Dokumente
zu Datenschutz
und Informationsfreiheit
2013

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
An der Urania 4–10, 10787 Berlin
Telefon: 030/13889-0
Telefax: 030/21550 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: druckpunkt Druckerei & Repro GmbH

Stand: Februar 2014

Inhaltsverzeichnis

Vorwort

Die flächendeckende, industrielle Überwachung der weltweiten Telekommunikation und Internetnutzung durch maßlose Nachrichtendienste hat ihren Niederschlag in mehreren Entschließungen gefunden, die die Datenschutzbeauftragten auf nationaler, europäischer und internationaler Ebene gefasst haben. Die Notwendigkeit, das Recht auf vertrauliche technikgestützte Kommunikation auch im 21. Jahrhundert zu sichern, zieht sich wie ein roter Faden durch diesen Dokumentenband. Erstmals enthält er auch eine Resolution der UN-Vollversammlung, die am 18. Dezember 2013 die Sicherung des Rechts auf Privatheit im digitalen Zeitalter gefordert hat. Dieser noch unverbindliche Appell könnte ein erster Schritt vom *soft law* hin zu einer Internationalen Konvention zum Datenschutz sein, wie sie die Datenschutzbeauftragten seit langem fordern.

Wie eng der Zusammenhang zwischen Datenschutz und Informationsfreiheit ist, verdeutlicht der von der Internationalen Konferenz der Informationsfreiheitsbeauftragten im September 2013 verabschiedete „Berliner Appell", der hier ebenfalls veröffentlicht ist. Exzessive Überwachung war und ist nur möglich unter exzessiver Geheimhaltung.

Auch diese Dokumentensammlung kann wieder über unsere Webseite abgerufen werden.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließung zwischen der 84. und 85. Konferenz (vom 25. Januar 2013)

Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

– Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.

– Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.

– Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken

außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.

– Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.

– Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

– Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

2. Entschließungen der 85. Konferenz am 13./14. März 2013 in Bremerhaven

Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.

- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.

- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.

- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.

- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.

- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.

- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen

und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.

- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

Erläuterungen

zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven „Europa muss den Datenschutz stärken“

- **Jedes personenbeziehbare Datum muss geschützt werden**

Nach Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z. B. IP-Adressen, Kenn-Nummern, Standortdaten ein.

- **Es darf keine grundrechtsfreien Räume geben**

Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

- **Einwilligungen müssen ausdrücklich erteilt werden**

Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willens-

bekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäische Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11,12) darf es – auch mit Blick auf Artikel 8 Abs. 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

- **Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**

Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Artikel 8 Abs. 2 der Grundrechtecharta – das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

- **Profilbildung muss beschränkt werden**

Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**

Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abge-

schwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**

Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**

Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

- **Grundrechtsschutz braucht effektive Kontrollen**

Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von

der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

- **Hoher Datenschutzstandard für ganz Europa**

Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandeneRechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit undPersönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von

Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

Anlage zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.

- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.

- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.

- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.

- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

3. Entschließung zwischen der 85. und 86. Konferenz (vom 5. September 2013)

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u. a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es, „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.

- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

  Dazu gehört,

  – zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.

  – sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.

  – die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.

- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.

- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

4. Entschließungen der 86. Konferenz am 1./2. Oktober 2013 in Bremen

Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit

der Kommunikation und der Privatsphäre rückt – wie repräsentative Studien belegen – mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste[1].

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden[2].

- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.[3]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

---

[1] Siehe dazu die Entschließungen „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ und „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“.

[2] Siehe dazu die heutige Entschließung „Stärkung des Datenschutzes im Sozial- und Gesundheitswesen“.

[3] Siehe dazu die heutige Entschließung „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“.

Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU-Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerkenund Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von „gläsernen Patientinnen und Patienten oder Versicherten“ weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein

berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung „Sicherheit bei E-Government durch Nutzung des Standards OSCI“ Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätzesich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

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

1. Beschluss der Sitzung am 26./27. Februar 2013 in Düsseldorf

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 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.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte

der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit „Unfallkameras“, wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

2. Beschluss der Sitzung am 11./12. September 2013 in Düsseldorf

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z. B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

III. Europäische Konferenz der Datenschutzbeauftragten

Lissabon, 16./17. Mai 2013

Entschließung über die Zukunft des Datenschutzes in Europa

Der Datenschutz und der Schutz der Privatsphäre in Europa befinden sich momentan an einem wichtigen Wendepunkt, der markiert wird durch die Überarbeitung des Übereinkommens Nr. 108 des Europarates und der EU-Datenschutz-Richtlinie, zweier Hauptinstrumente, die die Eckpfeiler des Datenschutzes in ganz Europa darstellen.

Es ist daher an der Zeit, Bilanz zu ziehen und die Gelegenheit wahrzunehmen, zukünftige Herausforderungen zu bewältigen und den Weg zur Stärkung der Standards und der Effektivität des Datenschutzes in einer globalisierten Welt konsequent weiter zu beschreiten. Dies ist keine leichte Aufgabe und erfordert die engagierte Beteiligung aller Akteure in diesem dynamischen Prozess, mit besonderer Bedeutung für die Rolle der Datenschutzbehörden, die in erster Linie Behörden der Gewährleistung der Rechte des Einzelnen sind.

Die Modernisierung des Übereinkommens Nr. 108 und die EU-Datenschutzreform bieten Europa die Chance, auf den Erfahrungen für eine bessere Gestaltung der Zukunft aufzubauen, indem die in unserer Tradition verankerten hohen Werte und Prinzipien bestmöglich bei der Fortentwicklung des Schutzes der Privatsphäre in einer in technologischer und gesellschaftlicher Hinsicht grundlegend veränderten Welt gewahrt bleiben. Die jetzt getroffenen Entscheidungen werden in den kommenden Jahren große Auswirkungen auf das Grundrecht der Bürger auf Datenschutz haben. Darüber hinaus gefährdet das Versäumnis, die Privatsphäre zu schützen, andere Rechte und Freiheiten, wie das Recht auf Nichtdiskriminierung, das Recht auf Freizügigkeit, das Recht auf Anonymität, das Recht auf freie Meinungsäußerung und letztlich die Menschenwürde. Zur Gewährleistung der wirksamen Ausübbarkeit der Grundrechte in einer demokratischen Gesellschaft ist es erforderlich, dass die notwendigen Garantien bestehen und jederzeit tatsächlich wahrgenommen werden können.

Im vollen Bewusstsein ihrer Aufgabe der Sicherung eines Grundrechts verpflichten sich die europäischen Datenschutzbeauftragten, weiterhin aktiv zur Entwicklung des Datenschutzes in allen Lebensbereichen in Europa beizutragen.

Die Konferenz der auf der Frühjahrskonferenz in Lissabon zusammen gekommenen europäischen Datenschutzbehörden

- fordert die europäischen Staaten, den Europarat und die Europäische Union auf, die Gelegenheit zur Überprüfung des Rechtsrahmens für den Datenschutz zu ergreifen, um die Rechte des Einzelnen zu stärken und einen wirksamen Schutz ihrer Privatsphäre in einer hoch technisierten und globalisierten Welt zu gewährleisten;

- bekräftigt die Notwendigkeit, einen einheitlichen und robusten Datenschutzrechtsrahmen zu entwickeln, der das gleiche Schutzniveau sowohl für den privaten als auch den öffentlichen Sektor gewährt, unter Berücksichtigung der erforderlichen spezifischen Regelungen auf dem Gebiet der Strafverfolgung;

- äußert ihre tiefe Besorgnis darüber, dass unterschiedliche Strömungen bei der Reform des EU-Datenschutzes die Möglichkeit eröffnen, dass der Bereich der Strafverfolgung dem praktischen Schutzbereich des Grundrechts auf Datenschutz entzogen wird;

- fordert die EU-Gesetzgeber auf, zur Vermeidung einer gefährlichen rechtlichen Lücke im Datenschutz die Datenschutzverordnung und die Richtlinie gleichzeitig zu verabschieden, insbesondere in Anbetracht der zunehmenden Weiterverwendung von privaten Stellen verarbeiteter personenbezogener Daten zu Strafverfolgungszwecken.

- appelliert an den Europarat und die Europäischen Union, den datenschutzrechtlichen Herausforderungen durch das Internet entschiedener zu begegnen durch Schaffung von Klarheit und Sicherheit für Unternehmen und betroffene Personen sowie die Entwicklung angemessener Schutzmechanismen für einen wirksamen Schutz der Rechte der Einzelnen und eine praktische Durchsetzung durch Datenschutzbehörden.

- ermutigt Unternehmen und Behörden und alle, die in Politik und Recht am Datenschutz beteiligt sind, sich um Datensicherheit als eine der wichtigsten Prioritäten der Datenverarbeitungstätigkeiten zu bemühen und darin zu investieren, damit die steigenden Risiken von Datenschutzverletzungen in der digitalen Welt bekämpft und die Privatsphäre der Bürger aktiv geschützt wird.

- betont die Notwendigkeit, angesichts der Entwicklung neuer Geschäftsmodelle die Kooperationsmechanismen zwischen den Datenschutzbehörden zu stärken und einen gemeinsamen Ansatz und Handlungsmöglichkeiten zu finden, um den Schutz der Rechte der Einzelnen in der Praxis zu gewährleisten, wobei die Unabhängigkeit der Datenschutzbehörden wechselseitig zu achten ist.

- unterstreicht die Notwendigkeit der angemessenen Verstärkung der regelmäßigen Zusammenarbeit und Unterstützung der Datenschutzbehörden auf EU-Ebene als Reaktion auf die erheblichen Anforderungen des enorm gewachse-

nen Austauschs personenbezogener Daten mittels zentraler oder dezentraler IT-Systeme sowie des grenzüberschreitenden Informationsaustauschs insbesondere durch die Strafverfolgungsbehörden, so dass die Datenschutzbehörden die Einhaltung des Datenschutzes besser kontrollieren können.

- bekräftigt die Wichtigkeit, die Datenschutzbehörden mit ausreichenden Befugnissen, Kompetenzen, finanziellen Mitteln und Ressourcen auszustatten, damit sie ihre Kontrolltätigkeiten in unabhängiger Art und Weise vollständig erfüllen können und damit sie in der Lage sind, den Schutz des Grundrechts der Bürger auf Datenschutz und Schutz der Privatsphäre zu gewährleisten.

- ermuntert alle Beteiligten, sich an der Diskussion zur Zukunft des Datenschutzes in Europa zu beteiligen und hierzu beizutragen.

Entschließung zur „Gewährleistung des Datenschutzes in einer transatlantischen Freihandelszone“

Sponsoren:
Comissão Nacional de Protecção de Dados (CNPD), Portugal
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Deutschland

Unterstützt von:
Commission Nationale de l’Informatique et des Libertés (CNIL), Frankreich
Garante per la protezione dei dati personali (Garante), Italien
Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO), Polen
Agencia Espanola de Protección de Datos (AEPD), Spanien

Da ein vom US-Präsidenten angekündigtes Freihandelsabkommen mit den Vereinigten Staaten von der Europäischen Union begrüßt wird und es zahlreiche Hinweise darauf gibt, dass eine solche transatlantische Freihandelszone wirtschaftliche Vorteile für beide Volkswirtschaften bringt,

- erinnert die Konferenz daran, dass nach den Standards der Welthandelsorganisation (Allgemeines Abkommen über den Handel mit Dienstleistungen, Artikel XIV) Staaten berechtigt sind, die zur Gewährleistung des Schutzes personenbezogener Daten erforderlichen Maßnahmen zu verabschieden und durchzusetzen;

- begrüßt die Konferenz die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz;

- vertritt die Konferenz die Auffassung, dass, soweit sich die bevorstehenden Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über die transatlantische Freihandelszone auf Fragen des Datenschutzes auswirken könnten, das in der Europäischen Grundrechtecharta verankerte Grundrecht auf Datenschutz und die daraus abgeleiteten hohen Standards gefördert und eingehalten werden sollten;

- weist die Konferenz darauf hin, dass jede diesbezügliche Regelung sowohl „inhaltliche" Grundsätze als auch Verfahrenserfordernisse wie zum Beispiel Regelungen zur Zweckbindung und Weitergabe von Daten, effektive Kontrolle durch eine unabhängige Behörde sowie Zugang zu behördlichen und gerichtlichen Rechtsbehelfen beinhalten muss. Die Frage nach den Möglichkeiten direkten Zugriffs auf Daten von privater Unternehmen durch Strafverfolgungs- und Sicherheitsbehörden außerhalb der EU sollte ebenfalls angemessen thematisiert werden;

- betont die Konferenz, dass auch in einer transatlantischen Wirtschaftsunion die Anwendung der nach europäischem Recht garantierten Grundrechte sichergestellt werden muss. Die Verhandlungen sollen sich nicht auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken;

- erwartet die Konferenz, dass die inspirierende Idee eines transatlantischen umfassenden Handelsabkommens nicht nur das Wirtschaftswachstum erhöhen, sondern auch die Bemühungen für ein hohes Maß an Datenschutz in den USA und in der Europäischen Union voranbringen wird. Dabei darf man nicht vergessen, dass Datenschutz weltweit als ein erheblicher Wettbewerbsvorteil anerkannt wird.

Entschließung zur Sicherstellung eines angemessenen Datenschutzniveaus bei Europol

Sponsoren:
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Deutschland
College Bescherming Persoonsgegevens (CBP), Niederlande
Garante per la protezione dei dati personali (Garante), Italien
Comissão Nacional de Protecção de Dados (CNPD), Portugal

Am 27. März 2013 hat die Europäische Kommission einen Vorschlag für eine Verordnung gemäß Artikel 88 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) vorgestellt. Dieser Verordnungsentwurf ändert inhaltlich grundlegend und weitreichend die geltende Rechtsgrundlage für das Europäische

Polizeiamt (Europol) – den Beschluss des Rates vom 6. April 2009 zur Errichtung Europols (2009/371/JI – ABl. L 121/37). Hierzu erklärt die Konferenz:

Mit der neuen Rechtsgrundlage soll Europol neue Aufgaben wahrnehmen und zusätzliche Befugnisse erhalten. Nach dem Willen der Kommission soll die Datenverarbeitung Europols nicht länger gemäß den im geltenden Recht definierten Systemen und Dateien erfolgen, um die Möglichkeiten Europols für eine Verknüpfung der Daten aus bzw. mit unterschiedlichen Systemen nicht zu behindern. Mit dem Verordnungsentwurf soll die Analysetätigkeit Europols in größtmöglicher Weise flexibilisiert werden, da die Analyse nach Ansicht der Kommission der „Grundpfeiler“[1] der modernen, „informationsauswertenden“[2] Strafverfolgungstätigkeit ist.

Angesichts der erweiterten Möglichkeiten zur Verarbeitung personenbezogener Daten muss für Europol der Datenschutz auf hohem Niveau gewährleistet werden. Dies ergibt sich auch aus Art. 8 der Europäischen Grundrechtecharta, der hohe Anforderungen an den Schutz der Privatsphäre und personenbezogener Daten stellt. Einrichtungen der EU, die – wie Europol – in großem Umfang personenbezogene Daten verarbeiten, sind diesen Vorgaben in besonderer Weise verpflichtet.

Keinesfalls wäre es hinzunehmen, wenn die neue Rechtsgrundlage das bestehende Datenschutzniveau absenken würde. Genau dies ist aber zu befürchten – legt man den von der Kommission vorgelegten Entwurf zu Grunde. Mit dem Wegfall der bestehenden Europol-Systeme und -Dateien würden systemspezifische Sicherungen entfallen, wie z. B. die im Europol-Beschluss und den Begleitregelungen enthaltenen engen Zweckbegrenzungen und Vorgaben für die Verarbeitung personenbezogener Daten in Analysedateien. Es scheint, als sollten durch den Kommissionsvorschlag bestehende Verfahrenssicherungen eingeschränkt sowie geltende Beschränkungen für die Datenübermittlung an Drittstaaten und -stellen aufgehoben werden.

Die Konferenz der europäischen Datenschutzbeauftragten fordert das Europäische Parlament, den Rat, und die Kommission auf, dafür zu sorgen, dass die neue Rechtsgrundlage für Europol den folgenden Anforderungen entspricht und dass die Kommissionsvorschläge in diesem Sinne nachgebessert werden.

1. Daten unschuldiger Personen (Opfer, Zeugen, Kontaktpersonen etc.) dürfen nur unter sehr strengen Voraussetzungen verarbeitet werden und bedürfen dabei besonderen Schutzes.

[1] „Cornerstone“ (öffentliches Memo der Europäischen Kommission vom 27. März 2013, (Memo/13/286) „Questions and Answers: Enhancing Europol´s support to law enforcement cooperation and training“, S. 1).

[2] „intelligence-led“ (a.a.O.)

2. Betroffenenrechte.
3. Verfahrensgarantien.
4. Unabhängige und effiziente Datenschutzkontrolle, sowohl extern als auch innerhalb von Europol, zur Gewährleistung eines effizienten Datenschutzes unter aktiver Beteiligung der nationalen Datenschutzbehörden.
5. Ein angemessenes Datenschutzniveau bei der Kooperation mit Drittstaaten und mit sonstigen Stellen außerhalb der EU.
6. Eine strenge Zweckbindung für die Verarbeitung personenbezogener Daten.

IV. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Arbeitsdokument 02/2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsdatenverarbeiter (WP 195)

Angenommen am 6. Juni 2012

Einführung

Die nach Artikel 29 gebildete Datenschutzgruppe hat bereits einige Instrumente[1] entwickelt, um die Anwendung verbindlicher unternehmensinterner Datenschutzregelungen (BCR) durch die für die Verarbeitung Verantwortlichen (BCR für die eigenen Daten) zu vereinfachen: Mit diesen Regelungen sollten Vorgaben für die Übermittlung personenbezogener Daten gemacht werden, die ursprünglich von dem Unternehmen in seiner Funktion als für die Verarbeitung Verantwortlicher verarbeitet wurden (etwa Daten, die seine Kunden, seine Angestellten usw. betreffen.).

