten täglich große Mengen an personenbezogenen Daten verarbeiten. Diese Daten werden mit anderen Diensten innerhalb und außerhalb der EU geteilt. Die Datenschutzgruppe hält es für wichtig, dass die Mitgliedstaaten über einen kohärenten Rechtsrahmen für die Nachrichtendienste, einschließlich Datenverarbeitungsvorschriften im Einklang mit den im EU- und Völkerrecht niedergelegten Datenschutzgrundsätzen, verfügen. Beim Schutz der gefährdeten öffentlichen Interessen sind die Rechte der betroffenen Personen in größtmöglichem Umfang zu gewährleisten.

Die Datenschutzgruppe empfiehlt darüber hinaus, dass der nationale Rechtsrahmen klare Vorschriften für die Zusammenarbeit und den Austausch von personenbezogenen Daten mit Strafverfolgungsbehörden bei der Verhütung, Bekämpfung und Verfolgung von Straftaten enthalten, so auch für die Übermittlung solcher Daten an Behörden in anderen EU- Mitgliedstaaten und in Drittstaaten.

2. Sicherstellung einer wirksamen Aufsicht über die Nachrichtendienste

Im nationalen Rechtsrahmen für die Nachrichtendienste sollte den bestehenden Aufsichtsmechanismen besondere Aufmerksamkeit gewidmet werden. In einer demokratischen Gesellschaft ist eine angemessene, unabhängige und wirksame Aufsicht von höchster Bedeutung. Die Datenschutzgruppe ist daher der Ansicht, dass die nachstehenden bewährten Praktiken, die derzeit in den Mitgliedstaaten innerhalb ihrer verschiedenen Aufsichtsmechanismen angewendet werden, fester Bestandteil der Aufsichtsmechanismen aller Mitgliedstaaten sein sollten. Den nationalen Datenschutzbehörden wird nahegelegt, diese Elemente in die nationale Debatte über die nachrichtendienstliche Aufsicht einzubringen:

– strenge interne Kontrollen der Einhaltung der nationalen Rechtsrahmen zur Gewährleistung von Rechenschaftspflicht und Transparenz;

– wirksame parlamentarische Kontrolle im Einklang mit den nationalen parlamentarischen Traditionen. Parlamente, die bereits über Aufsichtsbefugnisse über die Nachrichtendienste verfügen, sollten von den nationalen Datenschutzbehörden dazu angehalten werden, diese aktiv wahrzunehmen;

– effektive, solide und unabhängige externe Aufsicht, die entweder von einem zuständigen Gremium unter Mitwirkung der Datenschutzbehörden oder von der Datenschutzbehörde selbst wahrgenommen wird, die die Befugnis zum regelmäßigen Zugang zu Daten oder sonstigen einschlägigen Unterlagen auf eigene Initiative (von Amts wegen) sowie die Verpflichtung zur Prüfung eingelegter Beschwerden hat. Die vorherige Zustimmung des zu beaufsichtigenden Nachrichtendienstes darf nicht erforderlich sein.

C. Wirksame Anwendung des geltenden Rechts

1. Durchsetzung der bestehenden Verpflichtungen der EU-Mitgliedstaaten und der EMRK-Vertragsparteien zum Schutz der Rechte auf Achtung des Privatlebens und Datenschutz

Alle Mitgliedstaaten sind Vertragsparteien der Europäischen Menschenrechtskonvention. Daher müssen ihre Überwachungsprogramme den in den Artikeln 7 und 8 EMRK genannten Bedingungen genügen. Doch damit enden ihre Verpflichtungen noch nicht. Artikel 1 EMRK verpflichtet die Vertragsparteien außerdem dazu, allen ihrer Hoheitsgewalt unterstehenden Personen die in der Konvention bestimmten Rechte und Freiheiten zuzusichern. Sowohl als EU-Mitgliedstaaten als auch als EMRK-Vertragsparteien können sie wegen der Verletzung des Rechts auf Achtung des Privatlebens eines EU-Staatsbürgers vor den EGMR gebracht werden.

2. Dem EU-Recht unterliegende Datenverarbeiter müssen die einschlägigen EU-Datenschutzvorschriften einhalten

Datenverarbeiter, die in der EU niedergelassen sind oder Ausrüstung in einem Mitgliedstaat nutzen, müssen ihren EU-rechtlichen Verpflichtungen auch dann nachkommen, wenn die Rechtsvorschriften anderer Länder, in denen sie tätig sind, dem EU-Recht entgegenstehen. Datenschutzbehörden dürfen diesbezüglich nicht unberücksichtigt lassen, dass Daten unter Verstoß gegen das EU-Recht übermittelt werden können. Die Datenschutzgruppe weist daher erneut darauf hin, dass die Datenschutzbehörden gemäß den nationalen und EU-Datenschutz-

bestimmungen den Datenfluss innerhalb der Übermittlungsinstrumente aussetzen können, wenn eine hohe Wahrscheinlichkeit besteht, dass Datenschutzgrundsätze verletzt werden und die fortgesetzte Datenübermittlung für die betroffene Personen das unmittelbare Risiko eines schweren Schadens schaffen würde. Die nationalen Datenschutzbehörden sollten entsprechend ihrer nationalen Zuständigkeit entscheiden, ob Sanktionen in einer konkreten Situation angezeigt sind.

D. Verbesserung des Schutzes auf europäischer Ebene

1. Annahme des Datenschutz-Reformpakets

Um wesentliche Datenschutzgarantien in Europa bieten zu können, müssen die Verhandlungen über das Datenschutz-Reformpaket unbedingt zum Abschluss gebracht werden, denn die neue Datenschutz-Grundverordnung und die Richtlinie über den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit sollen nicht nur den Datenschutz für Privatpersonen verbessern, sondern auch ihren Anwendungsbereich klarstellen und die Durchsetzungsbefugnisse der Datenschutzbehörden stärken. Insbesondere durch die Möglichkeit, – als letztes Mittel – (Geld)Strafen zu verhängen, soll der Druck auf die Datenverarbeiter erhöht werden. Die Datenschutzgruppe begrüßt den Vorschlag des Europäischen Parlaments, Personen verpflichtend zu informieren, wenn einer Behörde innerhalb der letzten zwölf Monate Zugriff auf Daten gewährt wurde. Durch Transparenz bei diesen Handlungen wird das Vertrauen enorm gestärkt. Die Datenschutzgruppe fordert den Rat und das Europäische Parlament daher auf, sich an ihren vereinbarten Zeitplan zu halten[22] und dafür zu sorgen, dass beide Rechtsinstrumente im Laufe des Jahres 2014 angenommen werden können.

2. Präzisierung des Anwendungsbereichs der Ausnahmeregelung aus Gründen der nationalen Sicherheit

Es herrscht derzeit keine Einigkeit darüber, was unter nationaler Sicherheit zu verstehen ist. Weder hat der europäische Gesetzgeber eine klare Begriffsbestimmung vorgenommen, noch ist die Rechtsprechung der europäischen Gerichte schlüssig. Dessen ungeachtet darf sich die Ausnahmeregelung nicht auf die Verarbeitung personenbezogener Daten zu gegen das Gesetz verstoßenden Zwecken erstrecken.

Es stellt sich auch die Frage, inwieweit eine auf nationale Sicherheitsinteressen ausgerichtete Ausnahmeregelung noch der Realität entspricht, da nun offenbar geworden ist, dass die Tätigkeit der Nachrichtendienste mehr denn je mit der

[22] http://euobserver.com/justice/122853

Tätigkeit der Strafverfolgungsbehörden verflochten ist und mit ihr mehrere unterschiedliche Zwecke verfolgt werden. Daten werden kontinuierlich und weltweit ausgetauscht, wobei es keine Rolle spielt, wessen nationale Sicherheit von der Analyse dieser Daten profitiert. Die Datenschutzgruppe fordert den Rat, die Kommission und das Parlament daher auf, sich auf eine Definition des Begriffs der nationalen Sicherheit zu verständigen und schlüssig zu klären, was in die ausschließliche Zuständigkeit der Mitgliedstaaten fällt. Bei der Definition des Begriffs der nationalen Sicherheit sollten die Überlegungen der Datenschutzgruppe, einschließlich der Darlegungen in dieser Stellungnahme, gebührend berücksichtigt werden. Die EU-Organe sollten in dem Datenschutz-Reformpaket zudem klarstellen, dass der Schutz der nationalen Sicherheit von Drittstaaten allein kein Ausschlussgrund für die Anwendbarkeit des EU-Rechts sein kann.

E. Internationaler Schutz für in der EU ansässige Personen

1. Einforderung hinreichender Garantien für den Austausch nachrichtendienstlicher Daten

Die Behörden von Drittstaaten und insbesondere deren Nachrichtendienste dürfen keinen unmittelbaren Zugriff auf in der EU verarbeitete private Daten haben. Wenn sie im Einzelfall und bei begründetem Verdacht Zugriff auf solche Daten verlangen, müssen sie gegebenenfalls gemäß internationaler Übereinkünfte einen entsprechenden Antrag stellen und für angemessene Datenschutzgarantien sorgen. Beim Austausch nachrichtendienstlicher Informationen haben die Mitgliedstaaten sicherzustellen, dass die nationalen Rechtsvorschriften eine spezifische Rechtsgrundlage für diesen Austausch sowie hinreichende Garantien für den Schutz personenbezogener Daten vorsehen. Aus Sicht der Datenschutzgruppe erfüllen geheime Kooperationsvereinbarungen zwischen Mitgliedstaaten und/oder Drittstaaten nicht die Anforderungen des EGMR an eine klare und zugängliche Rechtsgrundlage.

2. Aushandlung internationaler Abkommen zur Gewährleistung angemessener Datenschutzgarantien

Das Konzept eines Rahmenabkommens, wie es derzeit zwischen den USA und der EU ausgehandelt wird, ist ein Schritt in die richtige Richtung. Ein solches Abkommen könnte allerdings in zweierlei Hinsicht unzulänglich sein: So wären Fälle, in denen es um die nationale Sicherheit geht, – zumindest aus europäischer Sicht – ausgenommen, da das Abkommen ausschließlich auf EU-Recht basieren soll. Zudem legt sein Aufbau nahe, dass es nur für Daten gelten soll, die zwischen Behörden der USA und der EU ausgetauscht werden, und nicht für von privaten Einrichtungen erhobene Daten. Dies geht auch aus dem Bericht der

Hochrangigen Kontaktgruppe EU-USA (HLCG) für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten[23] hervor, der den Verhandlungen über das Rahmenabkommen zugrundeliegt. Die Datenschutzgruppe betont, dass in dem Rahmenabkommen festgeschrieben werden sollte, dass die Verarbeitung der übermittelten Daten in der EU und den USA zum selben Zweck erfolgt. Es wäre nicht hinnehmbar, wenn von EU-Strafverfolgungsbehörden gesammelte Daten später von US-Geheimdiensten für nationale Sicherheitsbelange verwendet werden könnten, solange der EU nicht die gleichen Möglichkeiten offen stehen.

Da das Rahmenabkommen nicht allen Bürgern vollständigen Schutz bieten wird, bedarf es eines internationalen Abkommens, das angemessenen Schutz vor willkürlicher Überwachung gewährleistet. Auch der derzeitige Widerstreit der Rechtsprechung in Bezug auf Teile der enthüllten Überwachungstätigkeiten ließe sich entschärfen, wenn der Überwachung durch solch ein Abkommen klare Grenzen gesetzt würden. Dieses Abkommen wäre allerdings direkt an die Ausnahmeregelung aus Gründen der nationalen Sicherheit gekoppelt und fiele damit nicht in den Anwendungsbereich des EU-Rechts. Die Mitgliedstaaten müssen daher koordinierte Verhandlungen einleiten. Es sollte eindeutig festgestellt werden, welche der genannten Überwachungstätigkeiten tatsächlich unter die nationale Sicherheit fallen und welche eher mit der Strafverfolgung und außenpolitischen Zwecken in Verbindung stehen und damit unter EU-Recht fallende Bereiche berühren. Dies würde den EU-Organen die Möglichkeit zur stärkeren Beteiligung eröffnen, sollten Schritte in dieser Richtung unternommen werden.

Dieses neue Abkommen darf nicht geheim sein. Es muss veröffentlicht werden und sollte Verpflichtungen für die Vertragsparteien in Bezug auf die erforderliche Aufsicht über die Überwachungsprogramme, die Transparenz, die Gleichbehandlung zumindest der Bürger aller Vertragsparteien, die Rechtsbehelfsmechanismen und andere Datenschutzrechte enthalten. Die Beteiligten sollten zudem ermutigt werden, für eine regelmäßige Unterrichtung ihrer Parlamente über die Anwendung und den Nutzen des geschlossenen Abkommens zu sorgen.

3. Entwicklung eines weltweiten Instruments zum Schutz der Privatsphäre und personenbezogener Daten

Die Datenschutzgruppe unterstützt die Entwicklung eines weltweiten Instruments, das durchsetzbare Grundsätze für den Schutz der Privatsphäre und des Datenschutzes auf einem hohem Niveau vorschreibt, wie sie auf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

[23] Ratsdokument Nr. 15851/09 vom 23. November 2009.

in ihrer Erklärung von Madrid vereinbart wurden.[24] In diesem Zusammenhang könnte die Annahme eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts der Vereinten Nationen über bürgerliche und politische Rechte in Erwägung gezogen werden. In solch einem internationalen Rechtsakt müsste sichergestellt werden, dass die gewährten Garantien allen Betroffenen zugutekommen. Zudem ist eine allgemein gültige Auslegung des Begriffs „Datenverarbeitung" notwendig, da weltweit sehr unterschiedliche Auffassungen dazu bestehen.

Die Datenschutzgruppe unterstützt die Initiative der deutschen Regierung und den Aufruf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre.[25, 26] Zudem befürwortet sie auch weiterhin den Beitritt von Drittstaaten zur Konvention Nr. 108 des Europarates.

[24] Internationale Standards zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre, angenommen von der 31. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Madrid.

[25] http://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html

[26] Entschließung „Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht", angenommen von der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Warschau.

Gemeinsame Erklärung der europäischen Datenschutzbehörden im Rahmen der Art. 29-Datenschutzgruppe vom 26. November 2014 (WP 227)

Einleitung

Unser tägliches Leben ist zunehmend digitalisiert. In weniger als einem Jahrzehnt haben sich berufliche, wirtschaftliche und private Aktivitäten immer mehr in eine digitale Umgebung verlagert. Diese Entwicklung hat eine Welt neuer Chancen eröffnet und die Entwicklung außerordentlich innovativer Güter und Dienste ermöglicht, die individuelle und allgemeine Bedürfnisse befriedigen. Personenbezogene Daten sind die Grundlage dieser digitalen Welt.

Das Funktionieren der digitalen Umgebung beruht im Wesentlichen auf komplexen Informationsinfrastrukturen, die private Unternehmen für ihre Zwecke errichtet haben. Diese Unternehmen sammeln riesige Mengen personenbezogener Daten, die einige von ihnen speichern, weiterverarbeiten und übermitteln können, ohne ein angemessenes Maß an Kontrolle durch den Nutzer und außerhalb jeder Art von effektiver Aufsicht. Darüber hinaus haben die Snowden-Veröffentlichungen kürzlich verdeutlicht, dass Behörden und Geheimdienste in massivem Umfang Zugang zu dieser Dateninfrastruktur für andere Zwecke, nämlich der nationalen Sicherheit, verlangt haben.

Die systematische und massive Art dieses Zugangs hat die Öffentlichkeit rund um die Welt schockiert. Jetzt stellt sich die Frage, wie sowohl dem Vertrauensverlust gegenüber (ausländischen und eigenen) Regierungen, Geheimdiensten und Sicherheitsbehörden, wie auch dem zugrundeliegenden Problem der Kontrolle des Zugriffs auf umfangreiche Datenmengen begegnet werden soll. Wie kann ein Rahmen gestaltet werden, der privaten Unternehmen und anderen Einrichtungen Innovationen und die Erbringung von Gütern und Diensten erlaubt, die dem privaten und öffentlichen Bedarf entsprechen, und gleichzeitig nationalen Geheimdiensten die Erfüllung ihrer Aufgaben im Rahmen des geltenden Rechts ermöglicht, ohne in eine Überwachungsgesellschaft zu geraten?

Wegen seiner gemeinsamen Geschichte und Kultur muss Europa seine Stimme zur Geltung bringen, wenn es um die Beachtung der Menschenrechte einschließlich der Rechte auf Privatheit und Datenschutz geht, ohne die Innovation oder die Notwendigkeit der gesellschaftlichen Sicherheit zu beeinträchtigen. In diesem Zusammenhang wollen die unabhängigen Datenschutzbehörden im Rahmen der Art. 29-Arbeitsgruppe verschiedene zentrale Botschaften formulieren, um diese globale Herausforderung zu meistern.

Deshalb hat die Art. 29-Arbeitsgruppe in ihrer Plenarsitzung am 25. November 2014 die folgende Erklärung beschlossen:

Europäische Werte

1. **Der Schutz personenbezogener Daten ist ein Grundrecht**. Personenbezogene Daten (zu denen auch Metadaten gehören) dürfen nicht nur als Handelsobjekt, wirtschaftlicher Wertgegenstand oder öffentliches Gut behandelt werden.

2. **Datenschutzrechte müssen mit anderen Grundrechten abgewogen werden**. Dazu gehören die Nicht-Diskriminierung und die Meinungsfreiheit, die in einer demokratischen Gesellschaft gleichwertig sind. Sie müssen auch mit dem Erfordernis der Sicherheit abgewogen werden.