In diesem Arbeitsdokument will die nach Artikel 29 gebildete Datenschutzgruppe ein Instrumentarium zur Vereinfachung der Anwendung verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (BCR für die Daten Dritter) entwickeln; sie beschreibt darin die Bedingungen, die diesbezüglich erfüllt sein müssen.

Mit den BCR für Auftragsverarbeiter soll ein Rahmen für die Übermittlung personenbezogener Daten ins Ausland vorgegeben werden, die ursprünglich von dem Unternehmen in seiner Funktion als Auftragsverarbeiter im Einklang mit den externen Anweisungen eines für die Verarbeitung Verantwortlichen (etwa bei ausgelagerten Tätigkeiten) verarbeitet wurden.

Nach der Richtlinie 95/46/EG sollte zwischen einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter ein Vertrag geschlossen werden. Nachstehend wird ein solcher Vertrag als „Dienstevereinbarung“ bezeichnet.

[1] Siehe die Arbeitsdokumente WP153 (Instrumentarium zur Überprüfung der Frage, ob alle Bedingungen erfüllt sind), WP155 (häufig gestellte Fragen), WP 154 (Beispiel für BCR) sowie die Arbeitsdokumente WP 74 und 108 (Datenherkunft).

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
1 – BINDUNG IM INNENVERHÄLTNIS			
1.1 Pflicht zur Einhaltung der BCR	JA	JA	Die BCR müssen für alle Mitglieder der Unternehmensgruppe und für alle Beschäftigten eine klare Pflicht zur Einhaltung der BCR begründen. In den BCR muss ausdrücklich bestimmt sein, dass alle Mitglieder der Unternehmensgruppe und die Beschäftigten die Anweisungen bezüglich der Datenverarbeitung sowie die Sicherheits- und Vertraulichkeitsmaßnahmen entsprechend der Dienstevereinbarung (Art. 17 der Richtlinie) befolgen müssen.
1.2 Erläuterung, wie die Verbindlichkeit der BCR gegenüber den Mitgliedern der Unternehmensgruppe und den Beschäftigten garantiert wird	NEIN	JA	In ihrem Antrag muss die Unternehmensgruppe erläutern, wie die Verbindlichkeit der BCR garantiert werden soll: i) im Verhältnis zwischen den Unternehmen/Unternehmensteilen der Gruppe durch Vereinbarungen innerhalb der Gruppe, einseitige Erklärungen/Verpflichtungen, interne Regelungen, Unternehmensgrundsätze oder andere Maßnahmen; ii) gegenüber den Beschäftigten durch individuelle Vereinbarung/Verpflichtung mit Sanktionen, Klausel in Arbeitsverträgen mit Sanktionen, interne Unternehmensgrundsätze mit Sanktionen oder tarifvertragliche Vereinbarungen mit Sanktionen
AUSSENVERHÄLTNIS			
1.3 Drittbegünstigung für Betroffene einschließlich der Möglichkeit der Beschwerde bei den zuständigen Datenschutzbehörden und der gerichtlichen Klage (wahlweise am Gerichtsstand des Auftragsverarbeiters des EU-Datenexporteurs/der EU-Hauptniederlassung des Auftragsverarbeiters / des Mitglieds, das in der EU für den Datenschutz zuständig ist/des für die Verarbeitung Verantwortlichen in der EU; sofern diese Fälle nicht anwendbar sind, Gerichtsstand am Aufenthaltsort der betroffenen Person)	JA	JA	Die BCR müssen den betroffenen Personen als Drittbegünstigte Durchsetzungsrechte in dem Fall einräumen, dass sie nicht in der Lage sind, Ansprüche gegen den für die Verarbeitung Verantwortlichen geltend zu machen, weil dessen Unternehmen faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des für die Verarbeitung Verantwortlichen übernommen; in letzterem Fall kann die betroffene Person ihre Rechte gegenüber dem Rechtsnachfolger geltend machen. Zu den Rechten der betroffenen Personen zählen die gerichtlichen Rechtsbehelfe bei Verstoß gegen garantierte Rechte und Schadenersatzansprüche (aufgrund eines materiellen oder immateriellen Schadens). Eine betroffene Person hat das Recht, eine Beschwerde bei der Datenschutzbehörde oder dem Gericht einzulegen, die bzw. das für den für die Verarbeitung Verantwortlichen in der EU zuständig ist. Ist dies aus den vorstehend genannten Gründen nicht möglich, so kann die betroffene Person rechtliche Schritte bei der Datenschutzbehörde oder bei dem Gericht einleiten, das für das in der EU befindliche Unternehmen des Auftragsverarbeiters am Herkunftsort der Übermittlung oder die EU-Hauptniederlassung des Auftragsverarbeiters oder das EU-Mitglied, dem Verantwortlichkeiten des Auftragsverarbeiters für den

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Datenschutz übertragen sind, zuständig ist. Treffen diese Situationen nicht zu, ist die betroffene Person berichtigt, vor dem Gericht an ihrem Aufenthaltsort Beschwerde einzulegen. Sieht das innerstaatliche Recht eine günstigere Lösung für die betroffene Person vor, so wäre diese anwendbar. Das Recht als Drittbegünstigter betrifft die Ziffern 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2 und 6.3
1.4. Verantwortung gegenüber dem für die Verarbeitung Verantwortlichen	JA	JA	Die BCR werden gegenüber dem für die Verarbeitung Verantwortlichen durch ausdrücklichen Verweis auf sie in der Dienstevereinbarung verbindlich gemacht. In den BCR muss außerdem festgelegt werden, dass die für die Verarbeitung Verantwortlichen das Recht haben, die BCR gegenüber jedem Unternehmen wegen Verstößen, die ihm zuzurechnen sind, durchzusetzen, ferner gegenüber dem unter Ziffer 1.5 genannten Unternehmen wegen eines Verstoßes gegen die BCR oder der Dienstevereinbarung durch Mitglieder, für die die BCR für Auftragsverarbeiter außerhalb der EU gelten, oder wegen eines Verstoßes gegen die schriftliche Vereinbarung gemäß Ziffer 6.1.vii durch einen der externen Unterauftragsverarbeiter außerhalb der EU. Zu den Rechten der für die Verarbeitung Verantwortlichen zählen die gerichtlichen Rechtsbehelfe und Schadenersatzansprüche.
1.5 Das Unternehmen akzeptiert die Pflicht zur Leistung von Schadenersatz und zur Abhilfe bei Verstößen gegen die BCR.	JA	JA	In den BCR muss festgelegt werden, dass die EU-Hauptniederlassung des Auftragsverarbeiters oder das in der EU haftende Mitglied des Auftragsverarbeiters oder der Auftragsverarbeiter des EU-Datenexporteurs (z. B. die Vertragspartei des für die Verarbeitung Verantwortlichen in der EU) verpflichtet sind, die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU, die an die BCR gebunden sind, oder für Verstöße externer Unterauftragsverarbeiter außerhalb der EU zu übernehmen, Verstößen gegen die BCR abzuhelfen und Schadenersatz zu leisten. Dieses Mitglied akzeptiert, dass es haftet, als ob die Verletzung durch ihn in dem Mitgliedstaat erfolgt wäre, in dem es niedergelassen ist, und nicht durch das Mitglied der Unternehmensgruppe außerhalb der EU oder den externen Unterauftragsverarbeiter außerhalb der EU. Zum Ausschluss der eigenen Haftung kann sich dieses Mitglied nicht darauf berufen, dass der Verstoß gegen seine Pflichten durch einen (internen oder externen) Unterauftragsverarbeiter (der Unternehmensgruppe) begangen wurde. Sofern kein Mitglied des an die BCR gebundenen Auftragsverarbeiters in der EU niedergelassen ist, übernimmt die (außerhalb der EU befindliche) Hauptniederlassung der Unternehmensgruppe diese Haftung. In diesem Fall haben die betroffenen Personen und der für die Verarbeitung Verantwortliche das Recht, eine Beschwerde bei der Datenschutzbehörde oder den Gerichten am Ort des Aufenthalts bzw. der Niederlassung einzulegen.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
1.6 Das Unternehmen verfügt über ausreichende Mittel.	NEIN	JA	Dem Antrag muss eine Bestätigung beigefügt sein, wonach das Unternehmen, das die Haftung für Handlungen anderer Mitglieder außerhalb der EU, die an die BCR gebunden sind, und für externe Unterauftragsverarbeiter außerhalb der EU übernommen hat, über ausreichende Mittel verfügt, um den Schaden zu ersetzen, der aus einer Verletzung der BCR entstanden ist.
1.7 Die Beweislast trägt das Unternehmen, nicht die betroffene Person.	JA	JA	Aus den BCR muss Folgendes hervorgehen: Wenn eine betroffene Person oder der für die Verarbeitung Verantwortliche nachweisen kann, dass sie bzw. er geschädigt wurde, und Tatsachen vorbringt, aus denen hervorgeht, dass der Schaden wahrscheinlich wegen des Verstoßes gegen die BCR entstanden ist, muss dasjenige Mitglied der Unternehmensgruppe, das die Haftung übernommen hat, nachweisen, dass der Verstoß gegen die BCR, durch den der Schaden verursacht wurde, nicht dem außerhalb Europas ansässigen Mitglied der Unternehmensgruppe oder dem externen Unterauftragsverarbeiter zuzurechnen ist, oder dass ein solcher Verstoß nicht stattfand[2]. Kann das Unternehmen, das die Haftung übernommen hat, nachweisen, dass die schadensbegründende Handlung nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist, so ist es selbst von der Haftung befreit.
1.8 Die BCR sind für die betroffenen Personen leicht zugänglich. Gleiches gilt für Informationen über die Rechte der Betroffenen als Drittbegünstigte.	JA	NEIN	Zugang für den für die Verarbeitung Verantwortlichen: Mit der Dienstevereinbarung ist dafür gesorgt, dass die BCR Bestandteil des Vertrags sind. Die BCR werden der Dienstevereinbarung als Anlage beigefügt oder es wird auf sie und die Möglichkeit des elektronischen Zugangs verwiesen. Zugang für betroffene Personen: Die BCR sind auf der Website der Unternehmensgruppe des Auftragsverarbeiters dergestalt zu veröffentlichen, dass sie für betroffene Personen leicht zugänglich sind, oder es ist dort zumindest eine Unterlage zu veröffentlichen, die alle Informationen zu den Ziffern 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2 und 6.3 (und nicht eine Zusammenfassung der Informationen) enthält.
2 – WIRKSAMKEIT			
2.1 Geeignete Schulungsprogramme	JA	JA	In den BCR muss festgelegt sein, dass die Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, eine geeignete Schulung zur Anwendung der BCR erhalten. Die Datenschutzbehörden, die den Antrag auf Genehmigung der BCR prüfen, können verlangen, dass das Schulungsprogramm, das im Antrag anzugeben ist, anhand von Beispielen oder anderweitig erläutert wird.

[2] Siehe auch die häufig gestellte Frage Nr. 11 in dem Arbeitsdokument WP 155, in der es um die BCR für den für die Verarbeitung Verantwortlichen geht.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
2.2 Beschwerdeverfahren	JA	JA	Der Auftragsverarbeiter der Unternehmensgruppe muss sich in den BCR verpflichten, eigens einen Kontaktstelle für betroffene Personen vorzusehen. Alle Mitglieder, die an die BCR gebunden sind, müssen sich verpflichten, die Beschwerde oder Anfrage unverzüglich dem für die Verarbeitung Verantwortlichen mitzuteilen; sie selbst sind nicht verpflichtet, die Beschwerde oder Anfrage zu bearbeiten (es sei denn, mit dem für die Verarbeitung Verantwortlichen wurde etwas anders vereinbart). Der Auftragsverarbeiter muss sich in den BCR verpflichten, Beschwerden von betroffenen Personen zu bearbeiten, wenn das Unternehmen des für die Verarbeitung Verantwortlichen faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist. Die Bearbeitung von Beschwerden durch den Auftragsverarbeiter muss in jedem Fall durch eine klar benannte Abteilung oder Person geschehen, die bei der Wahrnehmung ihrer Aufgaben hinreichend unabhängig ist. In diesen Fällen ist die betroffene Person darüber zu informieren, – wo die Beschwerde einzureichen ist, – in welcher Form, – wie lange die Behandlung der Beschwerde dauern wird, – welche Folgen die Ablehnung der Beschwerde hat, – welche Folgen die Anerkennung der Beschwerde hat, – welche Rechtsbehelfe der betroffenen Person zur Verfügung stehen, wenn sie mit der Behandlung ihrer Beschwerde nicht zufrieden ist (Einlegung eines Rechtsbehelfs bei Gericht/der Datenschutzbehörde).
2.3 BCR-Audit	JA	JA	In den BCR muss festgeschrieben sein, dass die Unternehmensgruppe verpflichtet ist, regelmäßig oder auf Antrag des Datenschutzbeauftragten (oder einer anderen zuständigen Stelle im Unternehmen) Datenschutzaudits durchzuführen (entweder durch interne oder durch externe akkreditierte Auditoren). Aus den BCR muss hervorgehen, dass sich das Auditprogramm auf alle Aspekte der BCR erstreckt und Verfahren vorsieht, mit denen sichergestellt wird, dass Abhilfemaßnahmen getroffen werden. In den BCR ist ferner festzuhalten, dass das Ergebnis des Audits dem Datenschutzbeauftragten/der Datenschutzabteilung des Unternehmens sowie dem Aufsichtsrat der Muttergesellschaft mitgeteilt wird, aber auch dem für die Verarbeitung Verantwortlichen verfügbar gemacht wird. Ferner ist in den BCR vorzusehen, dass den Datenschutzbehörden, die für den für die Verarbeitung Verantwortlichen zuständig sind, auf Antrag Zugang zu den Ergebnissen des Audits zu gewähren ist und dass sie berechtigt sind, bei Bedarf und sofern dies rechtlich möglich ist, selbst einen Datenschutzaudit durchzuführen.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Jeder Auftragsverarbeiter oder Unterauftragsverarbeiter, der die Daten eines bestimmten, für die Verarbeitung Verantwortlichen verarbeitet, erklärt sich bereit, auf Verlangen dieses für die Verarbeitung Verantwortlichen seine Datenverarbeitungseinrichtungen zur Prüfung derjenigen Datenverarbeitungstätigkeiten zur Verfügung zu stellen, die mit dem betreffenden, für die Verarbeitung Verantwortlichen zu tun haben. Dieses Audit wird von dem für die Verarbeitung Verantwortlichen oder einem Prüfgremium durchgeführt, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind; das Prüfgremium wird von dem die Verarbeitung Verantwortlichen ausgewählt, gegebenenfalls in Absprache mit der Datenschutzbehörde. Dem Antrag ist eine Beschreibung des Auditsystems beizufügen. Darin ist zum Beispiel anzugeben, – welche Abteilung innerhalb des Unternehmens über den Auditplan/das Auditprogramm entscheidet, – welche Abteilung das Audit durchführt, – wann das Audit durchgeführt wird (regelmäßig oder auf Antrag des Datenschutzbeauftragten), – welchen Umfang das Audit hat (z. B. Anwendungen, IT-Systeme, Datenbanken, in denen Personaldaten verarbeitet werden, oder Weiterübermittlungen, Beschlüsse im Hinblick auf zwingende Erfordernisse nach nationalem Recht, die den BCR entgegenstehen, Überprüfung der Vertragsklauseln, auf deren Grundlage Daten an für die Verarbeitung Verantwortliche oder Auftragsverarbeiter außerhalb der Unternehmensgruppe übermittelt werden, Abhilfemaßnahmen usw.); – wer die Auditergebnisse erhält.
2.4 Einrichtung eines Stabs von Datenschutzbeauftragten oder sonstigen befähigten Mitarbeitern, die Beschwerden bearbeiten, die Vorschriften überwachen und für deren Einhaltung sorgen.			Selbstverpflichtung des Unternehmens, einen Mitarbeiterstab zu bilden (z. B. ein Netz von Datenschutzbeauftragten), der mit Unterstützung der Unternehmensspitze die Einhaltung der Vorschriften überwacht und gewährleistet. Kurze Beschreibung der Struktur, Aufgaben und Zuständigkeiten des Stabs der Mitarbeiter/Datenschutzbeauftragten o. ä., die die Einhaltung der BCR gewährleisten sollen. Z. B.: Der oberste Datenschutzbeauftragte berät die Unternehmensleitung, ist zuständig bei Untersuchungen der Datenschutzbehörden, berichtet jährlich über die Anwendung der BCR, sorgt auf Unternehmensebene für die Einhaltung der BCR. Die Datenschutzbeauftragten berichten dem obersten Datenschutzbeauftragten über größere Probleme beim Datenschutz und sorgen für die Einhaltung der Vorschriften auf lokaler Ebene.