3. **Technik ist ein Mittel, das dem Menschen zu dienen hat**. Die Tatsache, dass etwas technisch möglich ist und dass Datenverarbeitung manchmal zu nützlichen Ergebnissen führt oder die Entwicklung neuer Dienste ermöglicht, bedeutet nicht zwingend gleichzeitig, dass es sozial akzeptabel, ethisch, vernünftig oder rechtmäßig ist.

4. **Das Vertrauen der Öffentlichkeit in Produkte und Dienste der digitalen Wirtschaft** hängt weitgehend davon ab, dass die Technologie-Unternehmen sich an das Datenschutzrecht halten. Diese Rechtstreue ist ein positiver Wettbewerbsfaktor in der digitalen Wirtschaft; sie wird auch nachhaltige Entwicklung zum Nutzen der Verbraucher und der Industrie sicherstellen.

5. **Das Bewusstsein der Öffentlichkeit und die rechtliche und tatsächliche Stellung des Einzelnen müssen gestärkt werden**, um die Menschen besser vor exzessiver Überwachung durch öffentliche und private Stellen zu schützen. In dieser Hinsicht sind die Verbesserung der digitalen Kompetenz einschließlich der Datenschutzerziehung und die Eröffnung von kollektiven Klagemöglichkeiten für Einzelne von entscheidender Bedeutung, um die Offenlegung von weit verbreiteten Datenschutzverletzungen zu erleichtern.

Überwachung aus Gründen der Sicherheit

6. **Die heimliche, massive und ungezielte Überwachung** von Menschen in Europa, sei es durch öffentliche oder private Einrichtungen, die in einem EU-Mitgliedstaat oder aus anderen Ländern agieren, ist weder rechtmäßig im Hinblick auf die europäischen Verträge und Gesetze noch ist sie ethisch hinnehmbar.

7. **Die unbegrenzte flächendeckende Speicherung von personenbezogenen Daten auf Vorrat für Sicherheitszwecke ist in einer demokratischen Gesellschaft nicht akzeptabel**. Die Speicherung, der Zugang zu und die Nutzung von Daten durch die zuständigen nationalen Behörden sollten auf das begrenzt sein, was in einer demokratischen Gesellschaft zwingend notwendig und verhältnismäßig ist, und sie sollten einer effektiven Kontrolle und verfahrensmäßigen Sicherheitsgarantien unterworfen sein.

8. **Die Verarbeitung von personenbezogenen Daten im Zusammenhang mit Überwachungstätigkeiten** darf nur unter angemessenen rechtlichen Garantien und in Übereinstimmung mit Art. 8 der Europäischen Grundrechtecharta stattfinden. Solche Garantien schließen eine **unabhängige und effektive Aufsicht** ein, an der Datenschutzbeauftragte innerhalb ihrer Zuständigkeiten wirklich beteiligt sein sollten.

9. In der Regel sollte eine Behörde in einem Land außerhalb der Europäischen Union keinen unbeschränkten **direkten Zugang zu den Daten von Einzelpersonen haben, die nach den Regeln der Europäischen Union verarbeitet werden**, was auch immer die Bedingungen dieses Zugangs sein mögen, und unabhängig vom Speicherort der Daten. Konflikte zwischen Rechtsordnungen sollten nur unter bestimmten Bedingungen gelöst werden – z. B. durch die vorherige Erlaubnis einer Behörde in der Europäischen Union oder durch ein Rechtshilfeabkommen, die jeweils den Zugang durch ausländische Sicherheitsbehörden zu Daten, die aus der Europäischen Union übermittelt worden sind, oder zu in der Europäischen Union gespeicherten Daten regeln. Ausländische Informationsersuchen dürfen nicht direkt Unternehmen zugestellt werden, die EU-Recht unterliegen.

10. Keine der Bestimmungen der **Europäischen Rechtsakte zur Regelung internationaler Datenübermittlungen** zwischen privaten Unternehmen bietet eine Rechtsgrundlage für den Datentransfer zu einer Drittstaatsbehörde für Zwecke der massiven und ungezielten Überwachung (sei es Safe Harbor, bindende Unternehmensregeln oder Standardvertragsklauseln).

11. Wenn öffentliche oder private Einrichtungen massive Datenmengen erheben, die sehr präzise Informationen über das Privatleben von einzelnen Menschen liefern, deren Daten gespeichert werden, sollten sie die Speicherung dieser Daten so vornehmen, dass eine unabhängige Behörde überprüfen kann, ob die Vorgaben des Datenschutzes eingehalten werden. Die **Speicherung der betreffenden Daten innerhalb der Europäischen Union** ist eine effektive Möglichkeit, um die Ausübung einer derartigen Kontrolle zu ermöglichen.

Europäischer Einfluss

12. **Das Europäische Datenschutzpaket sollte 2015 verabschiedet werden**. Während es zur Vereinheitlichung des Europäischen digitalen Marktes beiträgt, muss es ein hohes Niveau des Datenschutzes für Betroffene in Übereinstimmung mit europäischen Werten und Grundrechten sicherstellen.

13. Das Europäische Datenschutzniveau sollte nicht ganz oder teilweise aufgeweicht werden durch bilaterale oder **internationale Abkommen, einschließlich Handelsabkommen** über Güter oder Dienstleistungen mit Drittstaaten.

14. Die Datenschutzregeln der Europäischen Union sind notwendig, um die politische, soziale und wirtschaftliche Lage der Europäischen Union und der Menschen und Einrichtungen zu sichern, die der EU-Gesetzgebung unterliegen. Deren Grundsätze sollten als **international zwingend nach Völkerrecht und internationalem Privatrecht** angesehen werden. Ausländische Rechtsordnungen oder internationale Verträge können sie weder verdrängen noch können Organisationen sie vertraglich abbedingen.

15. Wenn die richtige Balance zwischen Datenschutz, Innovation und Sicherheit hergestellt wird, so bedeutet **dies weder die Wiederherstellung interner Grenzen innerhalb der Europäischen Union noch das Schließen der Tore Europas** gegenüber außereuropäischen Partnern. Es setzt Respekt für das hohe Schutzniveau voraus, das von der Europäischen Datenschutztradition einschließlich der Konvention Nr. 108 des Europarats und der Datenschutzbestimmungen der Europäischen Union abgeleitet wird.

Nächste Schritte

16. Die Arbeitsgruppe begrüßt **Kommentare** zu dieser Erklärung von allen interessierten öffentlichen oder privaten Interessensträgern. Solche Kommentare können über die eingerichtete Webseite unter www.europeandatagovernance-forum.com abgegeben werden. Die Arbeitsgruppe wird diese Kommentare bei ihren Aktivitäten im Jahr 2015 berücksichtigen.

VI. Internationale Konferenz der Datenschutzbeauftragten

36. Konferenz vom 13. – 16. Oktober 2014, Mauritius

Entschließung zu Big Data

– Übersetzung –

Es wird häufig anerkannt, dass die Möglichkeit zur Speicherung und Analyse riesige Mengen von Daten sich für die Gesellschaft als vorteilhaft erweisen kann. So kann Big Data z. B. genutzt werden, um die Ausbreitung von Epidemien vorherzusagen, gravierende Nebenwirkungen von Medikamenten aufzudecken und die Verschmutzung in großen Städten zu bekämpfen. Einige dieser Nutzungen beinhalten keine Verwendung personenbezogener Daten; Big Data kann jedoch auch in einer Art genutzt werden, die zu gravierenden Besorgnissen in Bezug auf die Privatsphäre des Individuums und auf Bürgerrechte, den Schutz gegen Diskriminierungen und Beschränkungen des Rechts auf Gleichbehandlung führt.

Big Data bedingt einen neuen Blick auf Daten, mit dem Informationen sichtbar werden, die vorher nur schwer zu gewinnen oder in anderer Weise verschleiert waren. Big Data beinhaltet in großem Ausmaß die Wiedeverwendung von Daten. Der Wert der Daten kann mit der Möglichkeit verbunden sein, Vorhersagen über zukünftige Handlungen oder Ereignisse zu treffen. Big Data kann als Herausforderung für wesentliche Grundsätze des Schutzes der Privatsphäre, insbesondere für die Prinzipien der Zweckbindung und der Datenminimierung angesehen werden. Der Schutz, den diese Datenschutzprinzipien gewähren, ist wichtiger als je zuvor in einer Zeit, in der ein zunehmendes Ausmaß von Daten über jedermann gesammelt wird. Die Prinzipien stellen das Fundament für Schutzmaßnahmen dar gegen eine extensive Profilbildung in einer immer weiter zunehmenden Reihe von neuen Zusammenhängen. Eine Verwässerung grundlegender Datenschutzprinzipien in Kombination mit einer extensiveren Nutzung von Big Data wird sich aller Voraussicht nach nachteilig auf den Schutz der Privatsphäre und anderer Grundrechte auswirken.

Mitglieder der Internationalen Konferenz und andere Interessenvertreter wie z. B. die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT, auch bekannt als „Berlin Group“) haben sich mit Fragen des Datenschutzes und des Schutzes der Privatsphäre im Zusammenhang mit Big Data auseinandergesetzt. Datenschutzbedenken im Hinblick auf die Nutzung von Profilbildung sind von der Internationalen Konferenz in der Uruguayer Erklärung von 2012 und in der Warschauer Erklärung zur Profilbildung von 2013 aufgeworfen

worden. Um weitere Anstrengungen zur Reduzierung von Risiken bei der Verwendung von Big Data zu befördern,

fordert die 36. Internationale Konferenz der Datenschutzbeauftragten alle Parteien auf, die Big Data verwenden,

- den Grundsatz der Zweckbindung zu respektieren.

- Das Ausmaß der Datenerhebung und -speicherung auf das für den beabsichtigten, rechtmäßigen Zweck notwendige Maß zu beschränken.

- Eine rechtsgültige Einwilligung von den Betroffenen im Zusammenhang mit der Nutzung personenbezogener Daten für Zwecke der Analyse und Profilbildung einzuholen, wo dies angemessen ist.

- Transparent zu machen, welche Daten erhoben werden, wie die Daten verarbeitet werden, für welche Zwecke sie genutzt werden und ob die Daten an Dritte übermittelt werden oder nicht.

- Den Betroffenen angemessene Auskunft über die über sie gespeicherten Daten und über Informationen und sie betreffende Entscheidungen zu geben. Betroffene sollen auch über die Quellen der verschiedenen personenbezogenen Daten informiert werden und, wo dies angemessen ist, berechtigt sein, ihre Daten zu berichtigen und effektive Werkzeuge zu deren Kontrolle zu erhalten.

- Wo dies angemessen ist, den Betroffenen Auskunft über die wichtigen Faktoren und Kriterien für Entscheidungen (Algorithmen) zu gewähren, die als Basis für die Entwicklung des Profils genutzt wurden. Solche Informationen sollten in einem klaren und verständlichen Format dargestellt werden.

- Eine Vorabkontrolle (Privacy Impact Assessment) ist durchzuführen, besonders, wenn die Analyse von Big Data eine neue oder unerwartete Nutzung personenbezogener Daten beinhaltet.

- Big Data-Technologien nach den Prinzipien des „Privacy by Design“ zu entwickeln und zu nutzen.

- Zu prüfen, wo die Nutzung anonymisierter Daten den Schutz der Privatsphäre verbessern kann. Anonymisierung kann bei der Bewältigung der Risiken für die Privatsphäre helfen, die mit Big Data-Analysen zusammenhängen, aber nur, wenn die Anonymisierung angemessen entwickelt und gehandhabt wird. Über die optimale Lösung zur Anonymisierung der Daten sollte fallweise entschieden werden, möglicherweise durch Kombination verschiedener Techniken.

- Bei der Weitergabe oder Publikation pseudonymisierter oder in anderer Weise indirekt identifizierbarer Datensätze große Vorsicht walten zu lassen und in Übereinstimmung mit dem anwendbaren Datenschutzrecht zu handeln. Wenn die Daten hinreichend Details enthalten, mit anderen Datensätzen verknüpft werden können oder personenbezogene Daten enthalten, sollte der Zugang beschränkt und sorgfältig kontrolliert werden.

- Nachzuweisen, dass Entscheidungen über die Nutzung von Big Data fair, transparent und verantwortlich sind. Im Zusammenhang mit der Nutzung von Daten für Profilbildungszwecke erfordern sowohl die Profile als auch die zugrundeliegenden Algorithmen ständige Überprüfung. Dies verlangt regelmäßige Untersuchungen, um nachzuweisen, ob die Ergebnisse der Profilbildung verantwortlich, fair und ethisch und vereinbar und proportional zu den Zwecken sind, für die die Profile genutzt werden. Ungerechtigkeiten für Betroffene aufgrund vollautomatischer falsch-positiver oder falsch-negativer Ergebnisse sollten vermieden werden und es sollte stets eine manuelle Überprüfung von Ergebnissen mit signifikanten Auswirkungen auf Betroffene verfügbar sein.

Erklärung von Mauritius zum Internet der Dinge

(Balaclava, Mauritius – 14. Oktober 2014)

Das Internet der Dinge wird bleiben. Immer mehr Gegenstände sind mit dem Internet verbunden und in der Lage, miteinander zu kommunizieren, manchmal ohne dass die Nutzenden dies bemerken. Diese Gegenstände können unser Leben sehr viel einfacher machen. Zum Beispiel bei der Gesundheitsversorgung, beim Transport oder der Energieversorgung können die verbundenen Gegenstände die Art und Weise verändern, mit der wir etwas erledigen. Das Internet der Dinge kann allerdings auch intime Details über das Handeln und die Bewegungen der Eigentümer von Gegenständen mithilfe der in ihnen enthaltenen Sensoren offenbaren.

Selbstbestimmung ist ein unveräußerliches Recht aller Menschen. Die persönliche Entwicklung sollte nicht dadurch festgelegt werden, was Unternehmen und Regierungen über den Einzelnen wissen. Die Ausbreitung des Internets der Dinge vergrößert allerdings das Risiko, dass dies geschehen wird. Die versammelten Beauftragten für Datenschutz und Privatsphäre haben deshalb die Möglichkeiten des Internets der Dinge und seine Konsequenzen während der 36. Internationalen

Datenschutzkonferenz diskutiert, die in Balaclava, Mauritius am 13./14. Oktober 2014 stattfand. Vier Redner, die sowohl den wirtschaftlichen Sektor als auch die Wissenschaft repräsentierten, stellten den Beauftragten die positiven Veränderungen wie auch die Risiken vor, die das Internet der Dinge in unser tägliches Leben bringen kann. Die Redner gaben außerdem einen Überblick darüber, was getan werden muss, um den weiteren Schutz unserer personenbezogenen Daten wie auch unseres Privatlebens sicherzustellen.

Die anschließende Diskussion führte zu den folgenden Empfehlungen:

- Die beim Internet der Dinge verwendeten Sensoren erzeugen Daten in hoher Quantität, Qualität und Sensitivität. Dies bedeutet, dass sehr viel weiterreichende und sensitivere Folgerungen gezogen werden können und die Herstellung eines Personenbezugs wahrscheinlicher ist als dessen Vermeidung. Angesichts der Tatsache, dass die Personenbeziehbarkeit und der Datenschutz im Zusammenhang mit „Big Data“ an sich schon eine große Herausforderung sind, ist es deutlich, dass große Datenmengen, die von Gegenständen im Internet der Dinge gewonnen werden, diese Herausforderungen um ein Vielfaches vergrößern. Deshalb sollten solche Daten als personenbezogen angesehen werden.

- Obwohl für viele Unternehmen das Geschäftsmodell noch unbekannt ist, liegt der Wert des Internets der Dinge eindeutig nicht nur in den Geräten selbst. Das finanzielle Interesse liegt in den neuen Diensten im Zusammenhang mit dem Internet der Dinge und in den Daten.

- Jeder, der heute lebt, wird erkennen, dass Konnektivität allgegenwärtig ist. Dies mag noch mehr der Fall sein für die junge und zukünftige Generation, die sich keine Welt ohne Vernetzung vorstellen können. Es sollte aber nicht allein ihre Aufgabe sein, ob ihre Daten geschützt werden oder nicht. Es ist eine gemeinsame Verantwortung aller Handelnden in der Gesellschaft, damit das Vertrauen in vernetzte Systeme aufrechterhalten werden kann. Dafür ist Transparenz von entscheidender Bedeutung: Wer Dienstleistungen im Internet der Dinge anbietet, sollte klar sagen, welche Daten er sammelt, für welche Zwecke und wie lange diese Daten gespeichert werden. Er sollte Überraschungen für Verbraucher ausschließen. Beim Kauf von Gegenständen des Internets der Dinge oder entsprechender Programme sollte eine angemessene ausreichende und verständliche Information zur Verfügung stehen. Gegenwärtige Datenschutzerklärungen vermitteln nicht immer die Information in einer klaren, verständlichen Weise. Einwilligungen, die auf der Basis solcher Datenschutzerklärungen erteilt werden, können kaum als informierte Einwilligungen angesehen werden. Unternehmen müssen ihre Herangehensweise grundlegend verändern, damit Datenschutzerklärungen nicht länger in erster Linie dem Zweck dienen, sie vor Klagen zu schützen.

- Die Datenverarbeitung beginnt in dem Moment der Datenerhebung. Alle Schutzmaßnahmen sollten ab diesem Zeitpunkt greifen. Wir ermutigen zur Entwicklung von Technologien, die neue Wege der Einbeziehung von Datenschutz und Verbraucherschutz von Anfang an ermöglichen. „Privacy by Design and Default" sollte nicht länger als etwas Abseitiges betrachtet werden. Beide Prinzipien sollten ein wesentliches Verkaufsargument für innovative Technologien werden.

- Das Internet der Dinge wirft auch wesentliche Sicherheitsrisiken auf, die beherrscht werden müssen. Eine einfache Firewall reicht längst nicht mehr aus. Ein Weg, um das Risiko für Betroffene zu begrenzen, liegt darin, dass man die Datenverarbeitung auf das Endgerät selbst beschränkt (lokale Verarbeitung). Wenn dies nicht möglich ist, sollten Unternehmen Ende-zu-Ende-Verschlüsselung vorsehen, um die Daten vor ungerechtfertigter Einwirkung oder Manipulation zu schützen.

- Die Datenschutz- und Privatsphäre-Behörden werden weiterhin die Entwicklungen beim Internet der Dinge beobachten. Sie machen es sich zur Aufgabe, die Befolgung der Datenschutzgesetze in ihren jeweiligen Ländern sicherzustellen, ebenso wie die Einhaltung der international akzeptierten Prinzipien. Wenn Rechtsverstöße festgestellt werden, werden sie angemessene Sanktionsmaßnahmen ergreifen, entweder einseitig oder durch internationale Zusammenarbeit.

- Angesichts der großen Herausforderungen, denen sich die Entwickler im Internet der Dinge, die Datenschutzbehörden und die Betroffenen gegenübersehen, sollten sich alle Beteiligten an einer starken, aktiven und konstruktiven Debatte zu den Konsequenzen des Internets der Dinge und der aus ihm gewonnen großen Datenmenge beteiligen, um das Bewusstsein für die zu treffenden Entscheidungen zu erhöhen.

Jacob Kohnstamm
(Vorsitzender des Exekutivkomitees der Internationalen Datenschutzkonferenz)

Drudeisha Madhub
(Vorsitzende der Datenschutzbehörde von Mauritius)

Entschließung zum Datenschutz im digitalen Zeitalter[1]

Die 36. Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre

erinnert an die Entschließung der 35. Konferenz zur Verankerung des Datenschutzes und des Schutzes der Privatsphäre im Völkerrecht;

verweist auf die fortgesetzten Enthüllungen über die Existenz und die Nutzung massenhafter elektronischer Überwachungsprogramme seit dem Sommer 2013;

ist sich dessen bewusst, dass nicht alle Mitglieder der Konferenz über Zuständigkeiten im Bereich der Nachrichtendienste verfügen;

betont die grundlegende Bedeutung des Rechts auf Privatsphäre und Datenschutz;

nimmt zur Kenntnis und unterstützt die Resolution der Vollversammlung der Vereinten Nationen 68/167, mit der unterstrichen wurde, dass dieselben Rechte, die Menschen offline haben, auch online geschützt sein müssen, einschließlich des Rechts auf Privatsphäre;

nimmt die Berichte des United States Privacy and Civil Liberties Oversight über die Programme nach Section 215 des USA Patriot Act und Section 702 des USA Foreign Intelligence Surveillance Act *zur Kenntnis*;

ist sich der Stellungnahme der Art. 29-Datenschutzgruppe zur Überwachung von elektronischer Kommunikation für Zwecke der Nachrichtendienste und der nationalen Sicherheit *bewusst*;

begrüßt mit großem Interesse den Prüfbericht des Büros des Hochkommissars der Vereinten Nationen für Menschenrechte zum „Recht auf Privatsphäre im digitalen Zeitalter“;

1. betont seine Bereitschaft, sich am Dialog aller Interessensträger zu beteiligen, der im Bericht des Büros des Hochkommissars vorgeschlagen wird, um die Herausforderungen bezüglich des Rechts auf Privatsphäre und Datenschutz im Zusammenhang mit modernen Kommunikationstechnologien zu bewältigen;

2. beauftragt das Exekutivkomitee, die Konferenz bei diesem Dialog zu vertreten;

[1] Die US Federal Trade Commission enthält sich bei dieser Entschließung, die sich auf Angelegenheiten außerhalb ihrer Zuständigkeit bezieht.

3. fordert die Mitglieder der Konferenz auf, sich dafür einzusetzen, dass jedes elektronische Überwachungsprogramm zumindest den allgemeinen Datenschutz- und Privatsphäre-Prinzipien genügt, die in den Grundsätzen von Madrid aus dem Jahre 2009, dem Internationalen Pakt über bürgerliche und politische Rechte, der Konvention des Europarats über den Datenschutz im Zusammenhang mit der automatischen Verarbeitung von personenbezogenen Daten und seinem Zusatzprotokoll und den anderen internationalen Abkommen niedergelegt sind, und sich an nationalen und internationalen Dialogen zwischen den interessierten Stellen zu diesem Thema zu beteiligen;

4. fordert die Mitglieder der Konferenz auf, die Übereinstimmung jedes elektronischen Überwachungsprogramms mit diesen allgemeinen Grundsätzen des Datenschutzes und der Privatsphäre sicherzustellen, falls nötig, in dem sie sich für effektivere Befugnisse einsetzen, um den Herausforderungen und Risiken der Überwachung zu begegnen;

5. lädt seine Mitglieder ein, alle Informationen über massenhafte elektronische Überwachungsprogramme wie auch über vorbildliche Verfahrensweisen zur Kontrolle solcher Programme dem Exekutivkomitee zur weiteren Verbreitung unter den Mitgliedern und Beobachtern der Internationalen Konferenz mitzuteilen.

VII. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 55. Sitzung am 5./6. Mai 2014 in Skopje, Mazedonien

Arbeitspapier zu Big Data und Datenschutz: Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen

– Übersetzung –

Einleitung[1]

1. Der Begriff „Big Data" bezeichnet die enorme Zunahme von Zugriffen auf Informationen und deren automatisierte Nutzung[2]. Er bezieht sich auf die gigantischen Mengen digitaler Daten, über die Unternehmen, Behörden und andere große Organisationen verfügen und die sie mit Hilfe von Algorithmen umfassend analysieren[3].

2. Big Data gefährdet zentrale Datenschutzgrundsätze. Teilweise wird behauptet, dass eine Durchsetzung dieser Grundsätze in Zeiten von Big Data überhaupt nicht möglich sei[4]. Nach dieser Ansicht muss Datenschutz in erster Linie dadurch gewährleistet werden, dass Unternehmen eindeutig und umfassend über die Art und Weise des Umgangs mit personenbezogenen Daten informieren. Die Arbeitsgruppe ist jedoch der Meinung, dass der Schutz der Privatsphäre in Zeiten der Erfassung immer größerer Mengen personenbezogener Daten wichtiger denn je ist[5]. Die Datenschutzgrundsätze sind der

[1] Dieses Arbeitspapier enthält Hinweise zu gesetzlichen Bestimmungen, die möglicherweise nicht in allen in der Arbeitsgruppe repräsentierten Rechtssystemen enthalten sind.

[2] Vgl. White (2012): Big Data ist der Begriff für eine Datensammlung, die so groß und komplex ist, dass es schwierig wird, sie mit den vorhandenen Werkzeugen für die Verwaltung von Datenbanken oder traditionellen Datenverarbeitungsanwendungen zu verarbeiten.

[3] Vgl. Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung, S. 35 [der engl. Fassung]

[4] Vgl. z. B.: Tene, Omer und Polonetsky, Jules (2012) Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, im Erscheinen, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364; World Economic Forum (2013), Unlocking the Value of Personal Data: From Collection to Usage, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf; Cate, Fred H. und Mayer-Schönberger, Viktor (2013), Tomorrow's privacy. Notice and consent in a world of Big Data, International Data Privacy Law, 2013, Vol. 3, No. 2.

[5] Ähnliche Ansichten werden unter anderem von der Kommissarin der Federal Trade Commission Julie Brill (2013) geäußert: „Wir können das Potential von Big Data freilegen und seine Vorzüge genießen. Gleichzeitig können wir Datenschutzgrundsätze beachten, die den Konsumenten schützen."; in: „Reclaim Your Name: Privacy in the Age of Big Data", Sloan Cyber Security Lecture, Polytechnic Institute of NYU, October 23, 2013, und von Ann Cavoukian, Alexander Dix und Khaled El Emam (2014), „The Unintended Consequences of Privacy Paternalism", March 5, 2014, http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

Garant dafür, dass wir nicht einer umfassenden Profilbildung in einem ständig anwachsenden Gefüge neuer Zusammenhänge unterworfen werden. Eine Verwässerung zentraler Datenschutzgrundsätze in Verbindung mit einer immer umfangreicheren Nutzung von Big Data kann sich nachteilig auf den Schutz der Privatsphäre und auf andere wichtige gesellschaftliche Werte wie beispielsweise die Meinungsfreiheit und die Bedingungen für den Austausch von Ideen auswirken.

3. Die OECD und die Europäische Datenschutzrichtlinie haben in einigen Kernprinzipien festgelegt, wie personenbezogene Daten angemessen, korrekt und rechtmäßig verarbeitet werden dürfen[6]. Insbesondere die folgenden Grundsätze sind für Big Data von Relevanz: Zweckbeschränkung, Erforderlichkeit und Datenminimierung, Vollständigkeit und Qualität, Transparenz und das Recht auf Auskunft über personenbezogene Daten[7].

Geltungsbereich

4. Dieses Arbeitspapier stellt die mit Big Data einhergehenden Gefahren für den Datenschutz insbesondere auf dem Gebiet der Telekommunikation in den Mittelpunkt, damit diese von Datenschutzbehörden und anderen Interessengruppen berücksichtigt werden. Es richtet sich an Entscheidungsträger, Behörden, Wirtschaftsunternehmen und Bürger.

5. Big Data bringt ein breites Spektrum von Herausforderungen mit sich, von denen etliche, wie beispielsweise die Gefahr der Re-Identifizierung, bereits für sich allein genommen ein eigenes Thema umfangreicher Berichte darstellen könnten. Dieses Arbeitspapier befasst sich jedoch nicht im Detail mit einzelnen technischen Problemen, sondern mit den zentralen Gefahren für den Schutz der Privatsphäre.

Hintergrund

6. Daten sind allgegenwärtig. Weltweit nimmt die Datenmenge von Jahr zu Jahr um 50 % zu. Allein in den letzten beiden Jahren wurden 90 % aller weltweit vorhandenen Daten erzeugt[8]; die meisten davon durch Verbraucher und

[6] Vgl. die OECD Richtlinien über den Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (2013) und Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Entsprechende Grundsätze sind auch in der Empfehlung CM/Rec(2010)13 des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling niedergelegt.

[7] Die entsprechenden Grundsätze in den OECD-Richtlinien sind: Der Grundsatz der Beschränkung der Datenerhebung, der Grundsatz der Zweckbestimmung, der Grundsatz der Datenqualität, der Grundsatz der Nutzungsbeschränkung und der Grundsatz der Beteiligung des Einzelnen.

[8] http://www-01.ibm.com/software/data/bigdata/

deren Interaktion mit internetbasierten Diensten. Mit dem Aufkommen des „Internets der Dinge“[9] werden weitere Datenströme hinzukommen. Man schätzt, dass im Jahr 2015 über 50 Milliarden Sensoren existieren werden[10]. Diese werden Informationen darüber, wie Menschen mit den sie umgebenden Dingen interagieren, in Cloud-Computing-Dienste hochladen. Dies kann zu Veränderungen von Märkten und Geschäftsmodellen führen.

7. Es steht außer Frage, dass die Fähigkeit zur Speicherung und Analyse enormer Datenmengen der Gesellschaft auf unterschiedlichste Weise nützen wird[11]. Big Data wird bereits heute in einigem Umfang zur Analyse von Daten mit dem Ziel der Bestimmung und Vorhersage von Trends und Korrelationen genutzt. Mit Hilfe von Big Data können beispielsweise die Ausbreitung von Epidemien vorhergesagt, schwere Nebenwirkungen von Medikamenten festgestellt und die Umweltbelastung in großen Städten bekämpft werden. Analysen dieser Art stellen per se keine Gefährdung der Privatsphäre dar, sofern die Daten hinreichend anonym sind (das Konzept der Anonymisierung wird in diesem Papier an anderer Stelle ausführlich behandelt). Darüber hinaus verwenden einige Big-Data-Analysen überhaupt keine personenbezogenen Daten, beispielsweise Wetterdatenanalysen oder Analysen der Sensordaten von Ölbohrinseln.

8. Big Data kann aber auch dergestalt eingesetzt werden, dass Einzelpersonen direkt betroffen sind. So gibt es Techniken zur Erstellung von Profilen und zur Vorhersage des Verhaltens von Personen und Personengruppen durch Zusammenstellung und Analyse von aus einer Vielzahl unterschiedlicher Quellen stammenden personenbezogenen Daten. Selbst wenn diese Informationen zusammengefasst und anonymisiert werden, kann das Ergebnis der Analyse immer noch Folgen für den Einzelnen haben.

9. „Personenbezogene Daten“ sind alle sich auf eine identifizierte bzw. identifizierbare Person beziehenden Informationen[12]. IP-Adressen, Mobiltelefonnummern, RFID-Tags und UDID-Nummern sind Beispiele für als personenbezogene Daten geltende eindeutige Kennungen[13]. Daten, die Informationen über Gewohnheiten und Interessen eindeutig identifizierter Personen geben,

[9] „Internet der Dinge“ bezeichnet die Entwicklung einer steigenden Anzahl von Gegenständen und Personen, die mit Sensoren ausgestattet sind, die drahtlos miteinander in Netzwerken kommunizieren.

[10] The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, Cisco White Paper, 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[11] McKinsey Global Institute (2011), „Big Data: The next frontier for innovation, competition, and productivity“ http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

[12] So definiert in den OECD-Richtlinien über den Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, und in der Europäischen Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[13] Stellungnahme 04/2007 der Artikel 29-Datenschutzgruppe zum Begriff „personenbezogene Daten“.

sind für Unternehmen und Regierungen von großem Interesse. Die Industrie entwickelt daher ständig neue, diesem Ziel dienende Techniken wie etwa das Device Fingerprinting. Dadurch wächst der Umfang von als personenbezogene Daten definierten eindeutigen Kennungen beständig.

10. Die „Wertschöpfungskette" von Big Data umfasst mehrere Schritte, angefangen bei der Datenerhebung bis hin zu deren Speicherung und Verdichtung, ihrer Analyse sowie die Nutzung der Analyseergebnisse (siehe die Darstellung der Wertschöpfungskette am Ende des Dokuments). Auf diese einzelnen Schritte wird im Folgenden eingegangen.

11. Den ersten Schritt der Wertschöpfungskette bildet die *Datenerhebung*. Beispiele potenzieller Quellen personenbezogener Daten sind unter anderem Mobiltelefon-Apps, Smart-Grids, Straßenmaut-Transponder in Fahrzeugen, Patientenakten, Standortdaten, soziale Netzwerke, Flugzeugpassagierdaten, öffentliche Verzeichnisse, Kundenbindungsprogramme, Genomsequenzen, Einkaufshistorien etc. Aufgrund der zunehmenden Verbreitung der Sensortechnologie können Informationen von einer Vielzahl mobiler Geräte, darunter intelligente Zahnbürsten, Regenschirme, Kühlschränke, Schuhe, Fernsehgeräte etc. erhoben werden. Derartige Datenquellen können Informationen liefern, die potenziell sehr viel über die Lebensweise jedes Einzelnen preisgeben könnten.

12. Personenbezogene Daten können beispielsweise auf die folgende Weise *erhoben* werden:

    i. Personenbezogene Daten können vom Bürger selbst (beispielsweise durch Veröffentlichen persönlicher Angaben in sozialen Netzwerken) übermittelt werden.

    ii. Personenbezogene Daten können als Voraussetzung für die Erbringung einer Dienstleistung erhoben werden.

    iii. Personenbezogene Daten können aufgrund gesetzlicher Vorschriften erhoben werden.

    iv. Personenbezogene Daten können in Verbindung mit der Inanspruchnahme spezifischer Dienstleistungen (beispielsweise Transaktions- und Standortdaten von Mautzahlstellen) *automatisiert* erhoben werden. Diese Datenerhebung kann auch *ohne Wissen des Betroffenen* erfolgen (beispielsweise bei der Erhebung von Daten aus Hot Spots an Flughäfen zur Verfolgung von Reisenden[14]).

[14] http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

v. Personenbezogene Daten können durch Verarbeitung und Analyse von für frühere und andere Zwecke erhobene Daten *abgeleitet* werden. Weiterhin können personenbezogene Daten aus verschiedenen, vermeintlich anonymen Datensätzen abgeleitet werden.

vi. Personenbezogene Daten (beispielsweise Kundendaten [Costumer Relationship Management]) können aus externen Quellen *hinzugefügt werden*, um (zuvor erhobene) Datenbestände zu erweitern.

vii. Personenbezogene Daten (beispielsweise (detaillierte) Kundendatensätze) können an externe Stellen *weitergegeben werden*, um (personenbezogene) Datenbestände von Partnerunternehmen anzureichern.

13. Im Zusammenhang mit Big Data sind über Internetnutzer gesammelte Informationen äußerst attraktiv, da sie detaillierte Informationen über deren Interessen, Netzwerke, Gewohnheiten und Verhaltensmuster enthalten können. Derartige Informationen können explizit (beispielsweise bei der Registrierung eines sozialen Profils im Internet) oder eher verdeckt durch den Einsatz verschiedener Tracking-Technologien erhoben werden[15].

14. Der zweite Schritt ist die *Verdichtung und Speicherung*[16] der Daten nach ihrer Erhebung. Einige Stellen verdichten und anonymisieren die Daten vor deren Speicherung; andere speichern Daten zusammen mit personenbezogenen Kennungen. Die enorme Steigerung der Speicher- und Analyseleistung bei immer niedrigeren Kosten bedeutet, dass Big Data nicht mehr einigen wenigen Branchenriesen vorbehalten ist. Big Data ist heute ein Werkzeug, das sowohl kleinen als auch großen Unternehmen aller Wirtschaftsbereiche zugänglich ist. Die Big Data-Technologie bedeutet eine Abkehr vom bisherigen Denken zur Datenspeicherung und -verarbeitung mithilfe von Großrechenanlagen. Dank neuer Technologien ist es möglich, neue und unstrukturierte Datenquellen zu verarbeiten und daraus Wert zu schöpfen.