3 – KOOPERATIONSPFLICHT			
3.1 Pflicht zur Zusammenarbeit mit den Datenschutzbehörden	JA	JA	Die BCR müssen alle Mitglieder, die an die BCR gebunden sind, unmissverständlich dazu verpflichten, mit den Datenschutzbehörden, die für den betreffenden, für die

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Verarbeitung Verantwortlichen zuständig sind, zusammenzuarbeiten, deren Prüfungen zu dulden und ihren Mitteilungen, die die Anwendung der BCR betreffen, nachzukommen.
3.2 Pflicht zur Zusammenarbeit mit dem für die Verarbeitung Verantwortlichen			Die BCR müssen alle Auftragsverarbeiter oder Unterauftragsverarbeiter unmissverständlich dazu verpflichten, mit dem für die Verarbeitung Verantwortlichen zusammenzuarbeiten und ihn bei der Einhaltung der Datenschutzvorschriften zu unterstützen (z. B. bei der Erfüllung seiner Pflicht, die Rechte der betroffenen Personen zu wahren oder ihre Beschwerden zu bearbeiten oder auf eine Untersuchung oder Anfrage der Datenschutzbehörden zu reagieren). Dies hat binnen angemessener Frist und in dem Umfang zu geschehen, in dem dies vernünftigerweise möglich ist.
4 – BESCHREIBUNG DER DATENVERARBEITUNG UND DES DATENVERKEHRS			
4.1 Beschreibung der Übermittlungsvorgänge, die unter die BCR fallen, und des materiellen Anwendungsbereichs der BCR	JA	JA	Die BCR müssen ein Verzeichnis der Unternehmen enthalten, die an sie gebunden sind (siehe auch Ziffer 6.2) Der Auftragsverarbeiter, der BCR vorlegt, muss der Datenschutzbehörde auch eine allgemeine Beschreibung ihres materiellen Anwendungsbereichs beifügen (voraussichtliche Art der übermittelten Daten, voraussichtlicher Zweck sowie Datenimporteure/-exporteure innerhalb und außerhalb der EU).
4.2 Erklärung zum räumlichen Geltungsbereich der BCR (Art der Daten, Art der betroffenen Personen, Länder)	JA	JA	Aus den BCR muss hervorgehen, dass es Sache des für die Verarbeitung Verantwortlichen ist, die BCR anzuwenden i) auf alle personenbezogenen Daten, die für die Zwecke der Tätigkeit des Auftragsverarbeiters verarbeitet werden und dem EU-Recht unterliegen (z. B. von der Europäischen Union übermittelte Daten) ODER ii) auf jedwede Verarbeitung von Daten, die für die Zwecke der Tätigkeit des Auftragsverarbeiters in der Unternehmensgruppe verarbeitet werden, ungeachtet der Herkunft der Daten.
5 – SYSTEM FÜR DIE MELDUNG UND ERFASSUNG VON ÄNDERUNGEN			
5.1 Verfahren zur Aktualisierung der BCR	JA	JA	Die BCR können geändert werden *(z. B. zur Anpassung an eine Änderung der gesetzlichen Regelungen oder der Unternehmensstruktur)*, sie müssen jedoch eine Pflicht zur Meldung solcher Änderungen gegenüber allen Mitgliedern der Unternehmensgruppe, den Datenschutzbehörden und dem für die Verarbeitung Verantwortlichen vorsehen.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Betrifft eine Änderung die Verarbeitungsbedingungen, so sollte der für die Verarbeitung Verantwortliche hierüber so rechtzeitig informiert werden, dass es ihm möglich ist, einen Einwand gegen die Änderung vorzubringen oder von dem Vertrag zurückzutreten, bevor die Änderung vorgenommen wird (z. B. beabsichtigte Änderungen wegen Hinzufügen oder Ersatz von Unterauftragnehmern, bevor die Daten dem neuen Unterauftragsverarbeiter übermittelt werden). Unter folgenden Voraussetzungen sind Aktualisierungen der BCR oder der Liste der Mitglieder, die an die BCR gebunden sind, möglich, ohne eine neue Genehmigung beantragen zu müssen: i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder und der Unterauftragsverarbeiter führt, die an der Datenverarbeitungstätigkeit des für die Verarbeitung Verantwortlichen mitwirken; diese Liste ist dem für die Verarbeitung Verantwortlichen, den betroffenen Personen und den Datenschutzbehörden verfügbar zu machen. ii) Diese Person erfasst alle Aktualisierungen der BCR, macht die notwendigen Informationen dem für die Verarbeitung Verantwortlichen systematisch verfügbar und erteilt den Datenschutzbehörden auf Anfrage diesbezügliche Auskünfte. iii) Einem neuen Mitglied der Unternehmensgruppe dürfen personenbezogene Daten erst dann übermittelt werden, wenn dieses neue Mitglied an die BCR gebunden und die Einhaltung der Vorschriften gewährleistet ist. iv) Signifikante Änderungen der BCR oder der Mitgliederliste müssen den für die Genehmigung zuständigen Datenschutzbehörden jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.
6 – DATENSCHUTZ-GARANTIEN			
6.1 Beschreibung der Datenschutzgrundsätze, einschließlich der Vorschriften für die Datenübermittlung und die Weiterübermittlung aus der EU in Drittländer	JA	JA	Die BCR müssen die folgenden Grundsätze enthalten, die auf jedes Mitglied, das an die BCR gebunden ist, anzuwenden sind: i) Transparenz und Fairness: Die Auftragsverarbeiter und Unterauftragsverarbeiter sind generell verpflichtet, den für die Verarbeitung Verantwortlichen bei der Einhaltung der Rechtsvorschriften zu unterstützen (z. B. indem sie die Tätigkeiten der Unterauftragsverarbeiter transparent machen, damit der für die Verarbeitung Verantwortliche die betroffenen Personen ordnungsgemäß unterrichten kann). ii) Beschränkung der Zweckbestimmung: Es besteht ausschließlich die Pflicht zur Verarbeitung der personenbezogenen Daten im Auftrag des für die Verarbeitung Verantwortlichen und in Übereinstimmung mit dessen Anweisungen. Kann der Auftragsverarbeiter oder Unterauftragsverarbeiter dies aus irgendwelchen

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Gründen nicht einhalten, so muss er sich bereit erklären, den für die Verarbeitung Verantwortlichen unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten. Bei Beendigung der Datenverarbeitungsdienste müssen die Auftragsverarbeiter und Unterauftragsverarbeiter je nach Wunsch des für die Verarbeitung Verantwortlichen alle übermittelten personenbezogenen Daten und deren Kopien an den für die Verarbeitung Verantwortlichen zurückschicken oder alle personenbezogenen Daten zerstören und dem für die Verarbeitung Verantwortlichen bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der die Auftragsverarbeiter und Unterauftragsverarbeiter unterliegen, diesen die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall teilen die Auftragsverarbeiter und Unterauftragsverarbeiter dem für die Verarbeitung Verantwortlichen dies mit und garantieren ihm, dass sie die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleisten und diese Daten nicht mehr aktiv weiterverarbeiten. iii) Datenqualität: Die Auftragsverarbeiter und Unterauftragsverarbeiter sind generell verpflichtet, den für die Verarbeitung Verantwortlichen bei der Einhaltung der Rechtsvorschriften zu unterstützen; insbesondere - ergreifen die Auftragsverarbeiter und Unterauftragsverarbeiter alle erforderlichen Maßnahmen, wenn sie hierzu von dem für die Verarbeitung Verantwortlichen aufgefordert werden, um die Daten zu aktualisieren, zu berichtigen oder zu löschen. Die Auftragsverarbeiter und Unterauftragsverarbeiter unterrichten jedes Mitglied, dem die Daten übermittelt wurden, über jede Berichtigung oder Löschung von Daten; - ergreifen die Auftragsverarbeiter und Unterauftragsverarbeiter alle erforderlichen Maßnahmen, wenn sie hierzu von dem für die Verarbeitung Verantwortlichen aufgefordert werden, um die Daten zu löschen oder zu anonymisieren, sobald das Identifizierungsformular nicht mehr erforderlich ist. Die Auftragsverarbeiter und Unterauftragsverarbeiter unterrichten jedes Unternehmen, dem Daten übermittelt wurden, über jede Löschung oder Anonymisierung von Daten. iv) Sicherheit: Die Auftragsverarbeiter und Unterauftragsverarbeiter müssen Sicherheits- und organisatorische Maßnahmen einhalten, die mindestens den Anforderungen entsprechen, die in den Rechtsvorschriften festgelegt sind, die für den für die Verarbeitung Verantwortlichen gelten, sowie etwaige besondere Maßnahmen wie in der Dienstevereinbarung festgelegt.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Die Auftragsverarbeiter und Unterauftragsverarbeiter unterrichten den für die Verarbeitung Verantwortlichen unverzüglich über jede Sicherheitsverletzung. v) Rechte der betroffenen Personen: Die Auftragsverarbeiter und Unterauftragsverarbeiter ergreifen alle erforderlichen Maßnahmen, wenn sie hierzu von dem für die Verarbeitung Verantwortlichen aufgefordert werden, und teilen ihm alle nützlichen Informationen mit, um ihm bei der Erfüllung der Pflicht zu unterstützen, die Rechte der betroffenen Personen zu wahren. Die Auftragsverarbeiter und Unterauftragsverarbeiter übermitteln dem für die Verarbeitung Verantwortlichen alle Anfragen betroffener Personen, ohne sie zu beantworten, es sei denn sie sind hierzu ermächtigt. vi) Unterverarbeitung in der Unternehmensgruppe: Daten können von anderen Mitgliedern, die an die BCR gebunden sind, nur dann unterverarbeitet werden, wenn der für die Verarbeitung Verantwortliche* zuvor hierüber unterrichtet wurde und seine schriftliche vorherige Einwilligung erteilt hat. In der Dienstevereinbarung ist zu regeln, ob eine generelle vorherige Einwilligung, die zu Beginn der Erbringung des Dienstes erteilt wird, ausreichend ist oder ob eine Einwilligung eigens für jede neue Unterverarbeitung erforderlich ist. Wird eine generelle Einwilligung erteilt, so sollte der für die Verarbeitung Verantwortliche über alle beabsichtigten Änderungen, die das Hinzufügen oder den Ersatz von Unterauftragnehmern betreffen, so rechtzeitig unterrichtet werden, dass es ihm möglich ist, einen Einwand gegen die Änderung vorzubringen oder vom Vertrag zurückzutreten, bevor die Daten an den neuen Unterauftragsverarbeiter weitergeleitet werden. vii) Weiterleitung an externe Unterauftragsverarbeiter: Die Unterverarbeitung von Daten durch Mitglieder, die nicht an die BCR gebunden sind, ist nur dann möglich, wenn der für die Verarbeitung Verantwortliche* zuvor hierüber unterrichtet wird und seine schriftliche vorherige Einwilligung erteilt. Wird eine generelle Einwilligung erteilt, so sollte der für die Verarbeitung Verantwortliche über alle beabsichtigten Änderungen, die das Hinzufügen oder den Ersatz von Unterauftragnehmern betreffen, so rechtzeitig unterrichtet werden, dass es ihm möglich ist, einen Einwand gegen die Änderung vorzubringen oder vom Vertrag zurückzutreten, bevor die Daten an den neuen Unterauftragsverarbeiter weitergeleitet werden.

* Angaben zu den Hauptbestandteilen (Beteiligte, Länder, Sicherheit, Garantien im Falle der Datenübermittlung ins Ausland sowie die Möglichkeit, eine Kopie des angewandten Vertrags zu erhalten). Ausführliche Angaben, z. B. die Namen der Unterauftragsverarbeiter, könnten z. B. in einem öffentlichen digitalen Verzeichnis verfügbar gemacht werden.

Kriterien für die Genehmigung der BCR	In den BCR	Im Antrag	BCR für Auftragsverarbeiter
			Vergibt das Mitglied, das an die BCR gebunden ist, mit Einwilligung des für die Verarbeitung Verantwortlichen Unteraufträge, die den Pflichten der Dienstevereinbarung unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die vorsieht, dass ein ausreichender Schutz im Einklang mit den Artikeln 16, 17, 25 und 26 der Richtlinie 95/46/EG gewährleistet ist, und die dem externen Unterauftragsverarbeiter die gleichen Pflichten auferlegt, die auch das Mitglied, das an die BCR gebunden ist, nach der Dienstevereinbarung und den Abschnitten 1.3, 1.4, 3 und 6 dieses Arbeitsdokuments erfüllen muss.
6.2 Liste der Unternehmen, die an die BCR gebunden sind	JA	JA	Die BCR müssen eine Liste der Unternehmen enthalten, die an sie gebunden sind.
6.3 Transparenzgebot in Fällen, in denen das einzelstaatliche Recht der Einhaltung der BCR durch die Unternehmensgruppe entgegensteht	JA	NEIN	Informationspflichten: Hat ein Mitglied, das an die BCR gebunden ist, Grund zu der Annahme hat, dass die geltenden oder künftigen Rechtsvorschriften es gegebenenfalls daran hindern (werden), die Anweisungen zu befolgen, die es von dem für die Verarbeitung Verantwortlichen erhalten hat, oder seine Pflichten nach den BCR oder der Dienstevereinbarung zu erfüllen, muss es unverzüglich den für die Verarbeitung Verantwortlichen hierüber unterrichten, der berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten, sowie die Hauptniederlassung des Auftragsverarbeiters in der EU oder das Mitglied, das in der EU die Haftung für den Datenschutz übernommen hat, oder den zuständigen Datenschutzbeauftragten, aber auch die Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist. Über alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten ist der für die Verarbeitung Verantwortliche zu informieren, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen. Der Aufforderung zur Weitergabe ist keinesfalls nachzukommen, ohne die Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist, sowie die Datenschutzbehörde, die für die BCR federführend ist, hierüber zu unterrichten.
6.4 Erklärung zum Verhältnis zwischen nationalen Rechtsvorschriften und BCR	JA	NEIN	In den BCR sind auch Angaben zu dem Verhältnis zwischen den BCR und dem einschlägigen anwendbaren Recht zu machen. In den BCR ist festzulegen, dass in Fällen, in denen das geltende Recht – z. B. EU-Recht – ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den BCR vorgeht. Die Datenverarbeitung erfolgt in jedem Fall nach Maßgabe des anwendbaren Rechts.

II. IN DER DIENSTGÜTEVEREINBARUNG ZU REGELNDE PFLICHTEN

Die BCR für Auftragsverarbeiter sind zweifelsfrei mit der Dienstgütevereinbarung zu verknüpfen, die jeder Kunde unterzeichnet. Daher ist es wichtig, dafür zu sorgen, dass in der Dienstgütevereinbarung Folgendes geregelt bzw. enthalten ist:

– Verbindlichmachung der BCR durch Verweis auf sie in der Dienstgütevereinbarung (in der Anlage);

– bei Übermittlung besonderer Kategorien personenbezogener Daten Verpflichtung des für die Verarbeitung Verantwortlichen, die betroffene Person davon in Kenntnis zu setzen, dass ihre Daten in ein Drittland ohne ausreichenden Datenschutz übermittelt wurden, bzw. sie vor der Übermittlung davon in Kenntnis zu setzen, dass ihre Daten gegebenenfalls in ein Drittland ohne ausreichenden Datenschutz übermittelt werden;

– des Weiteren Verpflichtung des für die Verarbeitung Verantwortlichen, die betroffene Person über Auftragsverarbeiter außerhalb der EU und über die BCR in Kenntnis zu setzen. Der für die Verarbeitung Verantwortliche muss den betroffenen Personen auf Verlangen eine Kopie der BCR und der Dienstevereinbarung (ohne Offenlegung sensibler und vertraulicher Geschäftsinformationen) verfügbar machen;

– unmissverständliche Angaben zu Vertraulichkeits- und Sicherheitsmaßnahmen oder Verweis hierauf mittels elektronischem Link;

– unmissverständliche Angaben zu den Anweisungen und der Datenverarbeitung;

– genaue Angaben in der Dienstevereinbarung dazu, ob die Unterverarbeitung von Daten innerhalb oder außerhalb der Unternehmensgruppe erfolgen darf und ob hierfür die vorherige, generelle Einwilligung oder die vorherige, fallweise Einwilligung des für die Verarbeitung Verantwortlichen erforderlich ist.

Brüssel, den 6. Juni 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten (WP 202)

Angenommen am 27. Februar 2013

Zusammenfassung

Für alle gebräuchlichen intelligenten Endgeräte sind Hunderttausende verschiedener Apps von zahlreichen App-Stores erhältlich. Berichten zufolge werden täglich mehr als 1600 neue Apps in App-Stores angeboten. Ein durchschnittlicher Smartphone-Nutzer lädt 37 Apps auf sein Gerät herunter. Apps können dem Endnutzer entweder für geringe Anfangskosten oder auch kostenlos zur Verfügung gestellt werden. Die Nutzerbasis kann sich auf wenige Personen beschränken, aber auch vielen Millionen Nutzer umfassen.

Auf dem jeweiligen Endgerät können Apps Daten (beispielsweise vom Nutzer auf dem jeweiligen Gerät gespeicherte Daten oder Sensordaten wie z. B. Standortdaten) in großem Umfang erfassen und verarbeiten, um dem Endnutzer neue und innovative Dienstleistungen anbieten zu können. Die Daten können jedoch – gewöhnlich zur Erzielung von Einnahmen – in einer Weise weiterverarbeitet werden, die dem Endnutzer nicht bewusst ist und vom Endnutzer auch nicht gewünscht wird.

App-Entwickler, die mit den Datenschutzbestimmungen nicht vertraut sind, können erhebliche Risiken für die Privatsphäre und den Ruf von Nutzern intelligenter Endgeräte verursachen. Die wichtigsten Datenschutzrisiken für Endnutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App ausgeführten Verarbeitungen sowie das Fehlen einer expliziten Einwilligung des Endnutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein offenkundiger Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, erhöhen die Datenschutzrisiken bei Apps unter den gegenwärtigen Umständen zusätzlich.

Ein hohes Risiko für den Datenschutz besteht auch infolge des Umfangs der Fragmentierung unter den zahlreichen Akteuren im Umfeld der Entwicklung von Apps. Zu diesen Akteuren gehören Entwickler und Eigentümer von Apps, App-Stores, Hersteller von Betriebssystemen und Endgeräten sowie andere Dritte, die an der Erfassung und Verarbeitung personenbezogener Daten von intelligenten Endgeräten beteiligt sein können (z. B. Anbieter von Analyse- und Werbedienstleistungen). Die meisten Schlussfolgerungen und Empfehlungen in dieser Stellungnahme sind an App-Entwickler gerichtet (da diese am stärksten auf die genaue Art und Weise Einfluss nehmen können, in der die Verarbeitung erfolgt oder in der Informationen über die App vermittelt werden). Um die höchsten Standards

für den Datenschutz und den Schutz der Privatsphäre zu erreichen, müssen die App-Entwickler jedoch häufig mit anderen Parteien im App-Ökosystem zusammenarbeiten. Dies ist insbesondere in Bezug auf die Sicherheit wichtig, da die aus zahlreichen Akteuren bestehende Kette in diesem Bereich immer nur so stark ist wie das schwächste Glied.