15. Den dritten Schritt der Wertschöpfungskette stellen der Abgleich *und die Analyse* der erhobenen und gespeicherten Daten dar. Ein zentrales Element der Wertschöpfung dieser Stufe ist das Zusammenführen von Daten aus einer Vielzahl verschiedener Quellen zur Herstellung von Profilen sowie der Einsatz von Analysewerkzeugen zur Ableitung von ansonsten nicht verfügbaren Informationen. Die Nutzer von Big Data können entweder nur ihre eigenen

[15] Innerhalb der EU ist jetzt für den Einsatz bestimmter Cookies eine Einwilligung erforderlich, um das Sammeln von Daten für den Nutzer transparent zu machen und sicherzustellen, dass dieser mehr Kontrolle darüber erlangt.

[16] Aggregierung ist in diesem Zusammenhang zu verstehen als das Sich-Verschaffen von Erkenntnissen über eine Gruppe von Personen, nicht über Einzelpersonen. Aggregierung beinhaltet die Darstellung der Gesamtheit der Daten. Daten, die einer Einzelperson zugeordnet werden könnten oder diese identifizieren würden, werden nicht angezeigt. Abweichende Werte werden oft verborgen, indem sie als „unclear" dargestellt oder gelöscht werden. Ein Beispiel für Aggregierung ist das Verwenden von Durchschnittswerten.

internen Unternehmensdaten zusammentragen oder Daten von Dritten (oder aus öffentlich zugänglichen Quellen) erwerben und diese mit eigenen Daten verbinden. Einige Beispiele von Analysetechniken in Verbindung mit Big Data sind Data Mining, maschinelles Lernen, soziale Netzwerkanalyse, prädiktive Analyse, „Sensemaking", die Verarbeitung natürlicher Sprache und Visualisierung.

16. Der vierte Schritt der Wertschöpfungskette ist die *Nutzung* der Ergebnisse der Analyse. Big Data kann auf vielfältige Weise genutzt werden. Immer mehr Akteure, darunter beispielsweise Banken, Versicherungen, Ratingagenturen, Arbeitgeber sowie die Polizei sind im Interesse besserer und fundierterer Entscheidungen an einer Nutzung des durch die Analyse von Big Data erworbenen Wissens interessiert.

17. Eine Vielzahl von Interessengruppen ist an der gesamten Big-Data-Wertschöpfungskette beteiligt (siehe Abb.1 der Anlage). Einige Interessengruppen sind lediglich an ausgewählten Teilen der Wertschöpfungskette beteiligt. So nutzen beispielsweise Datenmakler personenbezogene Daten in der Regel nicht selbst, sondern verarbeiten und verkaufen sie lediglich weiter. Andere Interessengruppen können demgegenüber an sämtlichen Schritten der Wertschöpfungskette beteiligt sein. Ein Einzelhändler kann beispielsweise personenbezogene Daten mit Hilfe eines Kundenbindungsprogramms erheben, diese sodann speichern und verdichten und schließlich in seinem eigenen Geschäftsmodell verarbeiten und nutzen[17].

18. Personenbezogene Daten sind schon seit langer Zeit ein begehrtes Wirtschaftsgut und Anlass für die Entwicklung neuer, internetbasierter Dienstleistungen. Internetnutzer erhalten in der Regel Dienstleistungen kostenfrei, indem sie mit ihren personenbezogenen Daten dafür zahlen. Durch Big Data und die zunehmende Verbreitung des „Internets der Dinge" wird der Markt für personenbezogene Daten an Volumen zunehmen und möglicherweise auch neue Wirtschaftsbereiche erschließen. So könnten beispielsweise intelligente Schuhe mit Sensoren gratis angeboten werden, wenn der Benutzer der Erfassung und Analyse der Daten seiner Laufgewohnheiten zustimmt. Ein Zahnarzt könnte seinen Patienten (vom Hersteller gratis zur Verfügung gestellte) intelligente Zahnbürsten kostenfrei überlassen, wenn die Patienten die von der Zahnbürste erhobenen Daten diversen interessierten Unternehmen zur Nutzung überlassen. Neue Unternehmen und Geschäftsmodelle werden entstehen, um den Mehrwert der gigantischen Mengen in einer ständig wachsenden Zahl von Situationen entstehenden personenbezogenen Daten abzuschöpfen.

[17] OECD (2013), „Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing, http://dx.doi.org/10.1787/5k486qtxldmq-en

Konsequenzen für den Schutz der Privatsphäre

19. Anhand der obigen Darstellung lassen sich die folgenden zentralen Herausforderungen für den Schutz der Privatsphäre durch die Nutzung von Big Data formulieren.

Datennutzung für neue Zwecke:

20. Big Data bedeutet zu weiten Teilen die Wiederverwendung von Daten. Dies stellt insoweit ein Problem für den Schutz personenbezogener Daten dar, als eine Nutzung erhobener Daten nicht für Zwecke zulässig ist, die *nicht* mit dem ursprünglichen Zweck der Erhebung *vereinbar* sind[18]. Das Potenzial von Big Data, durch die Aufbereitung immer größerer Datensätze wertvolles Wissen zu erschließen, stellt diesen Grundsatz der Zweckbindung infrage. Dieser Grundsatz besagt, dass ein Unternehmen, das erhobene personenbezogene Daten als Grundlage für vorausschauende Analysen nutzt, dafür Sorge zu tragen hat, dass die Analyse mit dem ursprünglichen Zweck der Erhebung dieser Daten vereinbar ist. Eine Person, die Daten an Dritte weitergibt, stellt bestimmte natürliche Erwartungen an die Zwecke, für die diese Daten genutzt werden. Man überlässt einem Unternehmen oder dem Staat keine Informationen, wenn diese damit nach Belieben verfahren. Dies könnte eine erhebliche Herausforderung für die kommerzielle Nutzung von Big Data darstellen.

Datenmaximierung:

21. Big Data bedeutet Datenmaximierung. Big Data ist im Wesentlichen der absolute Gegenentwurf zu den Datenschutzgrundsätzen von Erforderlichkeit und Datenminimierung[19]. Diese Grundsätze sollen gewährleisten, dass nicht mehr personenbezogene Informationen erhoben und gespeichert werden, als für die Erreichung eindeutig definierter Zwecke erforderlich sind. Sobald die Daten nicht mehr für den ursprünglichen Zweck benötigt werden, sind sie zu löschen. Big Data bedeutet eine neue Betrachtungsweise von Daten, bei der diese einen Wert an sich erhalten. Der Wert von Daten wird mit ihren potenziellen *zukünftigen* Nutzungen verbunden. Diese Sicht auf Daten könnte den datenschutzrechtlichen Grundsatz infrage stellen, der besagt, dass die Verarbeitung von Daten für die zum Zeitpunkt ihrer Erfassung definierten und erklärten Zwecke angemessen, erforderlich und nicht übermäßig sein muss. Sie könnte auch den Wunsch und die Motivation der für die Datenverarbeitung verantwortlichen Stellen hinsichtlich des Löschens von Da-

[18] Vgl. Artikel 6 Abs. 1 Bst. b der Richtlinie 95/46/EG.

[19] Artikel 6 Abs. 1 Bst. c der Richtlinie 95/46/EG.

ten beeinflussen. Es ist denkbar, dass private Unternehmen und öffentliche Einrichtungen abgeneigt sind, Daten zu löschen, die sich irgendwann in der Zukunft als Quelle neuer Erkenntnisse und Einkünfte erweisen könnten. Die immer weiter verbreitete Nutzung von Big Data wird es den Datenschutzbehörden zunehmend erschweren, die Verpflichtung zur Löschung von Daten durchzusetzen.

Mangelnde Transparenz:

22. Das Recht auf Auskunft über die eigenen personenbezogenen Daten sowie über deren Verarbeitung ist ein wichtiger Grundsatz des Datenschutzes. Mangelnde Offenheit und fehlende Informationen hinsichtlich der Art der Erhebung und Nutzung von Daten können dazu führen, dass die Betroffenen Opfer von Entscheidungen werden, die für sie nicht nachvollziehbar sind und auf die sie keinen Einfluss haben. So weiß beispielsweise der durchschnittliche Internetnutzer nur sehr wenig darüber, wie der Online-Werbemarkt funktioniert und wie dort seine personenbezogenen Daten von einem breiten Spektrum kommerzieller Akteure gesammelt und genutzt werden[20]. Die meisten Bürger wissen nichts über etliche der auf diesem Markt tätigen Akteure, insbesondere über Datenmakler und Analysefirmen[21], wodurch die Wahrnehmung des Rechts des Einzelnen erschwert wird, Auskunft über seine Daten zu verlangen.

Aufdeckung sensitiver Informationen durch Kombination von Daten:

23. Ein bedenklicher Aspekt in Verbindung mit der Analyse von Big Data besteht darin, dass die Kombination erfasster Teilinformationen, die jeweils für sich genommen nicht notwendigerweise sensibel sind, zu einem sensitiven Ergebnis führen kann[22]. Mithilfe von Big-Data-Werkzeugen ist es möglich, Muster zu erkennen, die eine Vorhersage von Präferenzen Betroffener ermöglichen, beispielsweise in Bezug auf Gesundheit, politische Ansichten oder sexuelle Orientierung. Dies sind besonders schützenswerte

[20] Turow, Joseph (2011): „The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth, Yale University Press", New Haven & London

[21] Acxiom ist einer der großen Datenmakler. Es handelt sich um ein US-Unternehmen, das für seine Klienten deren Kunden- und Firmendaten sammelt, analysiert und sie bei gezielten Werbekampagnen etc. unterstützt. Der Kundenstamm in den Vereinigten Staaten besteht vorwiegend aus Unternehmen aus den Bereichen Finanzwesen, Versicherungen, Direktmarketing, Medien, Vertrieb, Technologie, Gesundheit, Telekommunikation und Behörden. Das Unternehmen ist einer der weltweit größten Verarbeiter von Kundeninformationen. Es verfügt angeblich über 20 Milliarden Datensätze über Kunden und Informationen über 96 Prozent aller Haushalte in den Vereinigten Staaten.

[22] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all

Informationen. Die verarbeitenden Stellen müssen sich dieses Risikos bei der Kombination und Analyse von Daten bewusst sein[23].

Risiko der Re-Identifizierung:

24. Eines der größten Risiken in Verbindung mit der Analyse von Big Data ist das der Re-Identifizierung. Durch die Zusammenstellung von Daten aus verschiedenen Quellen besteht das Risiko, dass eine Person anhand von Datensätzen identifiziert werden kann, die auf den ersten Blick anonym zu sein scheinen. Dies beeinträchtigt die Effektivität der Anonymisierung als Methode zur Verhinderung von Problemen für die Privatsphäre in Verbindung mit Profilbildung und mit anderen Datenanalysen[24, 25]. Das Risiko der Re-Identifizierung lässt sich dadurch verringern, dass gewährleistet wird, dass zur Analyse ausschließlich anonymisierte Daten verwendet werden. Allerdings kann nicht immer ohne Weiteres festgestellt werden, ob ein Datensatz ausreichend und belastbar anonymisiert ist. Dies kann aus zwei Gründen schwierig sein:

    - Erstens ist der Begriff „identifizieren" – und damit auch „anonymisieren" – komplex, weil eine Person auf viele verschiedene Arten identifiziert werden kann[26]. Hierzu gehören die direkte Identifizierung, bei der die Person anhand einer einzigen Datenquelle (beispielsweise einer Liste mit ihrem vollständigen Namen) eindeutig identifiziert wird, sowie die indirekte Identifizierung, bei der zwei oder mehr Datenquellen kombiniert werden müssen, um eine Identifizierung zu ermöglichen.

    - Zweitens kann ein Unternehmen, das einen vermeintlich anonymisierten Datensatz verwendet, nicht mit letzter Sicherheit sagen, ob nicht noch weitere Datensätze existieren, aufgrund derer es einem Dritten möglich wird, Einzelpersonen in dem anonymisierten Datenbestand zu identifizieren. Selbst nach Löschung der identifizierenden Informationen ist es unter

[23] Ein häufig zur Verdeutlichung dieses Problems herangezogenes Beispiel ist der sogenannte „Schwangerschafts-Algorithmus" der US-Kette Target. Target hat einen Algorithmus entwickelt, der auf der Grundlage der von ihnen gekauften Produkte bestimmen konnte, welche Kundinnen schwanger waren. Target sendete dann Gutscheine für „Schwangerschaftsprodukte" an diese Kundinnen. In einem Fall führte das Versenden dieser Gutscheine dazu, dass ein Vater auf Schwangerschaft seiner Tochter aufmerksam wurde, bevor diese die Möglichkeit hatte, ihn darüber zu unterrichten.

[24] Anonymisierung entsteht durch eine die Identifizierung irreversibel verhindernde Verarbeitung personenbezogener Daten, vgl. Richtlinie 95/46/EG. Anonymisierung wird zudem in internationalen Regelungsstandards wie ISO 29100 definiert als „Prozess, bei dem Informationen, die einer Person zugeordnet werden können, so modifiziert werden, dass diese Informationen weder direkt noch indirekt von dem Halter der Information allein oder im Zusammenwirken mit einer anderen Stelle eine Person identifizieren können." (ISO 29100:2011).

[25] In dem Arbeitspapier „Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar" (15./16. April 2013, Prag (Tschechische Republik)), werden die Herausforderungen im Zusammenhang mit der Re-Identifizierung als „Game-Changer" bezeichnet.

[26] Stellungnahme 05/2014 der Artikel 29-Datenschutzgruppe zu Anonymisierungstechniken

Umständen immer noch möglich, spezifische Informationen anhand von Verbindungen innerhalb verschiedener Sammlungen von Big Data einzelnen Personen zuzuordnen. Ein reales Beispiel hierfür enthält der Aufsatz „How to break anonymity of the Netflix Prize Dataset“[27].

Konsequenzen für die Informationssicherheit

25. Big Data bringt auch Probleme für die Informationssicherheit und damit möglicherweise auch für den Schutz der Privatsphäre mit sich. Beispiele für derartige Sicherheitsprobleme sind die Nutzung mehrerer Infrastrukturebenen zur Verarbeitung von Big Data, neue Infrastrukturtypen zur Bewältigung des enormen Datenstroms sowie die nicht skalierbare Verschlüsselung großer Datensätze. Darüber hinaus kann eine Verletzung des Schutzes personenbezogener Daten schwerwiegende Folgen haben, wenn sehr große Datenbestände gespeichert sind. Ein Unternehmen, das eine große Menge personenbezogener Daten erwirbt und speichert, muss ein verantwortungsvoller Verwalter dieser Informationen sein.

Unrichtige Daten:

26. Ein wichtiger Grundsatz des Datenschutzes besagt, dass Personen betreffende Entscheidungen auf zutreffenden Informationen basieren müssen. Die Anwendung leistungsfähiger Data-Mining-Techniken ist beispielsweise in der Versicherungswirtschaft und bei Ratingagenturen zunehmend beliebt. Big Data erleichtert die Nutzung eines weitaus größeren Spektrums sowie neuer Arten von Datenquellen bei der Erstellung von Bonitätsbeurteilungen und Risikoprofilen. Neue, auf die Nutzung von Big Data spezialisierte Ratingagenturen sind auf den Markt getreten. Diese Agenturen erstellen Profile von Personen auf der Grundlage von ausschließlich aus Onlinequellen bezogenen Informationen.

27. Entscheidungen aufgrund von Informationen zu treffen, die beispielsweise aus sozialen Medien gewonnen und zusammengestellt wurden, beinhaltet jedoch die Gefahr, dass diesen Entscheidungen ungenaue Informationen zugrunde liegen. Auf derartigen Informationen basierende Entscheidungen sind weniger transparent und nachprüfbar als auf der Grundlage von Informationen aus offiziellen Registern getroffene Entscheidungen. Eine Schwäche von Big-Data-Analysen liegt darin, dass der Kontext oftmals unberücksichtigt bleibt[28]. Selbst bei richtigen Daten können sich Probleme für die Pri-

[27] http://arxiv.org/abs/cs/0610105v1

[28] danah boyd und Kate Crawford sind zwei Forscherinnen, die die Wichtigkeit der Einbeziehung des Kontextes in Big Data-Analysen hervorgehoben haben. boyd, danah u. Crawford, Kate (2012), „Critical Questions for Big Data“, Information, Communication & Society 15:5, 662–679, http://dx.doi.org/10.1080/1369118X.2012.678878

vatsphäre dadurch ergeben, dass die Daten außerhalb ihres ursprünglichen Zusammenhangs verwendet werden. Eine Entscheidungsfindung aufgrund von für andere Zwecke gesammelten und in anderen Zusammenhängen erzeugten Informationen kann zu Ergebnissen führen, die der tatsächlichen Situation nicht gerecht werden. Es ist wichtig zu betonen, dass die Nutzung von für andere Zwecke bestimmte Informationen unter Datenschutzgesichtspunkten per se rechtswidrig ist, es sei denn, diese anderen Zwecke sind mit den ursprünglichen Zwecken vereinbar oder die Daten sind anonymisiert.

28. Transparenz, beispielsweise in Form des Rechts des Betroffenen auf Auskunft zu den über ihn verarbeiteten Informationen, ist eine Voraussetzung dafür, dass der Betroffene in der Lage ist, seine eigenen Interessen wahrzunehmen. Es ist ein zentraler Grundsatz des Datenschutzes, dass Betroffene die Berichtigung oder Löschung von nachweislich unrichtigen Informationen, Beurteilungen und Behauptungen verlangen können.

Ungleichgewicht der Kräfte:

29. Der Einzelne hat grundsätzlich kaum Einflussmöglichkeiten auf das Verhalten von Großunternehmen. Die extensive Nutzung von Big-Data-Analysen kann das Ungleichgewicht zwischen Großunternehmen und Verbrauchern noch weiter verstärken[29]. Es sind doch die Unternehmen, die personenbezogene Daten sammeln und in den Genuss des der Analyse und Verarbeitung dieser Informationen innewohnenden, ständig wachsenden Werts kommen, und nicht der Einzelne, von dem diese Informationen stammen. Die Datenverarbeitung kann sich vielmehr sogar zum Nachteil des Verbrauchers auswirken, indem sie ihn dem Risiko zukünftiger potenzieller Benachteiligungen (beispielsweise im Hinblick auf Beschäftigungschancen, Bankkredite oder Wahlmöglichkeiten bei Krankenversicherungen) aussetzt[30].

Datendeterminismus und Diskriminierung:

30. Die „Big-Data-Haltung" basiert auf der Annahme, dass man, je mehr Daten man sammelt und auf je mehr Daten man Zugriff hat, desto bessere, fundier-

[29] Vgl. Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung

[30] Die OECD hat diesem Thema ihre Aufmerksamkeit gewidmet und einen Bericht veröffentlicht, in dem auf die Methoden zur Schätzung des finanziellen Wertes personenbezogener Daten eingegangen wird. Nach diesem Bericht könnten die Methoden zur Bestimmung des Wertes personenbezogener Daten helfen, Transparenz zu gewährleiten und einen Einblick in den Markt für den Handel mit Daten zu erlangen. Zudem wird in dem Bericht argumentiert, dass ein gesteigertes Bewusstsein der Konsumenten über den Wert ihrer personenbezogenen Daten helfen könnte, das ökonomische Ungleichgewicht zwischen den Unternehmen und den Konsumenten auszugleichen. Dies könnte dem Konsumenten auch helfen, höhere Ansprüche und Erwartungen an den Umgang mit seinen personenbezogenen Daten zu stellen. OECD (2013), „Exploring the Economics of Personal Data: A survey of methodologies for measuring monetary value", OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

tere und genauere Entscheidungen treffen kann. Mehr Daten zu sammeln, bedeutet jedoch nicht notwendigerweise mehr Wissen. Mehr Daten können auch zu mehr Verwirrung und zu mehr „falsch positiven" Ergebnissen führen[31]. Ein übermäßiger Gebrauch von automatisierten Entscheidungen und Prädikatorenanalyse kann nachteilige Folgen für Betroffene haben. Algorithmen sind nicht neutral, sondern Ausdruck von Entscheidungen unter anderem in Bezug auf Daten, Verknüpfungen, Schlussfolgerungen, ihre Interpretation und Schwellenwerte für ihre Berücksichtigung, die einem spezifischen Zweck förderlich sind[32]. Big Data kann somit bestehende Vorurteile und Stereotypen bestätigen sowie soziale Ausgrenzung und Isolierung verstärken. Korrelationsanalysen können darüber hinaus im Einzelfall zu vollkommen falschen Ergebnissen führen. Korrelation wird oftmals mit Kausalität verwechselt. Wenn Analysen ergeben, dass Personen, die X mögen, mit einer Wahrscheinlichkeit von 80 % Y ausgesetzt werden, kann daraus unmöglich geschlossen werden, dass dies in 100 % der Fälle eintritt. Diskriminierungen auf der Grundlage statistischer Analysen kann daher zu einer Frage des Schutzes der Privatsphäre werden. Eine Entwicklung, bei der immer mehr gesellschaftliche Entscheidungen auf Algorithmen basieren, kann zu einer „Diktatur der Daten"[33] führen, in der wir nicht mehr anhand tatsächlicher Handlungen, sondern anhand dessen, was nach Datenlage die wahrscheinlichen Handlungen sein werden, beurteilt werden.

Der Einschüchterungseffekt („chilling effect"):

31. Wenn eine Entwicklung einsetzt, durch die Bonitätsbewertungen und Versicherungsprämien ausschließlich oder vorwiegend auf den Informationen basieren, die Nutzer in diversen Zusammenhängen im Internet und anderen Bereichen des Alltags hinterlassen, kann dies Folgen für den Schutz der Privatsphäre haben und für die Art und Weise, wie wir uns verhalten. So ist es möglich, dass unsere Kinder in zehn Jahren keinen Versicherungsschutz mehr bekommen, nur weil ihre Eltern beispielsweise in einem sozialen Netzwerk gepostet haben, eine Veranlagung für eine Erbkrankheit zu haben. Dies kann zu einer Selbstbeschränkung der Teilhabe am gesellschaftlichen Leben im Allgemeinen führen oder zu einer aktiven Anpassung des eigenen Verhaltens – sowohl online als auch im echten Leben. Wir könnte befürchten, dass sich die Spuren, die wir in den unterschiedlichsten Zusammenhängen hinterlassen, auf zukünftige Entscheidungen auswirken, wie beispielsweise

[31] Google „Grippe-Trends" war kürzlich Gegenstand einiger genauerer Untersuchungen; http://bits.blogs.nytimes.com/2014/03/28/google-flu-trends-the-limits-of-big-data/

[32] Dwork, Cynthia and Mulligan, Deirdre K. (2013), „It's not privacy, and it's not fair", 66 Stanford Law Review, Online 35, September 3, 2013, http://www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair

[33] Mayer-Schönberger, Viktor u. Cukier, Kenneth (2013), „Big Data. A Revolution That Will Transform How We Live, Work and Think", John Murray, London

auf Chancen auf dem Arbeitsmarkt, die Möglichkeit zum Erhalt von Krediten oder zum Abschluss von Versicherungen. Dies kann sogar so weit gehen, dass Nutzer davor zurückschrecken, sich online nach alternativen Ansichten umzusehen, aus Angst davor, identifiziert oder entdeckt zu werden oder um die Erstellung eines Nutzerprofils zu verhindern. Hinsichtlich der Nutzung von Big Data durch Behörden kann die Unsicherheit darüber, aus welchen Datenquellen Informationen erhoben und wie diese genutzt werden, das Vertrauen der Bürger in die Behörden selbst infrage stellen. Dies kann sich wiederum nachteilig auf die eigentlichen Grundlagen einer offenen und gesunden Demokratie auswirken. Ein unzureichender Schutz der Privatsphäre kann zu einer Schwächung der Demokratie führen, wenn Bürger ihre Beteiligung am offenen Meinungsaustausch einschränken. Im ungünstigsten Fall kann die übermäßige Nutzung von Big Data einen Einschüchterungseffekt in Bezug auf die Inanspruchnahme der Meinungsfreiheit haben, wenn die Voraussetzungen für die Nutzung von Big Data nicht offengelegt werden und nicht unabhängig überprüft werden können[34].

Echokammern:

32. Die Personalisierung im Internet durch individuell angepassten Medien und auf dem Internetverhalten des Einzelnen basierenden Nachrichtendiensten wird sich darüber hinaus auch auf die Rahmenbedingungen für öffentliche Debatten und den öffentlichen Gedankenaustausch auswirken und – wichtige Voraussetzungen für eine gesunde Demokratie. Dies ist nicht in erster Linie ein Problem des Datenschutzes, sondern stellt eine Gefahr für die Gesellschaft an sich dar. Die Gefahr aufgrund so genannter „Echokammern" oder „Filterblasen" liegt darin, dass der Nutzer nur solchen Inhalten ausgesetzt wird, die seinen ohnehin schon bestehenden Haltungen und Werten entsprechen. Der Austausch von Gedanken und Standpunkten kann gehemmt werden, wenn der Bürger seltener mit Ansichten konfrontiert wird, die von seinen bestehenden Meinungen abweichen.

Empfehlungen

33. Auch wenn Big Data in mehrfacher Hinsicht Gefahren für den Datenschutz mit sich bringt, ist dennoch eine Nutzung dieser Art von Analyse möglich,

[34] Die norwegische Datenschutzbehörde hat 2013 unter Norwegern eine Umfrage zu datenschutzbezogenen Themen durchgeführt. Eines der untersuchten Themen war die Frage nach dem Bestehen einer generellen Tendenz hin zu einem „chilling effect" in Norwegen. In der Umfrage wurden die Personen gefragt, ob sie sich entschlossen hätten, etwas nicht zu tun, weil sie sich nicht sicher waren, wie die Informationen darüber in der Zukunft verwendet würden. Die Ergebnisse deuten auf eine generelle Tendenz zu einem „chilling effect" hin. Sie zeigen, dass ein signifikanter Teil der Bevölkerung bestimmte Handlungen vermieden hat, weil sie über die mögliche zukünftige Verwendung der Informationen darüber unsicher sind. Es ist erwähnenswert, dass nicht weniger als 26 Prozent sich entschieden, eine Petition nicht zu unterzeichnen und 16 Prozent bestimmte Internetsuchen unterließen. Norwegian Data Protection Authority (2014), „The Chilling Effect in Norway", January, 2014. http://www.datatilsynet.no/Global/04_planer_rapporter/Nedkj%C3%B8ling%20i%20norge_eng_.pdf

ohne gegen grundlegende Datenschutzprinzipien zu verstoßen. Die Arbeitsgruppe gibt folgende Empfehlungen für eine Nutzung von Big Data bei gleichzeitiger Wahrung der Privatsphäre jedes Einzelnen.

Einwilligung:

34. Es wurde argumentiert, dass das Einwilligungserfordernis als rechtliche Grundlage für die Verarbeitung personenbezogener Informationen im Zeitalter von Big Data nur bedingt geeignet ist[35]. So wird gelegentlich vertreten, dass die ständige Forderung nach Einwilligung im Internet paradoxerweise sogar zu einem schlechteren Schutz des Einzelnen führen kann. Es lässt sich bereits jetzt eine Tendenz feststellen, dass Unternehmen ihre Kunden zur Abgabe sehr umfassender Einwilligungserklärungen auffordern, möglicherweise in der Hoffnung, dass derartige Erklärungen oftmals nicht gründlich gelesen werden und den Unternehmen damit „Ellbogenfreiheit" für die Nutzung der Informationen für zukünftige und andere Zwecke verschaffen. Eine solche Nutzung der Einwilligung ist rechtswidrig.

35. Auch wenn ohne Frage Schwierigkeiten bestehen, eine wirksame und aussagekräftige Einwilligung einzuholen, bleibt die Einwilligung gleichwohl der Eckpfeiler moderner Datenschutzgesetze. Eine Aufweichung der Einwilligung droht die Kontrolle des Einzelnen über die Nutzung seiner Daten ebenfalls zu schwächen[36]. Die Einwilligung ist nur eine von mehreren gesetzlichen Grundlagen für die Verarbeitung personenbezogener Daten. Auch wenn der Einwilligung eine wichtige Rolle zukommt, schließt dies je nach Kontext für die Verarbeitung jedoch nicht die Möglichkeit anderer rechtlicher Grundlagen aus, die unter Umständen aus Sicht sowohl der verantwortlichen Stelle als auch des Betroffenen geeigneter sind[37].

36. Im Zusammenhang mit der Nutzung personenbezogener Daten für Analyse- und Profilerstellungszwecke sollte eine wirksame Einwilligung des Betroffenen eingeholt werden[38].

---

[35] Vgl. Cate, Fred H. u. Mayer-Schönberger, Viktor (2013), „Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines", December 2013, http://op.bna.com/pl.nsf/id/dapn-9gyjvw/$File/Data-Protection-Principles-for-the-21st-Century.pdf

[36] „Beim Entfernen der Einwilligung aus der Betrachtung riskiert man, fundamentale Grundrechte, Schutzfunktionen und Freiheiten jenseits des ‚Information- und Einwilligungs'-Systems zu unterminieren. Anstatt die Einwilligung abzuschaffen, sollten wir daran arbeiten, die Transparenz und die individuellen Kontrollmechanismen zu verbessern, und die Herausforderungen direkt angehen" (Cavoukian et. Al (2014) „The Unintended Consequences of Privacy Paternalism").

[37] Stellungnahme 15/2011 der Artikel 29-Datenschutzgruppe zur Definition der Einwilligung.

[38] Eine zulässige Einwilligung muss ohne Zwang, für den konkreten Einzelfall und in Kenntnis der Sachlage erfolgen, vgl. Art. 2 Bst. h der Richtlinie 95/46/EG.

37. Falls eine Einwilligung nicht eingeholt werden kann, könnte eine Verarbeitung der Daten innerhalb sorgsam abgewogener Grenzen trotzdem möglich sein[39]. So könnte die verantwortliche Stelle die Daten beispielsweise dann verarbeiten, wenn dies für ihre legitimen Zwecke erforderlich ist, so lange die Interessen des Betroffenen nicht überwiegen. Die verantwortliche Stelle muss zwei entgegenstehende Interessen gegeneinander abwägen, nämlich einerseits ihre legitimen Interessen und andererseits die Interessen des Einzelnen. Das Ergebnis dieser Interessenabwägung wird von Fall zu Fall verschieden sein und hängt von den jeweils in Frage stehenden Datenschutzinteressen des Einzelnen und von den legitimen Interessen der verantwortlichen Stelle ab[40]. Je stärker die Auswirkungen auf den Betroffenen, desto wichtiger ist die Beachtung entsprechender Schutzmechanismen[41].

38. Verantwortliche Stellen, die die erhobenen Daten für einen anderen als den ursprünglichen Zweck verwenden wollen, sind verpflichtet, die Vereinbarkeit zwischen den ursprünglichen und den neuen Zwecken einzelfallabhängig zu prüfen[42]. Solange diese Vereinbarkeit nicht gewährleistet ist, dürfen keine Daten verarbeitet werden, die eine persönliche Identifizierung ermöglichen.

---

[39] Die Art. 29-Datenschutzgruppe hat Handlungsempfehlungen zu einer solchen Gratwanderung gegeben (Vgl. Arbeitspapier 217, S. 55–56 [der englischen Fassung]). Zudem betont der Bericht des Weißen Hauses zu Big Data die Wichtigkeit des Sachzusammenhangs in Situationen, in denen eine Einwilligung nicht praktikabel ist. (Executive Office of the President, White House (2014): „Big Data: Seizing opportunities, preserving values“).

[40] Obwohl sich nicht ausschließen lässt, dass eine Interessenabwägung in einigen Fällen die Verarbeitung personenbezogener Daten rechtfertigt, muss stets der Einzelfall berücksichtigt werden. Diese Möglichkeit kann deshalb kaum als allgemeine Rechtsgrundlage für die Erhebung und Analyse von Big Data dienen. In jedem Fall hat die verarbeitende Stelle die Beweislast, dass die Bedingungen für eine Interessenabwägung zu ihren Gunsten erfüllt sind. Diese Abwägung und ihre zahlreichen Ermessensbestandteile und Unklarheiten können in dieser Hinsicht Schwierigkeiten für die verarbeitende Stelle mit sich bringen.

[41] Die Art. 29-Datenschutzgruppe hat in ihrer Stellungnahme 06/2014 zu „berechtigten Interessen verarbeitender Stellen im Hinblick auf Art. 7 der Richtlinie 95/46/EG“ Handlungsanweisungen zu Faktoren gegeben, die bei einer Interessenabwägung zu berücksichtigen sind. Besondere Aufmerksamkeit wird dabei der Rolle gewidmet, die Schutzmaßnahmen bei der Reduzierung unzulässiger Auswirkungen für von der Datenverarbeitung Betroffene spielen könnten und dadurch die Gewichtung von Rechten und Interessen so verändern würden, dass die berechtigten Interessen der verarbeitenden Stelle zum Zuge kommen. Solche Schutzmaßnahmen könnten unter anderem Begrenzungen bezüglich der Datenmenge, eine unverzügliche Löschung der Daten nach ihrer Nutzung, technische und organisatorische Maßnahmen zur Sicherstellung von funktionaler Trennung, geeignete Anonymisierungstechniken, die Aggregierung von Daten sowie der Einsatz datenschutzfreundlicher Technologien, aber auch gesteigerte Transparenz, Verantwortlichkeit und die Möglichkeit zum Widerspruch gegen die Verarbeitung sein.

[42] Die Art. 29 Datenschutzgruppe schlägt in ihrer Stellungnahme 15/2011 zur Zweckbestimmung eine Beurteilung sämtlicher relevanter Umstände vor, insbesondere der folgenden Schlüsselfaktoren:
- das Verhältnis zwischen dem Zweck, für den die Daten erhoben wurden und den Zwecken weiterer Verarbeitung;
- der Sachzusammenhang, in dem die personenbezogenen Daten erhoben wurden und die berechtigten Erwartungen des Betroffenen der Datenverarbeitung bezüglich ihrer weiteren Nutzung;
- die Beschaffenheit der personenbezogenen Daten und die Auswirkungen der weiteren Verarbeitung auf den Betroffenen.
- die von der verarbeitenden Stelle zur Sicherstellung einer fairen Verarbeitung und zur Verhinderung unzulässiger Auswirkungen auf den Betroffenen angewandten Schutzmaßnahmen

Verfahren für eine wirksame Anonymisierung:

39. Die verantwortliche Stelle muss entscheiden, ob die in der Big-Data-Analyse zu verwendenden personenbezogenen Daten anonymisiert oder pseudonymisiert werden müssen oder ob sie identifizierbar bleiben können. Diese Entscheidung bestimmt, wie sich die Rechtsvorschriften zum Datenschutz auf die weitere Verarbeitung der Informationen durch das Unternehmen auswirken. Anonymisierte Daten sind vom Anwendungsbereich der Datenschutzrechtvorschriften nicht erfasst.