Zahlreiche auf einem intelligenten mobilen Endgerät verfügbare Daten sind personenbezogene Daten. Der geltende Rechtsrahmen in diesem Bereich ergibt sich aus der Datenschutzrichtlinie sowie aus den in der Datenschutzrichtlinie für elektronische Kommunikation enthaltenen Vorschriften zum Schutz mobiler Endgeräte als Teil der Privatsphäre der Nutzer. Diese Vorschriften gelten unabhängig vom Standort des App-Entwicklers oder vom App-Store für jede App, die an App-Nutzer in der EU vertrieben wird.

Die vorliegende Stellungnahme der Datenschutzgruppe verdeutlicht den Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Entwicklung, Verbreitung und Nutzung von Apps auf intelligenten Endgeräten. Dabei liegt der Schwerpunkt auf der Einwilligungsanforderung, den Grundsätzen der Zweckbindung und der Datenminimierung, der Notwendigkeit angemessener Sicherheitsmaßnahmen, der Verpflichtung zu einer korrekten Aufklärung der Endnutzer, den Rechten der Endnutzer, angemessenen Speicherfristen und insbesondere der Verarbeitung der von Kindern und über Kinder erfassten Daten nach Treu und Glauben.

Inhaltsverzeichnis

1. Einleitung

Apps sind Softwareanwendungen, die häufig für eine bestimmte Aufgabe entwickelt werden und für eine bestimmte Gruppe intelligenter Endgeräte wie Smartphones, Tablet-Computer und Fernsehgeräte mit Internetanschluss bestimmt sind. Sie organisieren Informationen in für die spezifischen Eigenschaften des jeweiligen Endgeräts geeigneter Form und interagieren häufig eng mit der Hardware und den Funktionen des auf den Geräten installierten Betriebssystems.

Für jede verbreitete Art von intelligenten Endgeräten sind in zahlreichen App-Stores Hunderttausende von Apps erhältlich. Apps werden für ein breites Spektrum von Zwecken eingesetzt: Internetzugriff, Kommunikation (E-Mail, Telefonie und webbasierte Nachrichten), Unterhaltung (Spiele, Filme/Videos und Musik), soziale Netzwerke, Online-Banking, standortbezogene Dienste usw. Berichten

zufolge werden täglich mehr als 1600 neue Apps in App-Stores angeboten.[1] Der durchschnittliche Smartphone-Nutzer lädt 37 Apps auf sein Gerät herunter.[2] Apps können dem Endnutzer entweder für geringe Anfangskosten oder auch kostenlos zur Verfügung gestellt werden. Die Nutzerbasis kann sich auf wenige Personen beschränken, aber auch vielen Millionen Nutzer umfassen.

Das zugrunde liegende Betriebssystem umfasst auch Software- oder Datenstrukturen, die für die Kerndienste des intelligenten Endgeräts wichtig sind (z. B. das Adressbuch eines Smartphones). Das Betriebssystem ist darauf ausgelegt, diese Komponenten über Programmierschnittstellen (APIs) für Apps nutzbar zu machen. Diese Programmierschnittstellen bieten Zugriff auf die zahlreichen Sensoren, die in intelligenten Endgeräten vorhanden sein können. Solche Sensoren sind beispielsweise ein Gyroskop, ein digitaler Kompass und ein Beschleunigungssensor zur Ermittlung der Geschwindigkeit und der Richtung von Bewegungen, Kameras an Vorder- und Rückseite zur Aufnahme von Videos oder Fotos und ein Mikrofon für Audioaufnahmen. Intelligente Endgeräte können auch mit Näherungssensoren ausgestattet sein[3] und über zahlreiche Netzschnittstellen verfügen (z. B. Wi-Fi, Bluetooth, NFC oder Ethernet). Schließlich kann durch Geolokalisierungsdienste der Standort eines Geräts präzise bestimmt werden (siehe Beschreibung in WP29, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten intelligenter mobiler Endgeräte[4]). Art, Genauigkeit und Messhäufigkeit dieser Sensordaten sind je nach Gerät und Betriebssystem unterschiedlich.

Über die Programmierschnittstellen können App-Entwickler solche Daten fortlaufend erfassen, auf Kontaktdaten zugreifen oder Kontaktdaten erstellen, E-Mails, SMS oder Nachrichten im Rahmen eines sozialen Netzwerks senden, Inhalte von SD-Karten lesen, ändern oder löschen, Audioaufnahmen erstellen, die Kamera nutzen und auf gespeicherte Bilder zugreifen, den Telefonstatus und die Gerätekennungen lesen, die globalen Systemeinstellungen ändern und den Standby-Modus deaktivieren. Außerdem können Programmierschnittstellen Informationen über das Gerät selbst in Form einer oder mehrerer eindeutiger Kennungen sowie Informationen über andere installierte Apps bereitstellen. Die Daten können jedoch – gewöhnlich zur Erzielung von Einnahmen – in einer Weise weiterverarbeitet werden, die dem Endnutzer nicht bewusst ist und vom Endnutzer auch nicht gewünscht wird.

[1] Bericht in ConceivablyTech vom 19. August 2012, abrufbar unter www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of; zitiert von Kamala D. Harris, Attorney General California Department of Justice, *Privacy on the go, Recommendations for the mobile ecosystem*, Januar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[2] Dies ist ein weltweiter Schätzwert von ABI Research für 2012, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o.

[3] Ein Sensor, der das Vorhandensein eines physischen Objekts berührungsfrei ermitteln kann; siehe http://www.w3.org/TR/2012/WD-proximity-20121206/.

[4] Siehe Stellungnahme 13/2011 der Artikel-29-Datenschutzgruppe zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (Mai 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf.

Mit dieser Stellungnahme soll der Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Verbreitung und Nutzung von Apps auf intelligenten Endgeräten beschrieben werden. Außerdem sollen weitere Verarbeitungen betrachtet werden, die möglicherweise außerhalb der App erfolgen (z. B. die Nutzung der erfassten Daten zur Erstellung von Profilen und Nutzer-Zielgruppen). In der Stellungnahme werden die wichtigsten Datenschutzrisiken analysiert, die unterschiedlichen beteiligten Parteien beschrieben und die jeweiligen gesetzlichen Pflichten dieser Akteure erläutert. Zu diesen Akteuren gehören App-Entwickler, App-Eigentümer, App-Stores, Hersteller von Geräten und Betriebssystemen und sonstige Dritte, die an der Erfassung und Verarbeitung personenbezogener Daten von intelligenten Endgeräten beteiligt sein können (z. B. Anbieter von Analyse- und Werbedienstleistungen).

Schwerpunkte der Stellungnahme sind die Einwilligungsanforderung, die Grundsätze der Zweckbindung und der Datenminimierung, die Notwendigkeit angemessener Sicherheitsmaßnahmen, die Verpflichtung zur korrekten Aufklärung der Endnutzer, die Rechte der Endnutzer und angemessene Speicherfristen sowie insbesondere die Verarbeitung erfasster Daten von Kindern und über Kinder nach Treu und Glauben.

Der Gegenstandsbereich der Stellungnahme umfasst zahlreiche Arten intelligenter Endgeräte, konzentriert sich jedoch besonders auf Apps, die für intelligente mobile Endgeräte verfügbar sind.

2. Datenschutzrisiken

Durch die enge Verzahnung mit dem Betriebssystem können Apps auf wesentlich mehr Daten zugreifen als ein herkömmlicher Internet-Browser.[5] Apps können auf dem jeweiligen Endgerät große Datenmengen (Standortdaten, vom Nutzer auf dem Gerät gespeicherte Daten sowie verschiedene Sensordaten) erfassen und verarbeiten, um dem Endnutzer neue und innovative Dienstleistungen anbieten zu können.

Ein hohes Risiko für den Datenschutz ergibt sich aus der ausgeprägten Fragmentierung unter den zahlreichen Akteuren im Umfeld der App-Entwicklung. Ein einzelnes Datenelement kann in Echtzeit vom Gerät übermittelt werden, um dann in einem anderen Teil der Welt verarbeitet oder zwischen Ketten dritter Akteure kopiert zu werden. Einige der bekanntesten Apps werden von großen Technologieunternehmen entwickelt. Viele Apps werden aber auch von kleinen, neu gegründeten Unternehmen hergestellt. Ein einziger Programmierer, der zwar eine Idee hat, aber vielleicht nur geringe oder keinerlei einschlägige Vorkenntnisse besitzt, kann in kurzer Zeit ein weltweites Publikum erreichen. App-Entwickler,

[5] Web-Browser für Desktop-Geräte erhalten aufgrund entsprechender Bestrebungen der Entwickler von Internetspielen ebenfalls einen immer umfangreicheren Zugriff auf Sensordaten.

die nicht mit den Datenschutzbestimmungen vertraut sind, können erhebliche Risiken für die Privatsphäre und den Ruf von Nutzern intelligenter Endgeräte verursachen. Gleichzeitig entwickeln sich rasch Drittanbieter-Dienste (z. B. Werbung), die erhebliche Mengen personenbezogener Daten weitergeben können, wenn sie von einem App-Entwickler ohne angemessene Vorsichtsmaßnahmen integriert werden.

Die größten Datenschutzrisiken für den Endnutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App ausgeführten Verarbeitungen sowie das Fehlen einer expliziten Einwilligung des Endnutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein offenkundiger Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, tragen zu einer weiteren Erhöhung der Datenschutzrisiken des derzeitigen App-Umfelds bei. Viele dieser Risiken wurden von anderen internationalen Regulierungsbehörden untersucht und in Angriff genommen, beispielsweise von der amerikanischen Wettbewerbsbehörde Federal Trade Commission (FTC), dem kanadischen Office of the Privacy Commissioner und dem Attorney General des kalifornischen Justizministeriums.[6]

- Ein wichtiges Datenschutzrisiko ist mangelnde Transparenz. Aufgrund der von den Herstellern der Betriebssysteme und von den App-Stores bereitgestellten Funktionen müssen App-Entwickler dafür sorgen, dass den Endnutzern zum angemessenen Zeitpunkt umfassende Informationen bereitgestellt werden. Diese Funktionen werden jedoch nicht von allen App-Entwicklern genutzt, da viele Apps keine Datenschutzerklärung enthalten oder die Nutzer nicht klar über die Art der personenbezogenen Daten, die die App möglicherweise verarbeitet, und über die Zwecke dieser Verarbeitung informieren. Die mangelnde Transparenz beschränkt sich nicht auf kostenlose Apps oder auf Apps von unerfahrenen Entwicklern. In einer kürzlich veröffentlichten Studie wurde berichtet, dass nur 61,3 % der 150 beliebtesten Apps eine Datenschutzerklärung enthielten.[7]
- Die mangelnde Transparenz geht häufig mit dem Fehlen einer Einwilligung ohne Zwang und in Kenntnis der Sachlage einher. Sobald eine App heruntergeladen wurde, beschränkt sich die Einwilligung häufig auf ein Kontrollkästchen zur Erklärung, dass der Endnutzer die vorgegebenen Bedingungen akzeptiert,

[6] Siehe unter anderem FTC-Bericht: Mobile Privacy Disclosures, Building Trust Through Transparency, Februar 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, FTC-Bericht: *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, Februar 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf, und Folgebericht: *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, Dezember 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, sowie *Canadian Offices of the Privacy Commissioners, Seizing Opportunity: Good Privacy. Practices for Developing Mobile Apps*, Oktober 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, Attorney General California Department of Justice, *Privacy on the go, Recommendations for the mobile ecosystem*, Januar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[7] FPF Mobile Apps study, Juni 2012, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

ohne dass auch nur die Auswahlmöglichkeit „Nein, danke“ angeboten wird. Nach einer Studie der GSMA vom September 2011 wünschen sich 92 % der App-Nutzer eine differenziertere Auswahl.[8]

- Unzureichende Sicherheitsmaßnahmen können zur unberechtigten Verarbeitung (sensibler) personenbezogener Daten führen, beispielsweise wenn ein App-Entwickler Opfer eines Diebstahls personenbezogener Daten wird oder wenn die App personenbezogene Daten aktiv überträgt.
- Ein weiteres Datenschutzrisiko ergibt sich aus der (absichtlichen oder durch Unwissenheit bedingten) Missachtung des Grundsatzes der Zweckbindung, nach dem personenbezogene Daten nur für genau festgelegte und rechtmäßige Zwecke erfasst und verarbeitet werden dürfen. Von Apps erfasste personenbezogene Daten können für nicht oder ungenau festgelegte Zwecke wie „Marktforschung“ an zahlreiche Dritte weitergegeben werden. Die gleiche besorgniserregende Missachtung besteht in Bezug auf den Grundsatz der Datenminimierung. Kürzlich durchgeführte Forschungsarbeiten haben ergeben, dass viele Apps große Datenmengen von Smartphones erfassen, ohne dass ein sinnvoller Bezug zur offensichtlichen Funktion der App besteht.[9]

3. Datenschutzgrundsätze

3.1 Anwendbares Recht

Der maßgebliche EU-Rechtsrahmen besteht in der Datenschutzrichtlinie (Richtlinie 95/46/EG). Die Datenschutzrichtlinie gilt immer dann, wenn die Nutzung von Apps auf intelligenten Endgeräten mit einer Verarbeitung personenbezogener Daten von natürlichen Personen einhergeht. Im Zusammenhang mit der Verarbeitung über mobile Apps ist für die Ermittlung des anwendbaren Rechts besonders wichtig, dass der für die Verarbeitung Verantwortliche bestimmt wird. Die Feststellung des für die Verarbeitung Verantwortlichen ist für die Anwendung des EU-Datenschutzrechts zwar nicht der einzige, aber doch ein entscheidender Schritt. Gemäß Artikel 4 Absatz 1 Buchstabe a der Datenschutzrichtlinie gilt das nationale Recht eines Mitgliedstaats für alle Verarbeitungen personenbezogener Daten, die „im Rahmen einer Niederlassung“ des für die Verarbeitung Verantwortlichen im Hoheitsgebiet dieses Mitgliedstaats durchgeführt werden. Gemäß Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie gilt das nationale Recht eines Mitgliedstaats auch in Fällen, in denen der für die Verarbeitung Verantwortliche *nicht* im Gebiet der Gemeinschaft *niedergelassen* ist und auf Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind.

[8] *„89 % [der Nutzer] finden es wichtig, zu wissen, wenn ihre personenbezogenen Informationen von einer App weitergegeben werden, und wie sie die entsprechende Funktion aktivieren und deaktivieren zu können.“* Quelle: *User perspectives on mobile privacy*, September 2011, http://www.gsma.com/publicpolicy/wp- content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

[9] Wall Street Journal, *Your Apps Are Watching You*, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

Dieses Kriterium ist normalerweise erfüllt, da das Endgerät an der Verarbeitung personenbezogener Daten vom Nutzer und über den Nutzer maßgeblich beteiligt ist.[10] Dies ist jedoch nur relevant, wenn der für die Verarbeitung Verantwortliche nicht in der EU niedergelassen ist.

Entsprechend gilt: Wenn eine an der Entwicklung, der Verbreitung und dem Betrieb von Apps beteiligte Partei als für die Verarbeitung Verantwortlicher angesehen wird, ist sie – allein oder gemeinsam mit anderen – dafür verantwortlich, die Einhaltung sämtlicher in der Datenschutzrichtlinie festgelegten Anforderungen zu gewährleisten. Die Ermittlung der Rollen der an mobilen Apps beteiligten Parteien wird in Abschnitt 3.3 eingehender behandelt.

Ergänzend zur Datenschutzrichtlinie legt die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG, geändert durch Richtlinie 2009/136/EG) weltweit einen spezifischen Standard für alle Parteien fest, die auf den Endgeräten von Nutzern im Europäischen Wirtschaftsraum (EWR) gespeicherte Informationen ihrerseits speichern oder auf diese Informationen zugreifen wollen.

Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation sieht vor, dass „*die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. (…)*“

Während viele Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation nur auf Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste und auf Betreiber öffentlicher Kommunikationsnetze in der Gemeinschaft anwendbar sind, gilt Artikel 5 Absatz 3 für jede Rechtsperson, die Informationen auf intelligente Endgeräte überträgt oder auf diesen Geräten liest. Er gilt unabhängig von der Art der Rechtsperson (öffentliche oder private Rechtsperson, einzelner Programmierer oder Großunternehmen, für die Verarbeitung Verantwortlicher, Auftragsverarbeiter oder Dritter).

Die Einwilligungsanforderung nach Artikel 5 Absatz 3 gilt unabhängig von der Art der zu speichernden oder zu lesenden Daten für sämtliche Informationen. Der Anwendungsbereich ist nicht auf personenbezogene Daten beschränkt. Die Informationen können jegliche Art von auf dem Gerät gespeicherten Daten sein.

[10] Sofern die App die Übertragung personenbezogener Daten an die für die Verarbeitung Verantwortlichen bewirkt; dieses Kriterium ist möglicherweise nicht erfüllt, wenn die Daten ausschließlich lokal auf dem eigentlichen Endgerät verarbeitet werden.