40. Anonymisierung kann bei der Reduzierung oder Beseitigung von Datenschutzrisiken im Zusammenhang mit Big-Data-Analysen hilfreich sein, jedoch nur, wenn die Anonymisierung technisch einwandfrei durchgeführt wird[43].

    Anonymisierung ist das Ergebnis einer Verarbeitung personenbezogener Daten mit dem Ziel, die Identifizierung des Einzelnen unumkehrbar zu verhindern. Dabei hat die verantwortliche Stelle verschiedene Aspekte zu bedenken, insbesondere sämtliche (entweder durch die verantwortliche Stelle selbst oder durch Dritte) „mit einiger Wahrscheinlichkeit" zu einer Identifizierung eingesetzten Mittel. Wichtig ist eine Prüfung anonymisierter Daten hinsichtlich ines akzeptablen Risikoniveaus[44]. Diese Prüfung ist beispielsweise im Rahmen einer Datenschutz-Folgenabschätzung zu dokumentieren.

41. Über die optimale Lösung zur Anonymisierung der Daten ist einzelfallabhängig zu entscheiden, ggf. auch mithilfe einer Kombination verschiedener Verfahren. Hierbei kommen verschiedene Anonymisierungsverfahren in Betracht; in erster Linie die Randomisierung und die Generalisierung der Daten[45]. Die Kenntnis der wesentlichen Stärken und Schwächen der einzelnen Verfahren kann bei der Gestaltung des geeigneten Verfahrens zur Anonymisierung hilfreich sein. Die Robustheit der einzelnen Verfahren sollte anhand von drei Kriterien ermittelt werden[46]:

---

[43] Die Art. 29 Datenschutzgruppe betont in ihrer Stellungnahme 05/2014 zu Anonymisierungstechniken, dass Anonymisierungstechniken Garantien für den Schutz der Privatsphäre bilden können, aber nur, wenn sie sachgemäß angewendet werden, d. h. dass die Voraussetzungen (Sachzusammenhang) und der Zweck (bzw. die Zwecke) des Anonymisierungsprozesses klar abgesteckt werden müssen, um den beabsichtigten Anonymisierungsgrad zu erreichen.

[44] Die Art. 29 Datenschutzgruppe hebt in ihrer Stellungnahme 05/2014 zu Anonymisierungstechniken hervor, dass es weder möglich noch hilfreich ist, eine abschließende Aufzählung von Umständen vorzugeben, bei deren Vorliegen eine Identifikation nicht mehr möglich ist. Dennoch gibt das Dokument einige generelle Handlungsempfehlungen zur Beurteilung des Identifizierungspotentials eines bestimmten Datensatzes, der einer Anonymisierung nach den unterschiedlichen verfügbaren Techniken unterzogen wird.

[45] Randomisierung und Generalisierung sind zwei Oberbegriffe für Anonymisierungstechniken, die zum Beispiel „Hinzufügen von Rauschen" (noise addition), Permutation, „differentielle Privatheit" (differential privacy), Aggregierung, k-Anonymität, l-Diversität und t-Nähe („t-closeness") abdecken.

[46] Die Art. 29 Datenschutzgruppe gibt in ihrer Stellungnahme 05/2014 zu Anonymisierungstechniken eine Übersicht zu den Stärken und Schwächen der Techniken, die die drei grundlegenden Kriterien berücksichtigen.

i. Ist es immer noch möglich, eine Einzelperson zu identifizieren?

ii. Ist es immer noch möglich, Datensätze einer Einzelperson zuzuordnen?

iii. Können Informationen über eine bestimmte Person abgeleitet werden?

42. Pseudonymisierte Daten sind nicht dasselbe wie anonymisierte Daten. Eine verantwortliche Stelle, die sich statt für eine Anonymisierung für eine Pseudonymisierung von Daten entscheidet, muss sich der Tatsache bewusst sein, dass diese Informationen nach wie vor als personenbezogene Daten gelten und daher zu schützen sind.

43. Es ist äußerste Vorsicht geboten, bevor pseudonymisierte oder anderweitig identifizierbare Datenbestände weitergegeben oder veröffentlicht werden. Falls die Daten detailliert sind, mit anderen Datensätzen verknüpft werden können[47] und personenbezogene Daten beinhalten, ist der Zugang zu beschränken und sorgfältig zu kontrollieren. Bei aggregierten Daten, bei denen ein geringeres Risiko einer Verknüpfung mit anderen Datensätzen besteht, ist die Wahrscheinlichkeit größer, dass diese Daten ohne erhebliche Risiken zugänglich gemacht werden können.

44. Für den Fall, dass verantwortliche Stellen anderen Einrichtungen pseudonymisierte oder auf sonstige Weise identifizierbare Daten zur Verfügung stellen, sollte vertraglich untersagt werden, Versuche zur Reidentifizierung der Daten zu unternehmen[48]. Dies sollte auch für frei verfügbare und nutzbare Daten („open data“) gelten[49].

45. Die Arbeitsgruppe empfiehlt die Einrichtung eines Gremiums oder Netzwerks, durch das jeder zur Anonymisierung oder Pseudonymisierung von Daten verpflichtete Akteur die Möglichkeit zum Austausch über die mit der Anonymisierung verbundenen Schwierigkeiten sowie von Erfahrungen erhält. Ein solches Netzwerk existiert bereits in Großbritannien (das UK Anonymisation Network (UKAN)). Es wird von den Universitäten Manchester und Southampton, dem Open Data Institute sowie dem Office for National Statistics koordiniert[50].

[47] Pseudonymisierte Informationen in einem Datensatz könnten mit Informationen in einem anderen Datensatz verbunden werden, z. B. bei Verwendung desselben eindeutigen Identifikators für jede Person.

[48] Diese Empfehlung wird auch von der Federal Trade Commission in dem Bericht „Protecting Consumer Privacy in an Era of Rapid Change“ vorgebracht, FTC Report, Federal Trade Commission, March 2012

[49] Art. 29 Datenschutzgruppe, Stellungnahme 6/2013 zu den Offenen Daten („Open Data“) und der Weiterverwendung von Informationen des öffentlichen Sektors („PSI“), S. 17f.

[50] http://www.ukanon.net/

Mehr Transparenz und Kontrolle von der Erhebung bis hin zur Nutzung von Daten:

46. Jeder Betroffene sollte darüber informiert werden, welche Daten gesammelt werden, wie mit diesen umgegangen wird, für welche Zwecke sie genutzt werden und ob die Daten an Dritte weitergegeben werden oder nicht[51].

47. Jeder Betroffene sollte Zugang zu seinem Profil sowie zu sämtlichen seiner Informationen erhalten, sich bei der verantwortliche Stelle befinden. Jeder Betroffene sollte darüber hinaus auch über die Quellen der diversen personenbezogenen Daten informiert werden. Er sollte zudem nach Maßgabe der einschlägigen gesetzlichen Bestimmungen[52] in der Lage sein, Informationen über sich zu berichtigen und deren Nutzung in Programmen zur Erstellung von (Verhaltens-)Profilen zu widersprechen bzw. darin einzuwilligen[53].

48. Klassifizierungssysteme können nachteilige Folgen für den Einzelnen haben. Jeder Bürger sollte daher Zugang zu Informationen darüber haben, welche Algorithmen als Grundlage für eine Profilerstellung oder für Entscheidungen verwendet worden sind. Diese Informationen sollten klar und verständlich gehalten sein, um unangemessene Diskriminierungen zu verhindern und für den Betroffenen bedeutsame Entscheidungen auf falscher Tatsachengrundlage zu vermeiden[54].

49. Jedem Einzelnen sollten auf Verlangen sämtliche Daten im Besitz der verantwortlichen Stelle auf benutzerfreundliche Weise und – wo dies angemessen ist – in maschinenlesbaren, portablen Formaten zur Verfügung gestellt werden. Dies erleichtert den Wechsel zu einem anderen Diensteanbieter mit den bestmöglichen Bedingungen einschließlich des besten Schutzes der Privatsphäre. Die Portabilität von Daten verhindert, dass der Kunde untrennbar an Dienstleistungen zu nicht akzeptablen Geschäftsbedingungen gebunden ist. Diese Forderung kann im Laufe der Zeit zur Entwicklung datenschutz-

[51] Zum Beispiel bieten einige Unternehmen ihren Kunden sogenannte „Übersichtsseiten für personenbezogene Daten" („personal data dashboards") an, die dem Kunden einen Überblick über die Verarbeitung ihrer personenbezogenen Daten geben.

[52] Für den öffentlichen und den privaten Bereich gelten ggf. unterschiedliche Bestimmungen.

[53] Die Kommissarin der FTC, Julie Brill, hat in ihrer „Reclaim Your Name"-Initiative ähnliche Empfehlungen abgegeben. Diese Initiative zielt darauf ab, Betroffene dergestalt zu stärken, dass sie herausfinden können, wie Datenhändler ihre Daten erheben und verwenden. „Reclaim Your Name" verschafft Kunden Zugang zu Informationen, die Datenhändler über sie angesammelt haben, und eröffnet ihnen die Möglichkeit, sich im Wege eines Opt-out-Verfahrens dieser Datenverarbeitung zu widersetzen, wenn die Betroffenen herausfinden, dass ein Datenhändler die Informationen für Marketingzwecke verkauft. Ebenso können Betroffene Informationen berichtigen lassen, die wesentlichen Entscheidungen zugrunde liegen. (Reclaim Your Name, 23rd Computers, Freedom and Privacy Conference, Grundsatzreferat v. Julie Brill, FTC, Washington, DC, 26. Juni 2013)

[54] Es ist wichtig, Transparenz bezüglich der bei der Profilbildung verwendeten Algorithmen zu schaffen. Angesichts der Komplexität von Algorithmen ist es jedoch unangemessen, zu erwarten, dass allein durch Transparenz möglichen inhärenten Verzerrungen abgeholfen wird. Automatisierte Systeme zur Entscheidungsfindung sollten ebenso Gegenstand ethischer und rechenschaftspflichtiger Aufsicht sein, wie bereits in Punkt 53 dargestellt.

freundlicherer Dienstleistungen führen und die Betroffenen darin unterstützen, ihr Verständnis der sie betreffenden Daten zu verbessern.

Privacy by Design und Rechenschaftspflicht:

50. Robustere Anonymisierungsverfahren allein sind noch keine Lösung der Herausforderungen, die Big Data an den Schutz der Privatsphäre stellt. Zusätzliche Lösungen sind erforderlich. „Privacy by Design" und Rechenschaftspflicht sind weitere wichtige Elemente zur Entschärfung der datenschutzrechtlichen Herausforderungen.

51. Die Anwendung von Big-Data-Technologien sollte auf den sieben Grundsätzen des „Privacy by Design" aufbauen[55]. „Privacy by Design" beinhaltet die Berücksichtigung des Schutzes der Privatsphäre in allen Stadien der Systementwicklung, in Verfahren und Geschäftspraktiken.

52. Um das Vertrauen derjenigen zu erhalten, deren personenbezogene Daten erhoben, verarbeitet und analysiert werden, bedarf es einer frühestmöglichen Abschätzung der Herausforderungen für den Schutz der Privatsphäre; auf jeden Fall vor Beginn der Verarbeitung von Big Data. Eine Möglichkeit hierfür stellt die Datenschutz-Folgenabschätzung dar. Diese sollte eine Beurteilung jeder rechtlichen Grundlage für die Verteilung und Wiederverwendung personenbezogener Daten umfassen, die Grundsätze der Zweckbegrenzung, Verhältnismäßigkeit und Datenminimierung ebenso wie Datenschutz- und Datensicherheitsmechanismen abschätzen. Bei einer solchen Folgenabschätzung sollten auch alle potenziellen Folgen für die Betroffenen sorgfältig untersucht werden[56, 57].

53. Rechenschaftspflicht ist ein weiterer wichtiger Grundsatz des Datenschutzes und schafft Vertrauen zwischen Betroffenen und verantwortlichen Stellen. Letztere müssen den Nachweis erbringen, dass sie ihre Rechenschaftspflicht

[55] Die sieben Prinzipien des eingebauten Datenschutzes sind: 1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe, 2. Datenschutz als Standardeinstellung, 3. Der Datenschutz ist in das Design eingebettet, 4. Volle Funktionalität – eine Positivsumme, keine Nullsumme, 5. Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus, 6. Sichtbarkeit und Transparenz – Für Offenheit sorgen, 7. Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen, https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf

[56] Art. 29 Datenschutzgruppe, Stellungnahme 06/2013 zu Open Data sowie Stellungnahme 06/2014 zum Begriff des berechtigten Interesses der verantwortlichen Stelle gemäß Artikel 7 der RL 95/46/EG.

[57] Die EU hat ein Rahmenkonzept für Datenschutz-Folgeabschätzungen bei RFID-Anwendungen geschaffen, das dabei helfen soll, die datenschutzrechtlichen Konsequenzen des Einsatzes der RFID-Technologie zu identifizieren. Dieses Rahmenkonzept ist ebenso für Unternehmen von Interesse, die Big Data im Zusammenhang mit der Entstehung des Internet der Dinge verwenden. Das Rahmenkonzept wurde von der RFID-Industrie entwickelt und von den Datenschutzaufsichtsbehörden in der EU als mit der Datenschutzgesetzgebung konform erachtet. Die Artikel-29-Datenschutzgruppe regt die Schaffung eines gleichartigen Rahmenkonzepts für die Nutzung von Big-Data-Technologien durch auf diesen Bereich spezialisierte Unternehmen an (Europäische Kommission (2011), „Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12. Januar 2011, http://ec.europa.eu/justice/policies/policy/docs/wpdocs/2011/wp/wp180_annex_en.pdf.)

wahrnehmen und in der Lage sind, verantwortungsvolle und ethische Entscheidungen bezüglich ihrer Nutzung von Big Data zu treffen. So müssen sich verantwortliche Stellen der Tatsache bewusst sein, dass auch ein anonymisierter Datensatz immer noch Folgen für den Einzelnen haben kann. Anonymisierte Datensätze können zur Vervollständigung existierender Profile von Personen genutzt werden, was neue Fragen für den Schutz der Privatsphäre aufwirft. Sowohl die Profile als auch die zugrunde liegenden Algorithmen bedürfen einer kontinuierlichen Begutachtung. Dies erfordert regelmäßige Kontrollen, um zu gewährleisten, dass auf der Profilerstellung aufbauende Entscheidungen verantwortungsbewusst, gerecht, ethisch und mit dem Zweck, für den die Profile genutzt werden, vereinbar sind. Eine ungerechte Behandlung Einzelner aufgrund automatisierter falsch positiver oder falsch negativer Ergebnisse gilt es zu vermeiden[58].

Verbesserung von Wissen und Bewusstsein:

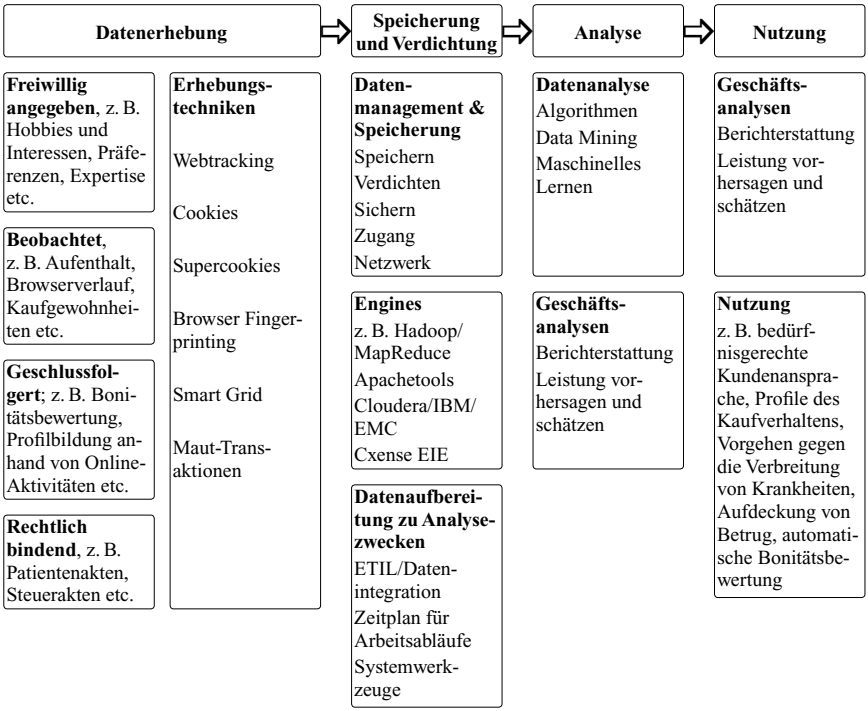
54. Das Wissen um und Bewusstsein von mit Big Data verbundene Herausforderungen für den Datenschutz sind bedeutsam für verantwortliche Stellen, die diese Technologie einsetzen. Die Industrie muss sich dieser Herausforderungen stellen und Schulungen hinsichtlich Maßnahmen zu ihrer Lösung anbieten, beispielsweise in Form von „Privacy by Design".

55. Der Schutz der Privatsphäre sowie die Herausforderungen für den Datenschutz im Zusammenhang mit Big Data sollten an Universitäten und sonstigen Hochschulen behandelt werden, an denen Informatik oder Informationswissenschaften gelehrt werden.

56. Behörden müssen über das notwendige Wissen und Bewusstsein hinsichtlich des Potenzials von Big Data verfügen. Dies ist insbesondere in Verbindung mit der Formulierung neuer Gesetze und Bestimmungen von Bedeutung. Weiterhin ist Problembewusstsein nötig, damit Behörden in der Lage sind, ihre Aufgabe zum Schutz einer Reihe zentraler Werte der Gesellschaft wahrnehmen können.

[58] „Uruguay Erklärung zum Profiling" (2012), 34. Internationale Konferenz der Datenschutzbeauftragten, 25.–26. Oktober 2012, http://privacyconference2012.org/wps/wcm/connect/7b10b0804d5dc38db944fbfd6066fd91/Uruguay_Declaration_final.pdf?MOD=AJPERES .

Die Big-Data-Wertschöpfungskette



Beispiele für Interessengruppen bei der Datenerfassung	Beispiele für Interessengruppen bei Speicherung und Aggregierung	Beispiele für Interessengruppen bei der Analyse	Beispiele für Interessengruppen mit Nutzung
Suchmaschinenanbieter	Suchmaschinenanbieter	Suchmaschinenanbieter	Informationswissenschaftler
Anbieter von Hardware, Software und Betriebssystemen	Anbieter von Hardware, Software und Betriebssystemen	Anbieter von Hardware, Software und Betriebssystemen	Suchmaschinenanbieter
Soziale Netzwerke	Soziale Netzwerke	Soziale Netzwerke	Anbieter von Hardware, Software und Betriebssystemen
Einzelhandel	Einzelhandel	Einzelhandel	Soziale Netzwerke
Datenhändler	Analysefirmen	Analysefirmen	Werbetreibende
Werbenetzwerke	Datenhändler	Datenhändler	Einzelhandel
Telekommunikationsanbieter	Werbenetzwerke	Werbenetzwerke	Kreditwirtschaft
Gesundheitsdienstleister	Telekommunikationsanbieter	Telekommunikationsanbieter	Versicherungen
Öffentlicher Sektor			Telekommunikationsanbieter
			Gesundheitsdienstleister
			Öffentlicher Sektor

2. 56. Sitzung am 14./15. Oktober 2014 in Berlin

Arbeitspapier zu Datenschutz- und Datensicherheitsrisiken bei der Nutzung von privaten Endgeräten in Unternehmensnetzwerken

– Übersetzung –

Anwendungsbereich

Dieses Arbeitspapier untersucht die mit der Nutzung privater, mobiler Endgeräte („Own Devices“) wie Tablet-Computer und Smartphones verbundenen Datenschutz- und Sicherheitsrisiken für den Zugriff auf Anwendungen und Daten einschließlich personenbezogener Daten, die in Unternehmensnetzwerken liegen.

Viele dieser Risiken sind bereits von der Arbeitsgruppe in den Arbeitspapieren zu „Mobile Verarbeitung personenbezogener Daten und Datensicherheit[1]“ und „Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes[2]“ behandelt worden, aber es gibt weitere, spezifische Fragestellungen bei der Nutzung von privaten Endgeräten in Unternehmensnetzwerken.

Hintergrund

„Bring Your Own Device“ (BYOD)-Praktiken sind im Geschäftsleben weit verbreitet, und es gibt einen zunehmenden Druck zu ihrer Einführung. Allerdings wächst auch die Besorgnis über die Auswirkungen auf Datenschutz und Datensicherheit bei der Einführung dieser Praktiken[3].

Organisationen empfinden BYOD als gesteigerten Komfort für ihre Beschäftigten, die ihnen bekannte Endgeräte bei der Arbeit nutzen können, und wenn sie unterwegs oder zuhause sind, und für leitende Angestellte, die häufig die erweiterten Funktionen und den Bedienungskomfort fordern, die ihre eigenen Endgeräte bieten.

Diesen möglichen Vorteilen stehen Risiken für die Vertraulichkeit und Integrität von Informationsverarbeitungssystemen von Unternehmen entgegen und das

[1] http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf.

[2] http://www.datenschutz-berlin.de/attachments/882/675.44.10.pdf

[3] http://enterprise-mobile-solutions.tmcnet.com/articles/359879-growth-byod-compels-companies-revisit-security-basics.htm

gesteigerte Risiko, dass personenbezogene Daten in diesen Systemen nicht länger adäquat geschützt sein könnten.

Jede Organisation, die BYOD erlaubt, muss adäquate Sicherheitsmaßnahmen anwenden, um den Schutz aller verarbeiteten Unternehmensdaten sicherzustellen. Organisationen müssen auch sicherstellen, dass die Auswirkungen dieser Sicherheitsmaßnahmen auf die Privatsphäre der einzelnen Nutzer minimiert werden[4].

Nutzer könnten jedoch darüber besorgt sein, dass die Organisation exzessive Überwachungsmaßnahmen durchführt, um diesen Risiken zu begegnen; z. B. könnte der Administrator des Unternehmensnetzwerkes vollen Zugriff auf das private Endgerät (d. h. einschließlich des Zugriffs auf alle privaten Daten) haben, um Unternehmensdaten zu erkennen und zu schützen. Im Fall des Verlustes des Endgeräts oder wenn es gestohlen wird, könnte eine „Fernlöschung" dazu führen, dass auf dem Endgerät gespeicherte, private Informationen dauerhaft gelöscht werden. Dementsprechend können private Endgeräte zusätzliche Risiken für die personenbezogenen Daten ihrer Nutzer mit sich bringen. Die korrekte Nutzung einer Anwendung zur Verwaltung mobiler Endgeräte kann die personenbezogenen Daten von Nutzern privater Endgeräte sichern und gleichzeitig die Vertraulichkeit und Integrität von Unternehmensdaten schützen.

Die Richtlinien des Weißen Hauses für Bundesbehörden[5] sprechen sich für BYOD aus, aber warnen davor, dass *„die Einführung eines BYOD-Programms Behörden vor unzählige Herausforderungen für die Sicherheit, vor konzeptuelle, technische und rechtliche Herausforderungen nicht nur für die interne Kommunikation, sondern auch in Bezug auf Beziehungen und das Vertrauen zwischen privatwirtschaftlichen und administrativen Partnern stellt."*

Empfehlungen für öffentliche Stellen der britischen Regierung klingen vorsichtiger; sie empfehlen: *„Es ist notwendig, dass das Endgerät für den gesamten Zeitraum, in dem es auf dienstliche Informationen zugreifen kann, unter die Verwaltungshoheit des Unternehmens gestellt wird. Somit ist ein BYOD-Modell möglich, jedoch aus verschiedenen technischen und nicht-technischen Gründen nicht empfohlen."*

Die französische nationale Sicherheitsbehörde (ANSSI) rät gegenwärtig von der Anwendung von BYOD ab[6].

[4] Z. B. durch die Anwendung von „Sandbox"-Techniken, bei denen ein Endgerät zwei verschiedene „Sandboxen" enthält, eine persönliche und eine geschäftliche.

[5] http://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations

[6] http://www.ssi.gouv.fr/IMG/pdf/Communique_de_presse_Assises_de_Monaco_2012_v2.pdf

Vom britischen Information Commissioner veröffentlichte Empfehlungen für verantwortliche Stellen[7] betonen: *„Die Erlaubnis, Endgeräte, mit IT-Systemen von Unternehmen zu verbinden, über die sie keine Kontrolle haben, kann zu einer Reihe von Risiken für die Verletzung der Sicherheit und anderen Datenschutzbedenken führen, wenn dies nicht richtig gehandhabt wird."*

Das „Überblickspapier Consumerisation und BYOD"[8] des Deutschen Bundesamt für Sicherheit in der Informationstechnik betont, dass *„die zunehmende berufliche Nutzung von Endgeräten aus dem privaten Umfeld durch Consumerisation und BYOD […] zu großen Herausforderungen für die Informationssicherheit, aber auch für den Datenschutz [führt]. Dies muss als strategische Herausforderung angesehen und von der Leitungsebene einer jeden Institution sinnvoll gestaltet werden. […] Technische Maßnahmen alleine [reichen] nicht aus, sondern diese müssen durch organisatorische Maßnahmen flankiert werden, die im Einklang mit der Gesamtstrategie der Institution stehen."*

Das Büro der Beauftragten für Datenschutz und Informationsfreiheit von Ontario (Kanada) hat gemeinsam mit TELUS[9] ein Papier veröffentlicht, das Risiken für das Informationsmanagement untersucht und Hinweise zu Maßnahmen gibt, um diesen zu begegnen.

Die Nutzung privater Endgeräte ist nicht auf BYOD begrenzt, sondern schließt auch Endgeräte ein, deren Eigentümer Dritte sind oder die von Dritten kontrolliert werden, z. B. Mit-Auftragnehmer, Unterauftragnehmer, Kunden und Klienten. Darüber hinaus beseitigt die Beschränkung der Verarbeitung personenbezogener Daten auf unternehmenseigene und von diesem verwaltete Geräte nicht alle Risiken, die in einer zunehmend mobilen Arbeitnehmerschaft vorkommen, da die Nutzung nicht-genehmigter Software oder von Online-Diensten, manchmal als „Bring Your Own App", „Bring Your Own Software" oder sogar „Bring Your Own Anything (BYOx")[10] bezeichnet, gleichartige Bedenken hinsichtlich Datenschutz und Datensicherheit aufwirft.

Datenschutz- und Datensicherheitsrisiken

Viele der Risiken, die mit der Nutzung von privaten Endgeräten verbunden sind, sind ebenso relevant für die persönliche Nutzung unternehmenseigener Endgeräte, einschließlich:

[7] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html

[9] http://www.ipc.on.ca/site_documents/pbd-byod.pdf

[10] https://byox.eq.edu.au/SiteCollectionDocuments/byox-project-research-report.pdf

a) Private Endgeräte sind in vielen Fällen klein und mobil; daher sind jegliche Daten, die auf ein privates Endgerät übertragen werden, anfällig für Verlust, Diebstahl und unkontrollierten Zugriff;

b) private Endgeräte können Unternehmensdaten zugänglich machen und technische Datenschutzkontrollen umgehen; und

c) private Endgeräte können für unbemerkte externe Attacken und Überwachung anfällig sein (z. B. durch Missbrauch von WiFi oder Bluetooth-Technologie und durch den Zugriff auf unsichere Internetseiten). Dies kann „social engineering"-Attacken einschließen, die von der Nutzung sozialer Medien oder anderen Online-Dienste für berufliche Zwecke herrühren.

Risiken, die in besonderer Weise mit der Nutzung privater Endgeräte verknüpft sind, umfassen:

d) Es ist schwierig, die Betriebssysteme privater Endgeräte zur Reduktion von Funktionalität und Erhöhung der Sicherheit anzupassen, wie dies bei unternehmenseigenen Endgeräten üblich ist, die im Besitz der Organisation sind und von dieser verwaltet werden;

e) private Endgeräte können oft einen größeren Umfang potenziell weniger sicherer Kommunikationsnetzwerke aus verschiedenen Umgebungen einschließlich des Arbeitsplatzes, des Zuhauses und nationaler oder internationaler öffentlicher Orte verwenden, auf die unternehmenseigene Geräte nicht zugreifen können, die im allgemeinen ein von dem Unternehmen verwaltetes Kommunikationsnetzwerk nutzen, z. B. ein Kabel-gestütztes LAN, das sich in einer sicheren Büroumgebung befindet;

f) vorhandene Unternehmensanwendungen und die Netzwerkinfrastruktur könnten nicht mit adäquaten Sicherheitseinrichtungen versehen sein, um dem Zugriff privater Endgeräte zu ermöglichen;

g) Unternehmensrichtlinien zur akzeptierten Nutzung des Internet oder von Webmail oder sozialen Netzwerken am Arbeitsplatz könnten schwieriger durchzusetzen sein, wenn Beschäftigte private Endgeräte nutzen;

h) das Betriebssystem privater Endgeräte könnte nicht so ausgereift sein wie die traditionelle Unternehmensendgeräte und anfällig für eine Reihe von Angriffen oder Sicherheitslücken sein, die nicht innerhalb eines angemessenen Zeitraums beseitigt werden; darüber hinaus ist die Aktualisierung eines privaten Endgeräts typischerweise in der Verantwortung des Nutzers,

i) ein wesentlicher Teil der Nutzung privater Endgeräte wird persönlicher Natur sein und die Nutzung des Endgeräts könnte auf andere Mitglieder der Familie oder des Haushaltsbesitzers ausgedehnt werden;

j) Dienste, die eine automatische Datensicherung verwenden oder Software Dritter, die durch den Nutzer installiert wird, könnten in der unerwarteten oder nicht-autorisierten Nutzung von Cloud-Diensten resultieren;

k) der Nutzer eines privaten Endgeräts könnte weniger aufmerksam sein oder größere Sicherheitsrisiken mit einem privaten Endgerät eingehen;

l) personenbezogene Daten könnten nicht wirksam von dem Endgerät vor dessen Entsorgung, Wiederverkauf oder Recycling entfernt werden; und

m) die unangemessene Nutzung von Management-Werkzeugen und -techniken zur Verwaltung mobiler Endgeräte könnte zu überzogener Überwachung der Beschäftigten führen.

Empfehlungen

Im Lichte der Risiken für den Schutz personenbezogener Daten und die IT-Sicherheit sollte jede Organisation, die die Erlaubnis der Nutzung privater Endgeräte in Erwägung zieht, vor der Entscheidung über die Anwendung eines solchen Systems eine Vorabkontrolle (Privacy Impact Assessment – PIA) durchführen. Es ist wichtig, dass die Vorabkontrolle die Risiken sowohl für geschäftliche personenbezogene Daten als auch für die personenbezogenen Daten der Nutzer privater Endgeräte einbezieht. Die Vorabkontrolle sollte auch untersuchen, ob eine Verarbeitung dieser personenbezogenen Daten mit privaten Endgeräten angemessen ist, sowie die Auswirkungen von Sicherheitsvorfällen im Hinblick auf die Sensitivität der Daten, die Auswirkungen auf die Betroffenen und die möglichen Reputationsschäden, die aus dem Verlust oder der Verbreitung resultieren. Die Einführung sollte in vorsichtigen, wohlüberlegten Schritten erfolgen und mit nicht-sensitiven und nicht-vertraulichen Informationen beginnen. Die Verarbeitung sensitiver Daten bedingt zusätzliche Bedenken und verlangt zusätzliche Sicherheitsmaßnahmen[11].

Jede Organisation, die entscheidet, die Nutzung privater Endgeräte zu erlauben, muss angemessene Sicherheitsmaßnahmen etablieren, einschließlich, aber nicht beschränkt auf die Folgenden:

[11] Vgl. das Arbeitspapier „Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes" – „Sopot Memorandum" (Sopot (Polen), 23./23. April 2012), Fußnote 2 oben

a) Eine Untersuchung der vertraulichen und personenbezogenen Daten, die von der Organisation verarbeitet werden und eine Überprüfung, ob es angemessen ist, diese mit privaten Endgeräten zu verarbeiten. Als generelle Regel sollte die Verarbeitung sensitiver Daten mit privaten Endgeräten nur als angemessen betrachtet werden, wenn die mit der Verarbeitung verbundenen Risiken auf ein akzeptables Minimum reduziert werden können;

b) Eine Untersuchung des Schadens potenzieller Datenschutz- und Sicherheitsvorfälle in Hinsicht auf deren Auswirkungen auf die Betroffenen, die Sensivität der Daten und die durch Verlust oder Offenlegung verursachte Rufschädigung;

c) Festlegung, auf welche Unternehmensanwendungen von privaten Endgeräten zugegriffen werden muss;

d) Festlegung, welche Kategorien von Daten mit privaten Endgeräten zugänglich sein müssen;

e) Schriftliche Festlegung von Richtlinien über die Verpflichtungen von Beschäftigten im Zusammenhang mit der Nutzung privater Endgeräte, die mindestens Folgendes beinhalten:

   1) Regeln über die Löschung personenbezogener Unternehmensdaten von privaten Endgeräten;

   2) Die Verpflichtung Beschäftigter, das Unternehmen zu informieren, wenn ein privates Endgerät oder personenbezogene Unternehmensdaten, die auf einem privaten Endgerät gespeichert sind, gestohlen oder kompromittiert wurden;

   3) Personenbezogene Unternehmensdaten, die auf privaten Endgeräten gespeichert oder mit privaten Endgeräten zugänglich sind, gegen unbefugten Zugriff zu sichern, einschließlich der Fälle, in denen andere Teile des privaten Endgeräts von einer berechtigten dritten Partei wie einem Familienmitglied genutzt werden können.

f) Sicherstellung fortlaufender Unterstützung der Nutzer von privaten Endgeräten in Bezug auf die Meldung von Vorfällen und allgemeine Einbeziehung in Verfahrensabläufe; und

g) die Festlegung der notwendigen Erweiterungen für die Sicherheitspolitik und die technische Infrastruktur der Organisation, um den Zugriff mit privaten Endgeräten zu ermöglichen, wie:

1) Die Absicherung von Prozessen zur Nutzerauthentifikation und Nutzung sicherer Kommunikationsmethoden zur Ermöglichung des Zugriffs mit privaten Endgeräten;

2) die Erweiterung der Sicherheit des Unternehmenssystems für Anwendungen, auf die von privaten Endgeräten zugegriffen werden soll;

3) die Erweiterung der Kommunikationsinfrastruktur zur Einbindung von Ende-zu-Ende-Verschlüsselung für die Kommunikation mit privaten Endgeräten;

4) die Erstellung eines Registers genehmigter privater Endgeräte, deren Nutzung erlaubt ist und von deren Nutzern;

5) die Erstreckung existierender Verfahren zur Zugriffskontrolle, wie z. B., wenn ein Nutzer die Organisation verlässt oder keinen Zugriff mehr benötigt;

6) die regelmäßige Sicherung von Unternehmensdaten, die auf privaten Endgeräten gespeichert sind;

7) klare Regeln zur Fernlöschung von Unternehmensinformationen, die auf privaten Endgeräten gespeichert sind, die als verloren oder gestohlen gemeldet sind oder in anderer Weise nicht länger autorisiert sind, auf das Unternehmensnetzwerk zuzugreifen;