Die Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation gilt für Dienste, die „*in der Gemeinschaft*" angeboten werden, d. h. unabhängig vom Standort des Dienstebetreibers für alle im Europäischen Wirtschaftsraum lebenden Personen. Es ist wichtig, dass App-Entwickler wissen, dass die beiden Richtlinien insofern zwingende Vorschriften darstellen, als die Rechte natürlicher Personen nicht übertragbar sind und keinem vertraglichen Verzicht unterliegen. Das bedeutet, dass die Anwendbarkeit des europäischen Rechts zum Schutz der Privatsphäre nicht durch eine einseitige Erklärung oder eine vertragliche Vereinbarung ausgeschlossen werden kann.[11]

3.2 Von Apps verarbeitete personenbezogene Daten

Viele Arten von Daten, die auf einem intelligenten mobilen Endgerät gespeichert sind oder von diesem Gerät erstellt werden, sind personenbezogene Daten. Erwägungsgrund 24 der Datenschutzrichtlinie für elektronische Kommunikation besagt:

> *„Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt."*

Informationen sind als personenbezogene Daten zu betrachten, wenn sie sich auf eine natürliche Person beziehen, die für den für die Verarbeitung Verantwortlichen oder einen Dritten direkt (z. B. durch den Namen) oder indirekt identifizierbar ist. Sie können sich auf den Besitzer des Geräts oder auf beliebige andere natürliche Personen beziehen (z. B. die Kontaktdaten von Freunden in einem Adressbuch).[12] Daten können auf dem Gerät oder – nach der Übertragung – an anderen Orten erfasst und verarbeitet werden: auf der Infrastruktur von App-Entwicklern oder Dritten, über die Verbindung mit einer externen Programmierschnittstelle, in Echtzeit und ohne Kenntnis des Endnutzers.

Beispiele für solche personenbezogenen Daten, die erhebliche Auswirkungen auf die Privatleben der Nutzer und anderer Personen haben können:

- Standortinformationen,
- Kontakte,

[11] Zum Beispiel durch Erklärungen, dass ausschließlich das Recht eines außerhalb des EWR liegenden Rechtssystems gilt.

[12] Daten können (i) vom Gerät automatisch auf aufgrund von Funktionen erstellt werden, die vom Betriebssystem und/oder dem Gerätehersteller oder vom jeweiligen Mobilfunkbetreiber im Voraus festgelegt werden (z. B. Geolokalisierungsdaten, Netzeinstellungen, IP-Adresse), (ii) vom Nutzer durch Apps erstellt werden (Kontaktlisten; Notizen, Fotos) und (iii) von den Apps erstellt werden (z. B. Browserverlauf).

- eindeutige Geräte- und Kundenkennungen (z. B. IMEI,[13] IMSI,[14] UDID[15] und Mobiltelefonnummer),
- Identität der betroffenen Person,
- Identität des Telefons (d. h. Name des Telefons),[16]
- Kreditkarten- und Zahlungsdaten,
- Anruflisten, SMS oder Instant Messaging,
- Browserverlauf,
- E-Mail,
- Authentifizierungsdaten für Dienste der Informationsgesellschaft (insbesondere Dienste mit sozialen Funktionen),
- Bilder und Videos und
- biometrische Daten (z. B. Muster für Gesichtserkennung und Fingerabdrücke).

3.3 An der Datenverarbeitung beteiligte Parteien

Viele verschiedene Parteien sind an der Entwicklung, der Verbreitung und dem Betrieb von Apps beteiligt, und jede dieser Parteien kann hinsichtlich des Datenschutzes unterschiedliche Pflichten haben.

Vier wichtige Parteien sind zu unterscheiden: (i) App-Entwickler (einschließlich der App-Eigentümer),[17] Hersteller von Betriebssystemen und Endgeräten,[18] (iii) App-Stores (Vertreiber der Apps) und (iv) sonstige an der Verarbeitung personenbezogener Dateien beteiligte Parteien. In einigen Fällen sind die Datenschutzpflichten verteilt, insbesondere, wenn ein und dieselbe Rechtsperson auf mehreren Ebenen beteiligt ist, zum Beispiel wenn der Hersteller des Betriebssystems auch den App-Store kontrolliert.

Die Endnutzer müssen in angemessener Weise eigenverantwortlich entscheiden, in welchem Umfang sie personenbezogene Daten über ihre mobilen Endgeräte

[13] *International Mobile Equipment Identity* (eindeutige Nummer des Endgeräts).

[14] *International Mobile Subscriber Identity* (eindeutige Nummer des Netzteilnehmers).

[15] *Unique Device Identifier* (eindeutige Gerätenummer für Apple-Produkte).

[16] Nutzer neigen dazu, ihr Telefon unter Verwendung ihres eigenen Namens zu benennen, z. B. „Max Mustermanns iPhone".

[17] Die Datenschutzgruppe verwendet die allgemeine Terminologie von App-Entwicklern, betont jedoch, dass der Begriff nicht auf die Programmierer oder die technischen Entwickler von Apps beschränkt ist, sondern die App-Eigentümer einschließt. Diese sind Unternehmen und Organisationen, die die Entwicklung von Apps in Auftrag geben und die Zwecke der Apps festlegen.

[18] In einigen Fällen bestehen Überschneidungen zwischen dem Hersteller des Betriebssystems und dem Hersteller des Endgeräts. In anderen Fällen ist der Hersteller des Geräts nicht gleichzeitig auch der Anbieter des Betriebssystems.

erstellen und speichern. Wenn eine solche Verarbeitung rein persönlichen oder familiären Zwecken dient, gilt die Datenschutzrichtlinie nicht (Artikel 3 Absatz 2), und der Nutzer ist von formalen Datenschutzverpflichtungen ausgenommen. Wenn Nutzer jedoch beschließen, Daten über die App weiterzugeben, indem sie beispielsweise über eine App für soziale Netzwerke Informationen für eine unbestimmte Zahl von Personen veröffentlichen,[19] geht die betreffende Verarbeitung von Informationen über die Bedingungen der Ausnahme für familiäre Tätigkeiten hinaus.[20]

3.3.1 App-Entwickler

App-Entwickler erstellen Apps und/oder stellen Endnutzern Apps zur Verfügung. Diese Kategorie beinhaltet Organisationen des privaten und des öffentlichen Sektors, die die App-Entwicklung extern vergeben, sowie die Unternehmen und die natürlichen Personen, die Apps erstellen und implementieren. Sie konzipieren und/oder erstellen die Software, die auf den Smartphones läuft, und entscheiden so über den Umfang, in dem die App auf die verschiedenen Kategorien personenbezogener Daten zugreift und diese auf dem Gerät und/oder über entfernte Rechenressourcen (Rechnereinheiten von App-Entwicklern oder Dritten) verarbeitet.

In dem Umfang, in dem ein App-Entwickler die Zwecke und die Mittel der Verarbeitung personenbezogener Daten auf intelligenten Endgeräten festlegt, ist er der für die Verarbeitung Verantwortliche gemäß der Definition in Artikel 2 Buchstabe d der Datenschutzrichtlinie. In diesem Fall muss er die Bestimmungen der gesamten Datenschutzrichtlinie einhalten. Die wichtigsten Bestimmungen sind in den Abschnitten 3.4 bis 3.10 der vorliegenden Stellungnahme erläutert.

Selbst wenn die Ausnahmebestimmung für familiäre Tätigkeiten für einen Nutzer gilt, kommt dem App-Entwickler die Rolle des für die Verarbeitung Verantwortlichen zu, wenn er die Daten für seine eigenen Zwecke verarbeitet. Dies ist beispielsweise dann relevant, wenn eine App Zugriff auf das gesamte Adressbuch erfordert, um den jeweiligen Dienst (Instant Messaging, Telefonanrufe, Videoanrufe) zu erbringen.

Die Verpflichtungen des App-Entwicklers werden als eingeschränkt angesehen, wenn keine personenbezogenen Daten außerhalb des Geräts verarbeitet und/oder verfügbar gemacht werden oder wenn der App-Entwickler mit angemessenen technischen und organisatorischen Maßnahmen sichergestellt hat, dass Daten auf

[19] Siehe Europäischer Gerichtshof, Rechtssache C-101/01, Strafverfahren gegen Bodil Lindqvist, Urteil vom 6. November 2003, und Rechtssache C-73/07, Tietosuojavaltuutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy, Urteil vom 16. Dezember 2008.

[20] Siehe Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe zur Nutzung sozialer Online-Netzwerke (Juni 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

dem Gerät irreversibel anonymisiert und aggregiert werden, bevor sie vom Gerät übertragen werden.

Wenn der App-Entwickler Zugriff auf Informationen erhält, die auf dem Gerät gespeichert sind, gilt in jedem Fall auch die Datenschutzrichtlinie für elektronische Kommunikation, und der App-Entwickler muss die in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehene Einwilligungsanforderung erfüllen.

In dem Umfang, in dem der App-Entwickler die tatsächliche Datenverarbeitung teilweise oder vollständig extern an einen Dritten vergeben hat und diesem Dritten die Rolle eines für die Verarbeitung Verantwortlichen zukommt, muss der App-Entwickler alle Verpflichtungen erfüllen, die sich aus dem Einsatz eines Auftragsverarbeiters ergeben. Dies gilt auch für die Nutzung eines Cloud-Computing-Anbieters (z. B. zur externen Datenspeicherung).[21]

In dem Umfang, in dem der App-Entwickler Dritten Zugriff auf Nutzerdaten gestattet (z. B. durch Online-Werbenetzwerke („Advertising Networks"), die auf die Standortdaten des Endgeräts zugreifen, um auf der Basis von Behavioural Targeting Werbung betreiben zu können), muss er angemessene Mechanismen einsetzen, um die Anforderungen des EU-Rechtsrahmens zu erfüllen. Wenn ein Dritter auf Daten zugreift, die auf dem Endgerät gespeichert sind, muss er die betreffende Einwilligung in Kenntnis der Sachlage gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation einholen. Wenn ein Dritter personenbezogene Daten für seine eigenen Zwecke verarbeitet, kann er darüber hinaus gemeinsam mit dem App-Entwickler als für die Verarbeitung Verantwortlicher betrachtet werden und muss daher die Beachtung des Grundsatzes der Zweckbindung und der Sicherheitsverpflichtungen[22] für den Teil der Verarbeitung gewährleisten, für den er die jeweiligen Zwecke und Mittel festlegt. Da zwischen App-Entwicklern und Dritten verschiedene (wirtschaftliche und technische) Vereinbarungen bestehen können, müssen die Verantwortlichkeiten der jeweiligen Partei im Einzelfall unter Berücksichtigung der spezifischen Umstände der entsprechenden Verarbeitung ermittelt werden.

Ein App-Entwickler kann Programmbibliotheken Dritter mit Software-Komponenten für allgemeine Funktionen nutzen (z. B. die Programmbibliothek einer Social-Gaming-Plattform). In diesem Fall muss der App-Entwickler gegebenenfalls u. a. unter Einholung der Einwilligung der Nutzer sicherstellen, dass den Nutzern

[21] Siehe Stellungnahme 05/2012 der Artikel-29-Datenschutzgruppe zum Cloud Computing (Juli 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.

[22] Siehe Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting (Juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf, sowie Stellungnahme 1/2010 der Artikel-29-Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (Februar 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

jegliche von diesen Programmbibliotheken durchgeführte Datenverarbeitung bekannt ist sowie dass die betreffende Datenverarbeitung dem EU-Rechtsrahmen entspricht. In diesem Sinne müssen App-Entwickler die Nutzung von Funktionen verhindern, die für den Nutzer nicht offensichtlich sind.

3.3.2 Hersteller von Betriebssystemen und Endgeräten

Die Hersteller von Betriebssystemen und Endgeräten sind für sämtliche personenbezogenen Daten, die für ihre eigenen Zwecke verarbeitet werden (z. B. für ein reibungsloses Funktionieren des Geräts oder für die Sicherheit), ebenfalls als für die Verarbeitung Verantwortliche (sowie gegebenenfalls als gemeinsam für die Verarbeitung Verantwortliche) zu betrachten. Diese Verarbeitung umfasst vom Nutzer erstellte Daten (z. B. Nutzerangaben bei der Registrierung), vom Gerät automatisch erstellte Daten (z. B. wenn das Gerät eine Phone-Home-Funktion in Bezug auf seinen Standort hat) oder personenbezogene Daten, die im Rahmen der Installation oder der Nutzung von Apps erstellt wurden und vom Hersteller des Betriebssystems oder des Geräts verarbeitet werden. Wenn der Hersteller des Betriebssystems oder des Geräts zusätzliche Funktionen (z. B. zur Datensicherung oder Fernstandortsbestimmung) bereitstellt, ist er auch für die zu diesem Zweck verarbeiteten personenbezogenen Daten der für die Verarbeitung Verantwortliche.

> Apps, die einen Zugriff auf die Geolokalisierung erfordern, müssen die Standortsbestimmungsdienste des Betriebssystems nutzen. Wenn eine App die Geolokalisierung verwendet, kann das Betriebssystem einerseits personenbezogene Daten erfassen, um den Apps die erforderlichen Geolokalisierungsinformationen zur Verfügung zu stellen, und andererseits die Daten zur Verbesserung der eigenen Standortsbestimmungsdienste verwenden. Für den letztgenannten Zweck ist der Hersteller des Betriebssystems der für die Verarbeitung Verantwortliche.

Die Hersteller von Betriebssystemen und Endgeräten sind auch für die Programmierschnittstelle (API) verantwortlich, die die Verarbeitung personenbezogener Daten auf dem intelligenten Endgerät durch Apps ermöglicht. Die App-Entwickler können auf diese Funktionen, die die Hersteller von Betriebssystemen und Endgeräten über die Programmierschnittstelle verfügbar machen, zugreifen. Da die Hersteller von Betriebssystemen und Endgeräten die Mittel (und den Umfang) des Zugriffs auf personenbezogene Daten festlegen, müssen sie gewährleisten, dass App-Entwicklern hinreichend differenzierte Kontrollmöglichkeiten gewährt werden, um sicherstellen zu können, dass sich Zugriffe auf die für die Funktion der Apps tatsächlich erforderlichen Daten beschränken. Die Hersteller von Betriebssystemen und Geräten sollten zudem gewährleisten, dass dieser Zugriff einfach und wirksam unterbunden werden kann.

Das Konzept des eingebauten Datenschutzes (Privacy by Design) ist ein wichtiger Grundsatz, der indirekt bereits in der Datenschutzrichtlinie[23] berücksichtigt wird und der – in Verbindung mit dem Konzept datenschutzfreundlicher Voreinstellungen (Privacy by Default) – in der Datenschutzrichtlinie für elektronische Kommunikation[24] eingehender erläutert wird. Dieser Grundsatz verlangt, dass die Hersteller eines Endgeräts oder einer Applikation den Datenschutz schon in der Anfangsphase der Konzeption integrieren müssen. Der eingebaute Datenschutz ist gemäß der Richtlinie über Funkanlagen und Telekommunikationsendeinrichtungen[25] für die Konzeption von Telekommunikationseinrichtungen ausdrücklich vorgeschrieben. Daher kommt den Herstellern von Betriebssystemen und Endgeräten gemeinsam mit den App-Stores wesentliche Verantwortung für die Bereitstellung von Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre von App-Nutzern zu. Im Rahmen dieser Verantwortung ist auch zu gewährleisten, dass angemessene Mechanismen verfügbar sind, um die Endnutzer darüber zu informieren und aufzuklären, welche Funktionen Apps ausführen und auf welche Daten sie zugreifen können. Außerdem sind angemessene Einstellungen bereitzustellen, mit denen App-Nutzer die Verarbeitungsparameter ändern können.[26]

3.3.3 App-Stores

Die am weitesten verbreiteten Arten intelligenter Endgeräte haben jeweils einen eigenen App-Store, und häufig ist ein bestimmtes Betriebssystem eng mit einem bestimmten App-Store verzahnt. App-Stores verarbeiten häufig Vorabzahlungen für Apps und können auch in Apps integrierte Kaufvorgänge unterstützen; daher erfordern sie eine Nutzerregistrierung mit Namen, Anschrift und Angaben für die Zahlung. Diese (direkt) identifizierbaren Daten können mit Daten über das Kauf- und Nutzungsverhalten sowie mit aus dem jeweiligen Gerät ausgelesen oder von diesem Gerät erstellten Daten (z. B. eindeutigen Kennungen) abgeglichen werden. Für die Verarbeitung dieser personenbezogenen Daten ist ein App-Store wahrscheinlich der für die Verarbeitung Verantwortliche; dies gilt auch, wenn er solche Informationen an die App-Entwickler weiterleitet. Wenn der App-Store Informationen über die heruntergeladenen Apps eines Endnutzers, den Nutzungsverlauf oder ähnliche Funktionen verarbeitet, um bereits heruntergeladene Apps

[23] Siehe Erwägungsgrund 46 und Artikel 17.

[24] Siehe Artikel 14 Absatz 3.

[25] Richtlinie 1999/5/EG vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität. Amtsblatt L 91/10 der Europäischen Gemeinschaften, 7.4.1999; nach Artikel 3 Absatz 3 Buchstabe c kann die Europäische Kommission festlegen, dass die Endnutzergeräte so hergestellt sein müssen, dass sie über Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre des Benutzers und des Teilnehmers verfügen.

[26] Die Datenschutzgruppe begrüßt in diesem Zusammenhang die Empfehlungen der FTC in ihrem in Fußnote 6 erwähnten Bericht „Mobile Privacy Disclosures“ (Datenschutzerklärungen bei mobilen Endgeräten), zum Beispiel auf Seite 15: „*(…) Plattformen [sind] in einer einzigartigen Position, einheitliche [Datenschutz-]Erklärungen für Apps bereitstellen zu können, und werden dazu ermutigt. Entsprechend den Workshop-Anmerkungen könnten sie auch in Erwägung ziehen, diese Erklärungen zu verschiedenen Zeitpunkten anzuzeigen (…).*“

wiederherzustellen, ist er auch der für die Verarbeitung Verantwortliche für die zu diesem Zweck verarbeiteten personenbezogenen Daten.

Ein App-Store speichert Anmeldedaten sowie die Verlaufsdaten bereits erworbener Apps. Er fordert den Nutzer auch auf, eine Kreditkartennummer anzugeben, die zusammen mit dem Nutzerkonto gespeichert wird. Der App-Store ist der für die Verarbeitung Verantwortliche für diese Vorgänge.

Websites, die das Herunterladen einer App zur Installation auf dem Endgerät ohne Authentifizierung erlauben, verarbeiten unter Umständen keine personenbezogenen Daten.

App-Stores spielen insofern eine wichtige Rolle, als sie App-Entwicklern ermöglichen können, angemessene Informationen über die App bereitzustellen (u. a. über die Arten von Daten, die die App verarbeiten kann, und über die Zwecke, zu denen die Daten verarbeitet werden). App-Stores können diese Regeln durch ihre Strategie zur Aufnahme der zu vertreibenden Apps (auf Grundlage von Ex-Ante- oder Ex-Post-Kontrollen) durchsetzen. In Zusammenarbeit mit dem Betriebssystemhersteller kann der App-Store einen Rahmen entwickeln, mit dem App-Entwickler konsistente und aussagekräftige Informationsmitteilungen erstellen können (z. B. Symbole für bestimmte Arten des Zugriffs auf Sensordaten); die betreffenden Symbole kann er gut sichtbar in seinem Katalog darstellen.

3.3.4 Dritte

An der Verarbeitung von Daten durch die Nutzung von Apps sind viele verschiedene Dritte beteiligt.

Beispielsweise finanzieren sich viele kostenlose Apps durch Werbung, die unter Verwendung von Protokollierungsvorrichtungen (Tracking-Vorrichtungen) wie Cookies oder andere Geräte-Identifikatoren auf Zusammenhänge oder Personen bezogen werden kann. Die Werbung kann in verschiedenen Formen erfolgen: Banner innerhalb der App, Werbeanzeigen außerhalb der App, die durch die Änderung von Browsereinstellungen eingeblendet werden, Platzierung von Symbolen auf dem Desktop des mobilen Endgeräts oder personalisierte Organisation der App-Inhalte (z. B. gesponserte Suchergebnisse).

Die Werbung für Apps erfolgt im Allgemeinen über Online-Werbenetzwerke oder ähnliche Vermittler, die mit der Rechtsperson des Betriebssystem-Herstellers oder des App-Store verknüpft oder identisch sein können. Wie in der Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe[27] erläutert, bringt Online-Werbung

[27] Siehe Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting (Juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf.

häufig die Verarbeitung personenbezogener Daten mit sich, wie sie in Artikel 2 der Datenschutzrichtlinie definiert und durch die Artikel-29-Arbeitsgruppe ausgelegt wurden.[28]

Weitere Beispiele für Dritte sind Analyse- und Kommunikationsdienstleister. Analysedienstleister ermöglichen den App-Entwicklern, Erkenntnisse über die Nutzung, die Beliebtheit und die Nutzbarkeit ihrer Apps zu gewinnen. Kommunikationsdienstleister[29] können eine wichtige Rolle auch bei der Festlegung der Standardeinstellungen und der Sicherheitsaktualisierungen vieler Endgeräte spielen und Daten über die Nutzung von Apps verarbeiten. Ihre spezifische Anpassung (Markenkennzeichnung) kann Auswirkungen auf mögliche technische und funktionelle Maßnahmen haben, die der Nutzer zum Schutz seiner personenbezogenen Daten anwenden kann.

Im Vergleich zu App-Entwicklern können Dritten zwei verschiedene Rollen zukommen. Eine Rolle besteht in der Durchführung von Vorgängen für den App-Eigentümer (etwa in der Bereitstellung von Analysen innerhalb der App). Wenn die betreffenden Dritten in diesem Fall ausschließlich im Namen des App-Entwicklers handeln und keine Daten zu ihren eigenen Zwecken verarbeiten und/oder Daten an andere Entwickler weiterleiten, handeln sie wahrscheinlich als Auftragsverarbeiter.

Die zweite Rolle besteht im Sammeln von Informationen von verschiedenen Apps, um weitere Dienste anzubieten, z. B. die Bereitstellung von Analysewerten in größerem Maßstab (Beliebtheit von Apps, personalisierte Empfehlung) oder die Vermeidung der wiederholten Einblendung von Werbeanzeigen für den gleichen Nutzer. Wenn Dritte personenbezogene Daten zu ihren eigenen Zwecken verarbeiten, handeln sie als für die Verarbeitung Verantwortliche und müssen sämtliche anwendbaren Bestimmungen der Datenschutzrichtlinie einhalten.[30] Bei Werbung auf Basis von Behavioural Targeting muss der für die Verarbeitung Verantwortliche eine gültige Einwilligung des Nutzers für die Erfassung und die Verarbeitung personenbezogener Daten einholen. Diese Verarbeitung umfasst beispielsweise die Analyse und Kombination personenbezogener Daten und die Erstellung und/oder Anwendung von Profilen. Wie die Datenschutzgruppe bereits in der Stellungnahme 2/2012 zur Werbung auf Basis von Behavioural Targeting erläutert hat, wird eine solche Einwilligung am besten durch die Verwendung eines vorgeschalteten Opt-in-Mechanismus veranlasst.

---

[28] Siehe auch die Auslegung des Begriffs „personenbezogene Daten“ in der Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe (Juni 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf

[29] Kommunikationsdienstleister unterliegen auch branchenspezifischen Datenschutzverpflichtungen, die außerhalb des Gegenstandsbereichs der vorliegenden Stellungnahme liegen.

[30] Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting, S. 10–11.

Ein Unternehmen stellt App-Eigentümern und Werbetreibenden durch die Verwendung von Tracking-Vorrichtungen Parameter zur Verfügung, die der App-Entwickler in die Apps integriert hat. Die Tracking-Vorrichtungen des Unternehmens können daher in zahlreichen Apps und auf zahlreichen Endgeräten installiert werden. Eine der Dienstleistungen des Unternehmens besteht darin, App-Entwickler durch Erfassung einer eindeutigen Kennung darüber zu informieren, welche sonstigen Apps von einem Nutzer verwendet werden. Das Unternehmen legt die Mittel (d. h. die Tracking-Vorrichtungen) und die Zwecke seiner Hilfsmittel fest, bevor das Unternehmen den App-Entwicklern, den Werbetreibenden und anderen Akteuren die betreffenden Mittel bereitstellt, und handelt daher als für die Verarbeitung Verantwortlicher.

In dem Umfang, in dem Dritte auf Informationen auf dem intelligenten Endgerät zugreifen oder Informationen auf dem Gerät speichern, müssen sie die Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erfüllen.

In diesem Zusammenhang ist darauf hinzuweisen, dass Nutzer Software zur Kontrolle der Verarbeitung personenbezogener Daten (wie im Umfeld der Internetnutzung auf Desktop-Geräten allgemein verbreitet) auf intelligenten Endgeräten normalerweise nur in beschränktem Umfang installieren können. Alternativ zur Verwendung von HTTP-Cookies greifen Dritte häufig auf eindeutige Kennungen zu, um Nutzer bzw. Gruppen von Nutzern auszuwählen und diesen gezielte Dienstleistungen, einschließlich Werbung, zu übermitteln. Da viele dieser Kennungen von den Nutzern nicht gelöscht oder geändert werden können (z. B. IMEI, IMSI, MSISDN[31] und spezifische vom Betriebssystem erstellte eindeutige Gerätekennungen), können diese Dritten große Mengen personenbezogener Daten erfassen, ohne dass der Endnutzer eine Kontrolle darüber hat.

3.4 Rechtsgrundlage

Die Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, deren Elemente in Artikel 7 der Datenschutzrichtlinie aufgezählt sind. Artikel 7 unterscheidet sechs Rechtsgrundlagen für die Datenverarbeitung: die ohne jeden Zweifel gegebene Einwilligung der betroffenen Person, die Notwendigkeit der Verarbeitung für die Erfüllung eines Vertrags mit der betroffenen Person, die Wahrung lebenswichtiger Interessen der betroffenen Person, die Notwendigkeit für die Erfüllung einer rechtlichen Verpflichtung, (für Behörden) die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, und die Notwendigkeit aufgrund berechtigter (geschäftlicher) Interessen.

[31] *Mobile Station Integrated Services Digital Network* (weltweit eindeutige Mobilfunk-Rufnummer).

In Bezug auf das Speichern von Informationen oder den Zugriff auf bereits auf dem Endgerät gespeicherte Informationen entsteht durch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation (d. h. die Einwilligungsanforderung für die Speicherung von Informationen und das Auslesen von Informationen aus einem Gerät) eine detailliertere Einschränkung der Rechtsgrundlagen, die berücksichtigt werden kann.

3.4.1 Einwilligung vor Installation und Verarbeitung personenbezogener Daten

Im Fall von Apps ist die wichtigste anwendbare Rechtsgrundlage die Einwilligung. Bei der Installation einer App werden Informationen auf dem Endnutzergerät gespeichert. Viele Apps greifen auch auf Daten zu, die auf dem Gerät gespeichert sind: Kontakte im Adressbuch, Bilder, Videos und andere personenbezogene Dokumente. In allen diesen Fällen setzt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation die Einwilligung des Nutzers auf der Grundlage klarer und umfassender Informationen voraus, bevor Informationen auf dem Gerät gespeichert oder vom Gerät gelesen werden.

Es ist wichtig, zwischen der für das Speichern und Lesen von Informationen auf dem Gerät erforderlichen Einwilligung und der Einwilligung zu unterscheiden, die als Rechtsgrundlage für die Verarbeitung verschiedener Arten personenbezogener Daten erforderlich ist. Beide Anforderungen gelten gleichzeitig (mit jeweils unterschiedlicher Rechtsgrundlage). Außerdem muss die Einwilligung in beiden Fällen ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen (nach Artikel 2 Buchstabe h der Datenschutzrichtlinie). Daher können beide Einwilligungen in der Praxis gemeinsam eingeholt werden, entweder während der Installation oder bevor die App mit der Erfassung personenbezogener Daten vom Gerät beginnt; Voraussetzung ist allerdings, dass der Nutzer unmissverständlich darüber informiert wird, wofür er seine Einwilligung erteilt.

Viele App-Stores ermöglichen den App-Entwicklern, die Endnutzer vor der Installation über die Grundfunktionen einer App zu informieren und eine aktive Eingabe von den Nutzern zu fordern, bevor die App heruntergeladen und installiert wird (z. B. Tippen auf eine Schaltfläche „Installieren“). Obwohl diese Eingabe unter bestimmten Umständen die Einwilligungsanforderung nach Artikel 5 Absatz 3 erfüllen könnte, werden Informationen wahrscheinlich nicht in hinreichendem Umfang bereitgestellt; in diesem Fall wäre eine gültige Einwilligung für die Verarbeitung personenbezogener Daten nicht gegeben. Die Datenschutzgruppe hat diese Thematik bereits in ihrer Stellungnahme 15/2011 zur Definition von Einwilligung[32] erörtert.

[32] Stellungnahme 15/2011 der Artikel-29-Datenschutzgruppe zur Definition von Einwilligung (Juli 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf.

Im Zusammenhang mit intelligenten Endgeräten bedeutet „ohne Zwang", dass einem Nutzer die Möglichkeit eingeräumt werden muss, die Verarbeitung seiner personenbezogenen Daten zu akzeptieren oder abzulehnen. Wenn eine App auf die Verarbeitung personenbezogener Daten angewiesen ist, muss dem Nutzer daher die diese Verarbeitung akzeptieren oder ablehnen können. Der Nutzer sollte nicht mit einem Bildschirm konfrontiert werden, über den die Installation ausschließlich mit der Option „Ja, ich bin einverstanden" abgeschlossen werden kann. Die Installation muss auch etwa über die Option „Abbrechen" abgebrochen werden können.

„In Kenntnis der Sachlage" bedeutet, dass die betroffene Person über die erforderlichen Informationen verfügen muss, um sich ein korrektes Urteil bilden zu können.[33] Zur Vermeidung jeglicher Mehrdeutigkeit müssen solche Informationen bereitgestellt werden, bevor personenbezogene Daten verarbeitet werden. Dazu gehört auch die Datenverarbeitung, die während der Installation erfolgen könnte, zum Beispiel zu Zwecken der Fehlerbeseitigung oder zum Tracking. Inhalt und Form dieser Informationen sind in Abschnitt 3.7 der vorliegenden Stellungnahme erläutert.

„Für den konkreten Fall" bedeutet, dass die Willensbekundung sich auf die Verarbeitung eines bestimmten Datenelements oder einer eingeschränkten Kategorie der Datenverarbeitung beziehen muss. Daher kann ein einfaches Tippen auf eine Schaltfläche „Installieren" nicht als gültige Einwilligung für die Verarbeitung personenbezogener Daten betrachtet werden, da eine Einwilligung nicht auf einer allgemein formulierten Autorisierung beruhen kann. In einigen Fällen können Nutzer eine differenzierte Einwilligung erteilen, wenn eine Einwilligung für jede Datenart eingeholt wird, auf die die App zugreifen soll.[34] Mit einem solchen Ansatz werden zwei wichtige rechtliche Anforderungen erfüllt: erstens die angemessene Unterrichtung der Nutzer über wichtige Elemente der Dienstleistung und zweitens die Einholung der Einwilligung für jeden konkreten Fall.[35] Der alternative Ansatz, bei dem ein App-Entwickler seine Nutzer auffordert, einen langen Text mit Nutzungsbedingungen und/oder eine lange Datenschutzerklärung zu akzeptieren, stellt keine Einwilligung für den konkreten Fall dar.[36]

---

[33] Ebenda, S. 19.

[34] Eine differenzierte Einwilligung bedeutet, dass Personen genau (spezifisch) kontrollieren können, welche von der App gebotenen Verarbeitungsfunktionen für personenbezogene Daten sie aktivieren möchten.

[35] Die Notwendigkeit einer solchen differenzierten Einwilligung wird auch von der FTC in ihrem aktuellen Bericht (siehe Fußnote 6), S. 15–16, ausdrücklich befürwortet: „*(…) die Plattformen sollten in Erwägung ziehen, Datenschutzerklärungen jeweils zum relevanten Zeitpunkt einzublenden und ausdrückliche positive Einwilligungen für die Erfassung anderer Inhalte einzuholen, die viele Verbraucher in vielen Zusammenhängen als sensibel einstufen würden, wie z. B. Fotos, Kontakte, Kalendereinträge oder Aufnahme von Audio- oder Videoinhalten.*"

[36] Ebenda, S. 34–35: „*Eine allgemeine Einwilligung ohne genaue Angabe des Ziels der Verarbeitung, der die betroffene Person zustimmt, entspricht dieser Anforderung nicht. Das bedeutet, dass die Informationen über das Ziel der Verarbeitung nicht Teil der allgemeinen Bestimmungen sein dürfen, sondern in einer gesonderten Einwilligungsklausel angeführt sein müssen.*"

Das Konzept „für den konkreten Fall“ betrifft auch die Praxis von Werbetreibenden und anderen Dritten, das Nutzerverhalten zu verfolgen (Tracking). Die von den Betriebssystemen und Apps vorgegebenen Standardeinstellungen müssen so gestaltet sein, dass jegliches Tracking vermieden wird, um es den Nutzern zu ermöglichen, für diese Art der Datenverarbeitung eine Einwilligung für den konkreten Fall zu erteilen. Diese Standardeinstellungen dürfen von Dritten nicht umgangen werden (wie derzeit häufig bei in Browsern implementierten „Do Not Track“-Mechanismen).

Beispiele für Einwilligung für den konkreten Fall

Eine App stellt Informationen über in der Umgebung befindliche Restaurants bereit. Der App-Entwickler muss eine Einwilligung für die Installation der App einholen. Für den Zugriff auf Geolokalisierungsdaten muss der App-Entwickler eine gesonderte Einwilligung einholen, z. B. während der Installation oder vor Zugriff auf die Geolokalisierung.

„Für den konkreten Fall“ bedeutet, dass die Einwilligung auf den spezifischen Zweck, dem Nutzer nahe gelegene Restaurants mitzuteilen, beschränkt sein muss. Ein Zugriff auf die Standortdaten des Endgeräts darf daher nur erfolgen, wenn der Nutzer die App für diesen Zweck verwendet. Die Einwilligung des Nutzers für die Verarbeitung von Geolokalisierungsdaten ist keine Erlaubnis dafür, dass die App fortlaufend Standortdaten vom Endgerät erfasst. Für diese weitere Verarbeitung wären eine zusätzliche Unterrichtung des Nutzers und eine gesonderte Einwilligung erforderlich.

Damit eine Kommunikations-App auf die Kontaktliste zugreifen kann, muss der Nutzer daher Kontakte auswählen können, mit denen er kommunizieren möchte, und darf nicht gezwungen sein, den Zugriff auf das gesamte Adressbuch (einschließlich der Kontaktdaten von Nichtnutzern dieses Dienstes, die der Verarbeitung der sie betreffenden Daten nicht zugestimmt haben können) zu gewähren.

Es ist jedoch zu beachten, dass selbst auch eine Einwilligung, die die vorstehenden Anforderungen erfüllt, keine Zustimmung zu einer Verarbeitung entgegen dem Gebot von Treu und Glauben und dem Gebot der Rechtmäßigkeit darstellt. Wenn der Zweck der Datenverarbeitung übermäßig und/oder unverhältnismäßig ist, besteht für den App-Entwickler selbst dann keine gültige Rechtsgrundlage für die Verarbeitung, wenn der Nutzer seine Einwilligung erteilt hat, und entsprechend ist in diesem Fall wahrscheinlich von einem Verstoß gegen die Datenschutzrichtlinie auszugehen.