8) Verfahren, um den Auswirkungen von Schadsoftware und Botnetzen auf Unternehmensnetzwerke zu begegnen. Wenn diese auf privaten Endgeräten entdeckt werden und Organisationen die Möglichkeit eines unrechtmäßigen Zugriffs auf personenbezogene Daten nicht ausschließen können (z. B. durch effektive Netzwerksegmentierung oder Zugriffsprotokolle), sollte von einem Sicherheitsvorfall ausgegangen und angemessene Schritte zu dessen Behebung ergriffen werden;

9) angemessene Fortbildung für Nutzer privater Endgeräte zum Datenschutz, zur Vertraulichkeit und zu den Praktiken und Maßnahmen, die die Organisation dazu ergriffen hat, einschließlich zusätzlicher Fortbildungen zu Sicherheit und der akzeptablen Nutzung;

10) die Isolierung privater Endgeräte in einem separaten Netzwerk;

11) die Implementierung, den Test und die Validierung technischer Maßnahmen einschließlich von Firewalls und „Sandboxing“ auf privaten Endgeräten, um den Zugriff anderer Anwendungen auf Unternehmensdaten zu

verhindern, während gleichzeitig die Privatsphäre der Nutzer respektiert wird;

12) die angemessene, relevante und proportionale Kontrolle von Verarbeitungsaktivitäten, die von privaten Endgeräten unternommen werden – insbesondere Minimierung der Notwendigkeit zum Zugriff auf den persönlichen Datenbereich der Nutzer und zur Überwachung des Standorts privater Endgeräte außerhalb festgelegter Arbeitszeiten. Es ist zwingend, dass Sicherheitsmaßnahmen zum Schutz der Daten der Organisation nicht die Privatsphäre der Nutzer oder eines anderen Betroffenen (eines Dritten) verletzen, dessen Daten in dem privaten Bereich des Endgeräts gespeichert sein können (z. B. in Adressbüchern, im Posteingang privater E-Mails, auf Familienfotos, usw.);

13) Verfahren zur Validierung der Integrität privater Endgeräte und zur Bestätigung, dass diese definierten, akzeptablen Standards entsprechen, wie mindestens: Versionen des Betriebssystems, Endgerätetyp, Passwortschutz, Verschlüsselung (einschließlich Verschlüsselung des Dateisystems) und aktueller Schutz gegen Schadsoftware; und

14) Verfahren zur Entdeckung und Verhinderung der Nutzung von Software, die nach den Regeln der Organisation verboten ist, wie File-sharing-Anwendungen, Anwendungen für Streaming und peer-to-peer-Anwendungen. Dies muss in einer Weise erfolgen, die die Privatsphäre der Beschäftigten respektiert.

B. Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließungen der 28. Konferenz am 17. Juni 2014 in Hamburg

Das Urheberrecht dient nicht der Geheimhaltung!

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland betrachtet mit Sorge die Entwicklung, dass sich auskunftspflichtige Stellen zur Ablehnung von Anfragen auf das Urheberrecht oder andere Rechte des „Geistigen Eigentums“ berufen. Das Urheberrecht darf nicht dazu eingesetzt werden, staatliche Informationen zurück zu halten.

Amtliche Vermerke sind in aller Regel nicht urheberrechtlich geschützt. Gedankliche Inhalte können in ihrer politischen, wirtschaftlichen oder gesellschaftlichen Aussage nicht über das Urheberrecht monopolisiert werden, sondern müssen vielmehr Gegenstand der freien geistigen Auseinandersetzung bleiben. Mit Steuermitteln finanzierte und für die Erfüllung einer öffentlichen Aufgabe erstellte Vermerke dürfen nicht unter Berufung auf Rechte des „Geistigen Eigentums“ zurückgehalten werden. Hintergrund insbesondere des urheberrechtlichen Schutzes ist die Garantie einer angemessenen Vergütung der Urheber. Diese ist aber nicht bedroht, wenn Werke betroffen sind, die in Erfüllung dienstlicher Pflichten erstellt wurden.

Nur in Ausnahmefällen kann es sein, dass von Dritten für staatliche Stellen erstellte Gutachten tatsächlich dem Urheberrecht unterfallen und die Dritten schutzbedürftig sind. Wer mit der Verwaltung Verträge schließt, muss wissen, dass diese an gesetzliche Transparenzpflichten gebunden ist, die sich nicht abbedingen lassen. Wo dies nicht bereits gesetzlich vorgeschrieben ist, sollen sich die staatlichen Stellen in solchen Fällen das Recht an einer Herausgabe einräumen lassen. Soweit diese Stellen einem Informationsfreiheitsgesetz unterliegen, ist es ihre Pflicht, dafür Sorge zu tragen, dass Rechte Dritter nicht einem gesetzlichen Informationszugang entgegenstehen. Was mit staatlichen Mitteln für die Verwaltung von staatlichen Stellen oder Dritten hergestellt wird, muss grundsätzlich zugänglich sein.

Keine Flucht vor der Informationsfreiheit ins Privatrecht!

Es ist für weite Bereiche der Rechtsordnung anerkannt, dass der Staat sich nicht durch Wahl einer privaten Rechtsform seiner verfassungsrechtlichen Bindungen entledigen kann. Für das Recht aller Bürgerinnen und Bürger, sich voraussetzungslos über staatliches oder kommunales Handeln zu informieren, gilt dies leider nicht in gleichem Maße. Entscheidet sich der Staat für eine formale Privatisierung und erledigt eine öffentliche Aufgabe durch eine juristische Person des Privatrechts, so ist diese nach vielen Informationsfreiheitsgesetzen nicht direkt auskunftsverpflichtet. Informationszugang muss für alle Unterlagen gelten, die im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen. Dabei darf es nicht darauf ankommen, ob die Aufgaben durch Behörden oder durch Private, an denen die öffentliche Hand mehrheitlich beteiligt ist, wahrgenommen werden. Ebenso wenig kommt es auf die Rechtsform an, in der jeweils gehandelt wird.

Da häufig gerade die Bereiche privatisiert werden, die über große Finanzvolumina verfügen, ist hier die Herstellung von Transparenz hinsichtlich der Verwendung öffentlicher Steuermittel besonders wichtig. Bereits 2003 hatten die Informationsfreiheitsbeauftragten die Gesetzgeber im Bund und in den Ländern dazu aufgerufen, die Herstellung von Transparenz nicht davon abhängig zu machen, in welcher Form die öffentliche Aufgabe erledigt wird. Leider ist diese Forderung längst nicht überall umgesetzt worden. Es gilt weiterhin: Für die Auskunftsverpflichtung sollte allein entscheidend sein, ob es sich um eine staatliche oder kommunale Aufgabe, insbesondere eine der Grundversorgung handelt. Bei der Erfüllung öffentlicher Aufgaben müssen Ansprüche auf Auskunft auch direkt gegenüber den Unternehmen geschaffen werden.

Die Anwendung der Informationsfreiheitsgesetze darf nicht von der Rechtsform abhängen, in der öffentliche Aufgaben erledigt werden. Eine Flucht vor der Informationsfreiheit in das Privatrecht ist mit einem modernen Staatsverständnis nicht zu vereinbaren.

Informationsfreiheit nicht Privaten überlassen!

Öffentliche Stellen vertreten vielfach die Auffassung, staatliche Transparenz könne durch die Bereitstellung amtlicher Informationen auf von Privaten nach deren Regularien betriebenen Plattformen wie Facebook, Twitter etc. hergestellt werden. Auch wenn derartige Internetdiensteanbieter einen großen Nutzerkreis erreichen, stehen kommerzielle Interessen der Betreiber vielfach einem bedingungslosen und freien Informationszugang entgegen.

Öffentlichkeit ist gekennzeichnet durch voraussetzungslose, für ausnahmslos alle Menschen bestehende Zugangsmöglichkeiten. Sie kann deshalb nicht durch die

Bereitstellung von Inhalten auf Internetseiten und -diensten hergestellt werden, die zum Beispiel ausschließlich durch allgemeine Geschäftsbedingungen Privater geregelt sind, nur Mitgliedern offen stehen oder keinen unbeobachteten Zugang gewähren. Staatliche Transparenz darf nicht durch die Offenbarung personenbezogener Daten erkauft werden.

Nur die Veröffentlichung auf von öffentlichen Stellen steuerbaren und der Allgemeinheit kostenfrei und anonym zugänglichen Kanälen genügt den Anforderungen der Herstellung staatlicher Transparenz. Die Konferenz der Informationsfreiheitsbeauftragten fordert, die Veröffentlichung amtlicher Informationen auf ausschließlich von den öffentlichen Stellen selbst gesteuerten Veröffentlichungsmedien vorzunehmen. Eine Steuerung und Kontrolle in diesem Sinne kann beispielsweise auch durch Einzelverträge mit Privaten geschehen. Der im Hamburger Transparenzgesetz formulierte Grundsatz, wonach der Zugang zum Informationsregister kostenlos und anonym ist, sollte in alle Informationsfreiheits- und Transparenzgesetze aufgenommen werden.

2. Entschließungen der 29. Konferenz am 9. Dezember 2014 in Hamburg

Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!

In den vergangenen Jahren wurden die Ermittlungsbefugnisse für Polizeien, Strafverfolgungsbehörden und Nachrichtendienste kontinuierlich ausgeweitet. Ihnen steht ein beträchtliches Instrumentarium unterschiedlich eingriffsintensiver technischer Maßnahmen zur Verfügung, wie zum Beispiel Funkzellenabfragen, Einsatz von IMSI-Catchern, Telekommunikationsüberwachung und Verkehrsdatenerhebung. Im Rahmen der Erweiterung wurden in die Landespolizeigesetze und die Strafprozessordnung Berichterstattungspflichten aufgenommen. Dadurch sollte garantiert werden, dass die Gesellschaft sich der Auswirkungen dieser neuen Maßnahmen bewusst ist.

Eine kritische Überprüfung der Berichtspflichten zeigt, dass eine Transparenz der Auswirkungen solcher Ermittlungsmaßnahmen nicht erreicht wird. Die Berichterstattungspflichten sind nicht nur uneinheitlich geregelt: Zum Teil fehlen für einige Maßnahmen wie zum Beispiel die Bestandsdatenabfrage Berichtspflichten vollständig, zum Teil lassen die bestehenden Berichtspflichten keine hinlänglichen Erkenntnisse über das Ausmaß der Überwachung und insbesondere die Zahl der Betroffenen zu. Die Berichte über Funkzellenabfragen zu Strafverfolgungszwecken lassen etwa nicht erkennen, dass von einer einzelnen gerichtlichen

Anordnung tausende Bürgerinnen und Bürger betroffen sein können, die keinen Anlass für die Erhebung ihrer Daten gegeben haben. Das Bundesverfassungsgericht verlangt in seinem Urteil zur Vorratsdatenspeicherung aber gerade, dass der Gesetzgeber eine „Überwachungsgesamtrechnung“ betreibt und beim Erlass neuer Überwachungsregelungen berücksichtigt. Nur so könne verhindert werden, dass die Freiheitswahrnehmung der Bürger total erfasst und registriert wird, denn dies verstieße gegen die verfassungsrechtliche Identität Deutschlands. Deshalb ist es jedenfalls erforderlich, nicht nur die theoretisch bestehenden, vom Gesetz erlaubten Überwachungsmöglichkeiten in den Blick zu nehmen, sondern gerade auch das konkrete Ausmaß ihres Einsatzes sichtbar zu machen.

Auf der Grundlage der gegenwärtig veröffentlichten Statistiken und zum Teil schmalen Berichtspflichten ist es nicht möglich, die gesamtgesellschaftlichen Auswirkungen aller Maßnahmen differenziert zu erfassen. Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern daher auf, die bestehenden Verpflichtungen zur Erstellung und Veröffentlichung von Statistiken auf alle Maßnahmen im Rahmen verdeckter Ermittlungsmethoden auszudehnen und sie durch die Angabe der Anzahl der Betroffenen so aussagekräftig zu gestalten, dass sich der Effekt auf die Bevölkerung klar erkennen lässt.

Darüber hinaus muss eine gesetzliche Veröffentlichungspflicht für die Berichte der Bundesnetzagentur zur Bestandsdatenabfrage festgeschrieben werden.

Eine besondere Bedeutung kommt der Transparenz der Nachrichtendienste zu. Erforderlich ist die Verschärfung bestehender bzw. Schaffung neuer Berichtspflichten gegenüber parlamentarischen Kontrollgremien und Datenschutzbeauftragten und die Verpflichtung zur Aufnahme aussagekräftiger statistischer Angaben zu Überwachungsmaßnahmen in die Verfassungsschutzberichte von Bund und Ländern. Geboten ist insbesondere eine Berichterstattung für den gesamten Bereich der strategischen Auslands-Telekommunikationsüberwachung.

Die Transparenz beim Einsatz staatlicher, insbesondere geheimer Ermittlungsmethoden ist neben den datenschutzrechtlichen Anforderungen eine wesentliche Voraussetzung für eine effiziente demokratische Kontrolle sowie die Beurteilung der Angemessenheit des staatlichen Eingriffshandelns und damit eine unabdingbare Wissensgrundlage für das Vertrauen der Bürgerinnen und Bürger in ihren Rechtsstaat.

Umfassende und effektive Informationsfreiheitsaufsicht unabdingbar!

Mit den Informationsfreiheitsgesetzen des Bundes und der Länder wurde der Bundes- bzw. den Landesbeauftragten für Informationsfreiheit die Aufgabe eines „außergerichtlichen Streitschlichters“ im Bereich des allgemeinen Infor-

mationsfreiheitsrechts übertragen. Sie kontrollieren die Anwendung der Informationsfreiheitsgesetze, vermitteln in Streitfällen und wirken auf die Einhaltung des geltenden Rechts hin. Im Bund sowie in den meisten Bundesländern verfügen die Informationsfreiheitsbeauftragten jedoch nur über eine eingeschränkte Kontroll- und Beratungskompetenz. Sie überwachen nur die Einhaltung des allgemeinen Informationsfreiheitsrechts, nicht jedoch der besonderen Informationszugangsrechte, wie z. B. nach dem Umwelt- oder dem Verbraucherinformationsrecht.

Diese Situation ist unbefriedigend. Bürgerinnen und Bürger erwarten, dass ihr Informationsanliegen von den Informationsfreiheitsbeauftragten umfassend geprüft wird. Mangels umfassender Kontroll- und Beratungszuständigkeit ist dies jedoch zu häufig nicht der Fall, sodass es im Umwelt- und im Verbraucherinformationsrecht an einer unabhängigen Aufsichtsbehörde fehlt.

Auch die wissenschaftlichen Evaluierungsberichte zum Informationsfreiheitsgesetz des Bundes und einiger Länder haben sich dafür ausgesprochen, den Informationsfreiheitsbeauftragten zusätzlich die Kontrollkompetenzen für das besondere Informationsfreiheitsrecht zu übertragen. Im Bereich des Datenschutzes sind die Beauftragten bereits für das besondere Datenschutzrecht zuständig. Dieser Standard muss auch in der Informationsfreiheit hergestellt werden.

Die Konferenz der Informationsfreiheitsbeauftragten fordert daher die Gesetzgeber in Bund und Ländern auf, die Kontroll- und Beratungskompetenzen der Informationsfreiheitsbeauftragten um das Umwelt- und das Verbraucherinformationsrecht – wo dies noch nicht geschehen ist – zu erweitern und die Informationsfreiheitsbeauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten, damit sie ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen können. Nur so ist gesichert, dass Bürgerinnen und Bürger bei der Ausübung ihrer Informationsrechte umfassend beraten werden und die Einhaltung der verschiedenen Informationsgesetze unabhängig kontrolliert wird.

Open Data muss in Deutschland Standard werden!

Die Bundesregierung hat mit der Digitalen Agenda 2014 – 2017, der Digitalen Verwaltung 2020 und dem nationalen Aktionsplan zur Umsetzung der G8 Open-Data-Charta wesentliche Regierungsprogramme zur Etablierung von E- und Open-Government sowie zur Digitalisierung der Verwaltung auf den Weg gebracht. Die Regierungsprogramme sehen aus informationsfreiheitsrechtlicher Sicht u. a. die Einführung einer gesetzlichen Open-Data-Regelung, die Schaffung von Open-Data-Ansprechpartnern in den Behörden, die Einführung der elektronischen Verwaltungsakte und eine verstärkte Zusammenarbeit mit den Ländern vor.

Die Konferenz der Informationsfreiheitsbeauftragten betont in diesem Zusammenhang das Erfordernis weitgehender gesetzlicher Veröffentlichungspflichten und die Übertragung der Aufgabe des Open-Data-Ansprechpartners auf behördliche Informationsfreiheitsbeauftragte.

Insbesondere bei Planung und Einführung der eAkte sind Aspekte der Informationsfreiheit und des Datenschutzes frühestmöglich im Anforderungskatalog abzubilden. Schon bei Anlage einer Akte sollten personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse und sonstige Beschränkungen vor einer weiteren Verwendung markiert werden, so dass sie automatisiert ersetzt oder hervorgehoben werden können. Dies erleichtert eine nachfolgende Weitergabe und Weiterverwendung erheblich und unterstützt die aktenführenden Stellen bei der effizienten Bearbeitung von IFG-Anträgen.

Es gilt jetzt, die Regierungsprogramme zügig in die Tat umzusetzen, damit Open Data in Deutschland zum Standard werden kann. Die Konferenz fordert die Länder und den Bund auf, soweit noch nicht geschehen, mit dieser Zielsetzung E- und Open-Government-Strategien gemeinsam zu entwickeln.