Beispiel für übermäßige und unrechtmäßige Datenverarbeitung

Eine Wecker-App bietet eine optionale Funktion, mit der der Nutzer per Sprachbefehl den Weckton ausschalten oder den Schlummerstatus aktivieren kann. In diesem Beispiel ist die Einwilligung für die Aufnahmefunktion auf den Zeitraum beschränkt, in dem der Weckton erklingt. Jegliche Audioüberwachung oder -aufnahme in der Zeit, in der der Weckton nicht erklingt, wird als übermäßig und unrechtmäßig angesehen.

Bei Apps, die standardmäßig auf dem Endgerät installiert sind (bevor der Endnutzer das Gerät erwirbt), und bei sonstigen vom Betriebssystem durchgeführten Verarbeitungen, die einer Einwilligung als Rechtsgrundlage bedürfen, müssen die für die Verarbeitung Verantwortlichen sorgfältig abwägen, ob diese Einwilligung wirklich gültig ist. In vielen Fällen sollte ein gesonderter Einwilligungsmechanismus erwogen werden, zum Beispiel beim ersten Aufruf der App, um dem für die Verarbeitung Verantwortlichen eine ausreichende Gelegenheit zu geben, den Endnutzer vollständig zu informieren. Wenn es sich bei den Daten um spezielle Datenkategorien gemäß Artikel 8 der Datenschutzrichtlinie handelt, muss eine ausdrückliche Einwilligung vorliegen.

Und schließlich müssen Nutzer die Möglichkeit erhalten, ihre Einwilligung einfach und wirksam zu widerrufen. Dies wird in Abschnitt 3.8 der vorliegenden Stellungnahme näher ausgeführt.

3.4.2 Rechtsgrundlagen für Datenverarbeitung während der Nutzung der App

Wie bereits erläutert, bildet die Einwilligung die Rechtsgrundlage dafür, dass der App-Entwickler Informationen rechtmäßig lesen und/oder schreiben und daher personenbezogene Daten verarbeiten darf. In einer späteren Phase kann sich der App-Entwickler während der Nutzung der App für andere Arten der Datenverarbeitung auf weitere Rechtsgrundlagen berufen, sofern keine sensiblen personenbezogenen Daten verarbeitet werden.

Solche Rechtsgrundlagen können nach Artikel 7 Buchstaben b und f der Datenschutzrichtlinie die Notwendigkeit für die Erfüllung eines Vertrags mit der betroffenen Person oder die Notwendigkeit für rechtmäßige (geschäftliche) Interessen sein.

Diese Rechtsgrundlagen sind auf die Verarbeitung nicht sensibler Daten eines spezifischen Nutzers beschränkt und können nur in dem Umfang geltend gemacht werden, in dem eine bestimmte Datenverarbeitung für die Erbringung des gewünschten Dienstes erforderlich ist, bzw. – im Fall von Artikel 7 Buchstabe f – wenn die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Beispiele für vertragliche Rechtsgrundlagen

Ein Nutzer erteilt seine Einwilligung für die Installation einer Mobile-Banking-App. Um eine Anforderung für die Durchführung einer Zahlung zu erfüllen, benötigt die Bank keine gesonderte Einwilligung des Nutzers zur Weitergabe seines Namens und seiner Kontonummer an den Zahlungsempfänger. Diese Weitergabe ist für die Erfüllung des Vertrags mit diesem spezifischen Nutzer unbedingt erforderlich, und daher hat die Bank eine Rechtsgrundlage gemäß Artikel 7 Buchstabe b der Datenschutzrichtlinie. Die gleiche Argumentation gilt für Kommunikations-Apps. Wenn Kommunikations-Apps einer anderen Person, mit der der Nutzer kommunizieren möchte, wichtige Informationen wie einen Kontonamen, eine E-Mail-Adresse oder eine Telefonnummer übermitteln, ist diese Weitergabe von Daten naturgemäß für die Erfüllung des Vertrags erforderlich.

3.5 Zweckbindung und Datenminimierung

Die Zweckbindung und die Datenminimierung sind Grundprinzipien der Datenschutzrichtlinie. Aufgrund der jeweiligen Zweckbindung können Nutzer bewusst entscheiden, ob sie ihre personenbezogenen Daten einer Partei anvertrauen möchten, da sie erfahren, wie ihre Daten verwendet werden, und da sie aufgrund der Beschreibung der Zweckbindung verstehen können, wozu ihre Daten verwendet werden. Die Zwecke der Datenverarbeitung müssen daher genau festgelegt und für einen durchschnittlichen Nutzer ohne rechtliche oder technische Fachkenntnisse verständlich sein.

Gleichzeitig bedeutet die Zweckbindung, dass App-Entwickler einen guten Überblick über ihren Business Case haben, bevor sie mit der Erfassung personenbezogener Daten von Nutzern beginnen. Personenbezogene Daten dürfen nur für Zwecke verarbeitet werden, die dem Gebot von Treu und Glauben und dem Gebot der Rechtmäßigkeit entsprechen (Artikel 6 Absatz 1 Buchstabe a der Datenschutzrichtlinie). Diese Zwecke müssen vor Durchführung der Datenverarbeitung festgelegt sein.

Der Grundsatz der Zweckbindung schließt plötzliche Änderungen in den wichtigen Bedingungen der Verarbeitung aus.

Beispiel: Eine App hatte sollte den Nutzern ursprünglich ermöglichen, per E-Mail miteinander zu kommunizieren. Der Entwickler beschließt jedoch, sein Geschäftsmodell zu ändern und führt die E-Mail-Adressen seiner Nutzer mit den Telefonnummern von Nutzern einer anderen App zusammen. In diesem Fall müssten die jeweiligen für die Verarbeitung Verantwortlichen alle Nutzer einzeln verständigen und ihre vorherige ohne jeden Zweifel gegebene Einwilligung für diesen neuen Zweck der Verarbeitung ihrer personenbezogenen Daten einholen.

Die Zweckbindung ist mit dem Grundsatz der Datenminimierung eng verknüpft. Um eine unnötige und potenziell unrechtmäßige Datenverarbeitung zu verhindern, müssen App-Entwickler sorgfältig abwägen, welche Daten für die Durchführung der gewünschten Funktion unbedingt erforderlich sind.

Apps können einen Zugriff auf viele Funktionen des Endgeräts erlangen und daher viele Aktionen durchführen (z. B. eine Stealth SMS senden oder auf Bilder und das gesamte Adressbuch zugreifen). Viele App-Stores unterstützen (halb-) automatische Aktualisierungen, bei denen der App-Entwickler unter geringen Eingaben des Endnutzers oder sogar ohne jegliche Eingaben des Endnutzers neue Funktionen integrieren und verfügbar machen kann.

Die Datenschutzgruppe betont an dieser Stelle, dass Dritte, die über Apps Zugriff auf die Nutzerdaten erlangen, die Grundsätze der Zweckbindung und der Datenminimierung beachten müssen. Eindeutige und häufig unveränderliche Gerätekennungen sollten nicht zur interessenbezogenen Werbung und/oder Analyse verwendet werden, da die Nutzer keine Möglichkeit haben, ihre Einwilligung zu widerrufen. App-Entwickler sollten gewährleisten, dass eine schleichende Ausweitung der Zweckbestimmung verhindert wird, indem sie die Verarbeitung von einer App-Version zur nächsten nicht ändern, ohne den Endnutzern angemessene Informationsmeldungen zu senden und Gelegenheiten einzuräumen, entweder die Verarbeitung zu unterbinden oder den gesamten Dienst zu kündigen. Außerdem sollten technische Mittel bereitgestellt werden, mit denen die Nutzer die Angaben über die erklärten Zwecke überprüfen können, indem sie Zugriff auf die Informationen über die ausgehende Datenverkehrsmenge pro App im Verhältnis zum nutzerinitiierten Datenverkehr erhalten.

Die Unterrichtung der Nutzer und Nutzerkontrollen sind die wichtigsten Funktionen, mit den die Beachtung der Grundsätze der Datenminimierung und der Zweckbindung gewährleistet werden kann.

Indem die Hersteller von Betriebssystemen und Endgeräten sowie App-Stores über Programmierschnittstellen auf die zugrunde liegenden Daten auf dem Endgerät zugreifen, erhalten sie die Möglichkeit, spezifische Regeln durchzusetzen und den Endnutzern angemessene Informationen bereitzustellen. Beispielsweise sollten die Hersteller von Betriebssystemen und Endgeräten eine Programmierschnittstelle mit präzisen Kontrollfunktionen zur Differenzierung zwischen den verschiedenen Datenarten bereitstellen und gewährleisten, dass App-Entwickler Zugriff nur zu den Daten anfordern können, die für die (rechtmäßige) Funktion ihrer App unbedingt erforderlich sind. Die von den App-Entwicklern angeforderten Datenarten können dann im App-Store deutlich angezeigt werden, um die Nutzer vor der Installation entsprechend zu informieren.

In dieser Hinsicht beruht die Kontrolle des Zugriffs auf die Daten, die auf dem Endgerät gespeichert sind, auf verschiedenen Mechanismen:

a. Hersteller von Betriebssystemen und Endgeräten legen **Regeln** fest, die für das Angebot von Apps in ihrem App-Store gelten: App-Entwickler müssen diese Regeln beachten oder das Risiko eingehen, dass ihre Apps in diesen App-Stores nicht angeboten werden können.[37]

b. Die **Programmierschnittstellen (APIs)** der Betriebssysteme legen Standardmethoden für den Zugriff von Apps auf die auf dem Telefon gespeicherten Daten fest. Sie wirken sich auch auf die serverseitige Erfassung von Daten aus.

c. **Ex-ante-Kontrollen** sind Kontrollen, die vor der Installation einer App durchgeführt werden.[38]

d. **Ex-post-Kontrollen** sind Kontrollen, die nach der Installation einer App durchgeführt werden.

3.6 Sicherheit

Gemäß Artikel 17 der Datenschutzrichtlinie müssen die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Schutzes der von ihnen verarbeiteten personenbezogenen Daten durchführen. Insoweit müssen alle in Abschnitt 3.3 genannten Akteure Maßnahmen entsprechend ihrer jeweiligen Rolle und Verantwortlichkeit durchführen.

Durch die Erfüllung der Sicherheitsverpflichtung werden zwei Ziele erreicht: Die Nutzer werden in die Lage versetzt, ihre Daten besser zu kontrollieren, und das Vertrauen in die Rechtspersonen, die die Nutzerdaten tatsächlich nutzen oder verarbeiten, wird erhöht.

Um ihren jeweiligen Sicherheitsverpflichtungen als für die Verarbeitung Verantwortliche nachzukommen, müssen App-Entwickler, App-Stores, Hersteller von Betriebssystemen und Endgeräten sowie Dritte die Grundsätze des eingebauten Datenschutzes (Privacy by Design) und der datenschutzfreundlichen Voreinstellungen (Privacy by Default) beachten. Dies setzt die fortlaufende Bewertung bestehender wie zukünftiger Datenschutzrisiken sowie die Einführung und Bewertung wirksamer Maßnahmen zur Minimierung dieser Risiken voraus (u. a. durch Datenminimierung).

[37] Endgeräte, die mittels eines „Jailbreak“ entsperrt wurden, erlauben die Installation von Apps außerhalb offizieller App-Stores; Android-Geräte erlauben ebenfalls die Installation von Apps, die von anderen Quellen erworben wurden.

[38] Sonderfall: vorinstallierte Apps.

App-Entwickler

Hersteller von Betriebssystemen und Endgeräten sowie unabhängige Dritte (z. B. die ENISA) haben zahlreiche Leitlinien zur Sicherheit mobiler Apps veröffentlicht.[39]

Ein Überblick über sämtliche bewährten Praktiken im Bereich der Sicherheit bei der Entwicklung von Apps würde den Rahmen dieser Stellungnahme sprengen. Die Datenschutzgruppe nutzt diese Gelegenheit jedoch für einen Überblick über die Sicherheitspraktiken, die mit schwerwiegenden Auswirkungen auf die Grundrechte von App-Nutzern verbunden sein können.

Eine wichtige Entscheidung vor der Konzeption einer App ist die Frage, wo die Daten gespeichert werden. In einigen Fällen werden Nutzerdaten auf dem Endgerät gespeichert, aber App-Entwickler können auch eine Client-Server-Architektur nutzen. In diesem Fall werden personenbezogene Daten auf die Systeme der Dienstleister übertragen oder kopiert. Wenn die Speicherung und Verarbeitung der Daten auf dem Gerät erfolgt, haben die Endnutzer die größte Kontrolle über diese Daten. Sie können die Daten beispielsweise löschen, wenn sie ihre Einwilligung für ihre Verarbeitung widerrufen. Eine sichere Speicherung von Daten an einem entfernten Standort kann jedoch eine Wiederherstellung der Daten nach Diebstahl oder Verlust eines Geräts erleichtern. Mischlösungen sind ebenfalls möglich.

App-Entwickler müssen eine klare Strategie für die Entwicklung und die Verbreitung der Software festlegen. Auch die Hersteller der Betriebssysteme und der Endgeräte spielen bei der Förderung einer sicheren Verarbeitung durch Apps eine Rolle; diese Rolle wird in einem späteren Abschnitt näher ausgeführt. Außerdem müssen App-Entwickler und App-Stores eine sicherheitsfördernde Umgebung erarbeiten und einführen, in der geeignete Hilfsmittel die Verbreitung bösartiger Apps verhindern und die einfache Installation/Deinstallation einzelner Apps ermöglichen.

Bewährte Praktiken, die während der Konzeption einer App implementiert werden können, beinhalten die Minimierung der Länge und der Komplexität des Codes sowie die Implementierung von Kontrollen, durch die eine unbeabsichtigte Datenübertragung oder ein unberechtigter Datenzugriff ausgeschlossen wird. Ferner sollten alle Eingaben validiert werden, um einen Pufferüberlauf oder Injection-Angriffe zu verhindern. Weitere erwähnenswerte Sicherheitsmechanismen sind angemessene Strategien für Sicherheitspatches und regelmäßige unabhängige Systemsicherheitsprüfungen. Außerdem sollten die Kriterien für die Konzeption von Apps regelmäßig das Prinzip der geringstmöglichen Berechti-

[39] ENISA „Smartphone Secure Development Guideline“: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

gungsvergabe („Least Privilege"-Prinzip) beinhalten, nach dem Apps nur auf die Daten zugreifen können, die sie tatsächlich benötigen, um eine Funktion für den Nutzer bereitzustellen. App-Entwickler und App-Stores sollten die Nutzer auch durch Warnhinweise motivieren, diese bewährten Konzeptionspraktiken durch gute Nutzerpraktiken (z. B. Aktualisierung der Apps auf die neuesten verfügbaren Versionen) zu ergänzen, und durch wiederholte Hinweise daran erinnern, die Verwendung des gleichen Passworts für verschiedene Dienste zu vermeiden.

In der Konzeptionsphase von Apps müssen die App-Entwickler auch Maßnahmen zur Verhinderung eines unberechtigten Zugriffs auf personenbezogene Daten treffen, indem sie sicherstellen, dass die Daten gegebenenfalls sowohl bei der Übertragung als auch nach Speicherung geschützt sind.

Mobile Apps sollten innerhalb spezifischer Speicherbereiche des Endgeräts („Sandboxes"[40]) laufen, um die Folgen von Schadprogrammen/bösartigen Apps zu verringern. Die App-Entwickler müssen in enger Zusammenarbeit mit dem Hersteller des Betriebssystems und/oder dem App-Store verfügbare Mechanismen einsetzen, durch die die Nutzer zum einen sehen können, welche Daten von welchen Apps verarbeitet werden, und zum anderen Berechtigungen gezielt aktivieren und deaktivieren können. Die Verwendung verborgener Funktionen sollte nicht zugelassen sein.

App-Entwickler müssen ihre Methoden der Nutzeridentifizierung und -authentifizierung bewusst wählen. Sie sollten keine persistenten (gerätespezifischen) Kennungen, sondern stattdessen appspezifische oder temporäre Kennungen mit niedriger Entropie verwenden, um ein langfristiges Tracking der Nutzer zu verhindern. Es sollten datenschutzfreundliche Authentifizierungsmechanismen in Erwägung gezogen werden. Bei der Authentifizierung von Nutzern müssen die App-Entwickler besondere Sorgfalt auf die Verwaltung von Nutzerkennungen und Passwörtern verwenden. Passwörter müssen verschlüsselt und sicher als verschlüsselte kryptografische Hashwerte gespeichert werden. Die Bereitstellung eines Tests für die Sicherheit der gewählten Passwörter für die Nutzer ist ebenfalls eine gute Methode für die Förderung besserer Passwörter (Entropieprüfung). Gegebenenfalls (beim Zugriff auf sensible Daten, aber auch beim Zugriff auf zahlungspflichtige Ressourcen) könnte eine erneute Authentifizierung in Betracht gezogen werden. Dabei könnten mehrere Faktoren einbezogen und unterschiedliche Kanäle (z. B. Senden des Zugangscodes per SMS) und/oder auf den Endnutzer (und nicht auf das Endgerät) bezogene Authentifizierungsdaten genutzt werden. Außerdem sollten bei der Wahl von Sitzungskennungen nichtvorhersagbare Zeichenfolgen verwendet werden, möglicherweise kombiniert mit Kontextinformationen wie Datum und Uhrzeit, aber auch IP-Adresse oder Geolokalisierungsdaten.

[40] Eine „Sandbox" ist ein Sicherheitsmechanismus zur Trennung laufender Programme.

App-Entwickler sollten auch die Anforderungen der Datenschutzrichtlinie in Bezug auf Verletzungen des Schutzes personenbezogener Daten und die Notwendigkeit einer proaktiven Unterrichtung der Nutzer beachten. Diese Anforderungen gelten derzeit zwar nur für Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste. Es wird jedoch erwartet, dass die Verpflichtung entsprechend den Vorschlägen der Kommission im Rahmen der zukünftigen Datenschutzrichtlinie (COM 2012/0011/COD) auf alle für die Verarbeitung Verantwortlichen (und Auftragsverarbeiter) ausgeweitet wird. Auch dies unterstreicht die Notwendigkeit der Erstellung und der fortlaufenden Bewertung eines umfassenden „Sicherheitsplans", der die Erfassung, Speicherung und Verarbeitung sämtlicher personenbezogener Daten abdeckt, um solche Datenschutzverletzungen sowie die Verhängung der für solche Fälle vorgesehenen hohen Geldstrafen zu vermeiden. Der Sicherheitsplan muss unter anderem ein Schwachstellenmanagement (Vulnerability Management) und sichere Freigabeabläufe für zuverlässige Aktualisierungen zur Fehlerbehebung (Bugfixes) vorsehen.

Die Verantwortung der App-Entwickler für die Sicherheit ihrer Produkte endet nicht mit der Freigabe einer Arbeitsversion auf dem Markt. Wie jedes Software-Produkt können Apps Sicherheitsmängel und Schwachstellen aufweisen, und die App-Entwickler müssen entsprechende Fixes oder Patches entwickeln und entweder den Nutzern direkt zur Verfügung stellen oder den Akteuren übermitteln, die diese Fixes oder Patches den Nutzern bereitstellen.

App-Stores

App-Stores sind ein wichtiger Vermittler zwischen Endnutzern und App-Entwicklern und sollten die Apps einer Reihe robuster und wirksamer Kontrollen unterziehen, bevor sie Apps für den Markt freigeben. Sie sollten Informationen über die tatsächlich durchgeführten Kontrollen bereitstellen (u. a. Informationen über die Art der durchgeführten Datenschutzprüfungen).

Diese Maßnahme kann zwar die Verbreitung bösartiger Apps nicht vollständig unterbinden, aber die Statistik zeigt, dass die Verfügbarkeit bösartiger Funktionen in „offiziellen" App-Stores durch diese Praxis stark reduziert wird.[41] Zur Bewältigung der großen Mengen von Apps, die täglich neu angeboten werden, könnte dieser Prozess durch die Verfügbarkeit automatischer Analysewerkzeuge und durch die Einführung von Informationsaustausch-Kanälen zwischen Sicherheitsfachleuten und Software-Spezialisten sowie durch die Einführung wirksamer Verfahren und Strategien für die Handhabung gemeldeter Probleme optimiert werden.

Zusätzlich zur Prüfung von Apps vor der Aufnahme in den App-Store könnte auch ein öffentlicher Reputationsmechanismus für Apps eingeführt werden. Die Nutzer sollten sich nicht nur daran orientieren, wie „cool" eine App ist, sondern

[41] *„Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets"*, Y Zhou u. a., Network and Distributed System Security Symposium (NDSS) 2012.

auch Grundlage der angebotenen Funktionen berücksichtigen; dabei sind insbesondere die Mechanismen zur Gewährleistung des Datenschutzes und des Schutzes der Privatsphäre zu beachten. Außerdem sollten Reputationsmechanismen so gestaltet sein, dass falsche Bewertungen verhindert werden. Die Qualifizierungs- und Reputationsmechanismen für Apps können wirksam zum Vertrauensaufbau zwischen den verschiedenen Akteuren beitragen, besonders wenn die Daten über eine lange Kette von Dritten ausgetauscht werden.

App-Stores verfügen häufig über eine Methode zur Fern-Deinstallation bösartiger oder unsicherer Apps. Bei ungeeigneter Konzipierung kann dieser Mechanismus allerdings kontraproduktiv für das angestrebte Ziel sein, dass die Nutzer ihre Daten besser kontrollieren können sollen. Ein datenschutzfreundliches Mittel zur Fern-Deinstallation von Apps durch einen App-Store sollte daher auf der Unterrichtung und der Einwilligung der Nutzer beruhen. Unter eher praktischen Aspekten sollte den Nutzern darüber hinaus die Übermittlung von Rückmeldungen ermöglicht werden, damit die Nutzer Informationen über Sicherheitsprobleme bei ihren Apps und über die Wirksamkeit möglicher Fern-Deinstallationsverfahren mitteilen können.

Ebenso wie die App-Entwickler sollten auch die App-Stores zukünftige Mitteilungspflichten bei Verletzungen des Schutzes personenbezogener Daten berücksichtigen und eng mit den App-Entwicklern zusammenarbeiten, um entsprechende Verletzungen zu vermeiden.

Hersteller von Betriebssystemen und Endgeräten

Hersteller von Betriebssystemen und Endgeräten sind ebenfalls wichtige Akteure bei der Festlegung von Mindeststandards und bewährten Praktiken für App-Entwickler, nicht nur in Bezug auf die Sicherheit der zugrunde liegenden Software und der Programmierschnittstellen, sondern auch in Bezug auf die Werkzeuge, Leitlinien und Referenzmaterialien, die sie bereitstellen. Hersteller von Betriebssystemen und Endgeräten sollten sichere und bekannte Verschlüsselungsalgorithmen bereitstellen und angemessene Schlüssellängen unterstützen. Außerdem sollten sie strenge und sichere Authentifizierungsmechanismen für die App-Entwickler bereitstellen (z. B. die Verwendung von seitens vertrauenswürdiger Zertifizierungsbehörden signierten Zertifikaten zur Prüfung der Autorisierung einer entfernten Ressource). Dadurch würde auch die Notwendigkeit der Entwicklung proprietärer Authentifizierungsmechanismen durch App-Entwickler entfallen. In der Praxis werden diese Mechanismen häufig unzureichend umgesetzt und können eine gravierende Schwachstelle sein.[42]

[42] Vor Kurzem wurde darauf hingewiesen, dass fehlende visuelle Sicherheitshinweise für die SSL-/TLS-Verwendung sowie die unzureichende Verwendung von SSL/TLS für Man-in-the-Middle-Angriffe (MITM-Angriffe) genutzt werden können. Aktuellen Forschungsergebnissen zufolge umfasst die gesamte installierte Basis der Apps mit bestätigten Schwachstellen in Bezug auf MITM-Angriffe mehrere Millionen Nutzer. „*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security*“, Bernd Freisleben und Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

Der Zugriff auf personenbezogene Daten und die Verarbeitung solcher Daten durch Apps sollten über in die Programmierschnittstelle integrierte Klassen und Methoden erfolgen, die angemessene Kontrollen und Sicherheitsvorrichtungen bieten. Die Hersteller von Betriebssystemen und Endgeräten sollten sicherstellen, dass die Methoden und Funktionen für den Zugriff auf personenbezogene Daten Funktionen umfassen, die auf die Implementierung differenzierter Einwilligungsanfragen abzielen. Ferner sollten Maßnahmen ergriffen werden, um den Zugriff auf personenbezogene Daten unter Verwendung von Low-Level-Funktionen oder anderen Mitteln (die in die Programmierschnittstellen integrierte Kontrollen und Sicherheitsvorrichtungen umgehen könnten) auszuschließen oder einzuschränken.

Die Hersteller von Betriebssystemen und Endgeräten müssen klare Prüfpfade für die Geräte entwickeln, damit die Endnutzer eindeutig feststellen können, welche Apps auf die Daten auf ihren Geräten zugegriffen haben.

Alle Parteien müssen rasch auf Sicherheitsschwachstellen reagieren, damit Endnutzer nicht unnötig lange mit Sicherheitsmängeln konfrontiert sind. Einige Hersteller von Betriebssystemen und Endgeräten (sowie Telekommunikationsbetreiber, die Markengeräte verbreiten) stellen leider keine langfristige Unterstützung für Betriebssystem-Versionen bereit; in diesen Fällen sind die Nutzer in Bezug auf bekannte Sicherheitsschwachstellen nicht geschützt. Gemeinsam mit den App-Entwicklern müssen die Hersteller von Betriebssystemen und Endgeräten die Endnutzer im Voraus über den Zeitraum informieren, in dem sie regelmäßige Sicherheitsaktualisierungen erwarten können. Zudem sollten sie die Nutzer schnellstmöglich unterrichten, wenn ein Sicherheitsproblem mithilfe einer Aktualisierung behoben werden muss.

Dritte

Die vorstehend genannten Sicherheitsfunktionen und -überlegungen gelten auch für Dritte, wenn diese personenbezogene Daten für ihre eigenen Zwecke erfassen und verarbeiten (d. h. in erster Linie Werbetreibende und Analysedienstleister). Dies umfasst die sichere Übertragung und die verschlüsselte Speicherung von eindeutigen Gerätekennungen und von Kennungen der App-Nutzer sowie von sonstigen personenbezogenen Daten.

3.7 Information

3.7.1 Informationspflicht und vorgeschriebener Inhalt

Gemäß Artikel 10 der Datenschutzrichtlinie hat jede betroffene Person das Recht, die Identität des für die Verarbeitung Verantwortlichen zu erfahren, der ihre personenbezogenen Daten verarbeitet. In Bezug auf Apps hat der Endnutzer zudem

das Recht, zu erfahren, welche Art personenbezogener Daten verarbeitet wird und für welchen Zweck die Daten verwendet werden sollen. Wenn die personenbezogenen Daten des Nutzers aus den Datenbeständen anderer Akteure im App-Ökosystem erfasst werden (entsprechend der Beschreibung in Abschnitt 3.3 der vorliegenden Stellungnahme), hat der Endnutzer gemäß Artikel 11 der Datenschutzrichtlinie trotzdem das Recht, über eine solche Datenverarbeitung in gleicher Weise unterrichtet zu werden. Wenn der entsprechende für die Verarbeitung Verantwortliche personenbezogene Daten verarbeitet, muss er potenzielle Nutzer zumindest mitteilen,

– wer er ist (Identität und Kontaktdaten),

– welche Kategorien personenbezogener Daten der App-Entwickler im Einzelnen erfassen und verarbeiten wird,

– warum die betreffenden personenbezogenen Daten erfasst und verarbeitet werden (genaue Zwecke),

– ob die Daten an Dritte weitergegeben werden,

– wie Nutzer ihre Rechte in Bezug auf Widerruf der Einwilligung und Löschung von Daten wahrnehmen können.

Die Verfügbarkeit dieser Informationen über die Verarbeitung personenbezogener Daten ist entscheidend für die Einholung der Einwilligung für die Datenverarbeitung vom Nutzer. Eine Einwilligung kann nur gültig sein, wenn die betroffene Person zuvor über die wichtigsten Elemente der Datenverarbeitung informiert wurde. Wenn diese Informationen erst bereitgestellt werden, nachdem die App bereits mit der Verarbeitung personenbezogener Daten begonnen hat (was häufig schon während der Installation geschieht), wird dies nicht als ausreichend erachtet und ist rechtlich unwirksam. In Übereinstimmung mit dem FTC-Bericht betont die Datenschutzgruppe die Notwendigkeit, Informationen zu dem Zeitpunkt bereitzustellen, an dem sie für die Verbraucher relevant sind: direkt vor der Erfassung von Daten durch Apps. Die Unterrichtung darüber, welche Daten verarbeitet werden, ist besonders wichtig in Anbetracht des umfassenden Zugriffs, den Apps normalerweise auf Sensoren und Datenstrukturen auf dem Gerät haben, wobei dieser Zugriff in vielen Fällen nicht intuitiv offensichtlich ist. Eine angemessene Unterrichtung ist auch dann von entscheidender Bedeutung, wenn die App besondere Kategorien personenbezogener Daten verarbeitet, z. B. Daten über den Gesundheitszustand, politische Überzeugungen, sexuelle Ausrichtung usw. Und schließlich sollte der App-Entwickler deutlich zwischen obligatorischen und optionalen Informationen unterscheiden, und das System sollte dem Nutzer ermöglichen, mit datenschutzfreundlichen Standardoptionen den Zugriff auf optionale Informationen zu verweigern.

Hinsichtlich der Identität des für die Verarbeitung Verantwortlichen ist festzustellen, dass die Nutzer wissen müssen, wer für die Verarbeitung ihrer personenbezogenen Daten rechtlich verantwortlich ist und wie der für die Verarbeitung Verantwortliche kontaktiert werden kann. Ansonsten können sie ihre Rechte (z. B. das Recht auf Zugang zu den (an einem entfernten Standort) über sie gespeicherten Daten) nicht wahrnehmen. Aufgrund der Fragmentierung im App-Umfeld ist es überaus wichtig, dass für jede App ein einziger Ansprechpartner besteht, der für die gesamte Datenverarbeitung über die jeweilige App die Verantwortung übernimmt. Es darf nicht dem Endnutzer überlassen bleiben, die Beziehungen zwischen App-Entwicklern und anderen Parteien zu recherchieren, die personenbezogene Daten über die App verarbeiten.

In Bezug auf den Zweck/die Zwecke müssen die Nutzer angemessen darüber informiert werden, welche Daten über sie erfasst werden und warum die Daten erfasst werden. Die Nutzer sollten in klarer und verständlicher Sprache darüber unterrichtet werden, ob die Daten von Dritten weiterverwendet werden können, und wenn ja, für welche Zwecke. Ungenau festgelegte Zwecke wie „Produktinnovation" sind für die Unterrichtung der Nutzer unzureichend. Es sollte klar mitgeteilt werden, ob die Nutzer zu einem späteren Zeitpunkt um ihre Einwilligung zur Weitergabe von Daten an Dritte zu Werbe- und/oder Analysezwecken gebeten werden. Den App-Stores obliegt die wesentliche Verantwortung, sicherzustellen, dass diese Informationen für jede App verfügbar und leicht zugänglich sind.

Die App-Stores tragen wesentliche Verantwortung dafür, eine angemessene Unterrichtung der Nutzer sicherzustellen. Es wird nachdrücklich empfohlen, visuelle Hinweise oder Symbole in Bezug auf die Datenverwendungen einzusetzen, um die Nutzer über die Arten der Datenverarbeitung zu informieren.

Zusätzlich zu dem genannten Mindestumfang der Informationen, die für die Einholung einer Einwilligung der App-Nutzer erforderlich sind, empfiehlt die Datenschutzgruppe zum Zwecke einer Verarbeitung nach Treu und Glauben nachdrücklich, dass die für die Verarbeitung Verantwortlichen den Nutzern auch folgende Informationen bereitstellen:

– Erwägungen zur Verhältnismäßigkeit für die Arten der Daten auf dem Gerät, die erfasst werden oder auf die zugegriffen wird,

– Speicherfristen für die Daten,

– vom für die Verarbeitung Verantwortlichen ergriffene Sicherheitsmaßnahmen.

Außerdem empfiehlt die Datenschutzgruppe, dass App-Entwickler in ihren für europäische Nutzer bestimmten Datenschutzerklärungen Informationen darüber aufnehmen, in welcher Weise die App dem europäischen Datenschutzrecht ent-

spricht. In diesem Zusammenhang sollten auch mögliche Übertragungen personenbezogener Daten aus Europa beispielsweise in die USA berücksichtigt werden. Außerdem sollte erläutert werden, ob und wie die App in solchen Fällen der Safe-Harbor-Vereinbarung entspricht.

3.7.2 Form der Aufklärung

Die entscheidenden Informationen über die Datenverarbeitung müssen den Nutzern vor der Installation der App über den App-Store zur Verfügung stehen. Außerdem müssen die relevanten Informationen über die Datenverarbeitung auch nach der Installation innerhalb der App zugänglich sein.

Hinsichtlich der Aufklärung der Nutzer kommt den App-Stores zusammen mit den Entwicklern der Apps die Rolle eines gemeinsam für die Verarbeitung Verantwortlichen zu. In dieser Eigenschaft müssen sie sicherstellen, dass jede App die entscheidenden Informationen über die Verarbeitung personenbezogener Daten bereitstellt. Sie sollten die Hyperlinks zu Seiten mit Datenschutzinformationen überprüfen und Apps mit fehlerhaften Links oder anderweitig nicht zugänglichen Informationen über die Datenverarbeitung entfernen.

Nach Auffassung der Datenschutzgruppe sollten Informationen über die Verarbeitung personenbezogener Daten ebenfalls verfügbar und leicht auffindbar sein, beispielsweise innerhalb des App-Store und vorzugsweise auf den regulären Websites des für die App verantwortlichen App-Entwicklers. Es ist nicht akzeptabel, dass Nutzer vom App-Entwickler oder einem sonstigen für die Verarbeitung Verantwortlichen nicht direkt informiert werden, sondern genötigt werden, im Internet nach Informationen über die Datenverarbeitungsstrategie einer App zu suchen.

Zumindest sollte jede App eine lesbare, verständliche und leicht zugängliche Datenschutzerklärung beinhalten, in der sämtliche vorstehend genannten Informationen enthalten sind. Viele Apps erfüllen diese Mindestanforderung an die Transparenz nicht. Nach einer FPF-Studie vom Juni 2012 haben 56 % der kostenpflichtigen Apps und fast 30 % der kostenlosen Apps keine Datenschutzerklärung.

Apps, die keine personenbezogenen Daten verarbeiten oder nicht für eine solche Verarbeitung bestimmt sind, sollten dies in ihrer Datenschutzerklärung klar angeben.

Natürlich ist der Umfang der auf einem kleinen Display darstellbaren Informationen beschränkt. Dies ist jedoch keine Entschuldigung für eine unzureichende Information der Endnutzer. Mit unterschiedlichen Strategien kann sichergestellt werden, dass den Nutzern die wichtigsten Elemente des Dienstes bekannt sind. Die Datenschutzgruppe hält die Verwendung von Mehrebenen-Erklärungen für

hilfreich (siehe Stellungnahme 10/2004 der Datenschutzgruppe),[43] bei denen die zuerst angezeigte Erklärung die im EU-Rechtsrahmen vorgeschriebenen Mindestinformationen enthält, und weitere Informationen über Hyperlinks zur vollständigen Datenschutzerklärung abzurufen sind. Die Informationen sollten direkt auf dem Bildschirm angezeigt werden und leicht zugänglich und gut sichtbar sein. Neben verständlichen Informationen, die für das kleine Display mobiler Endgeräte geeignet sind, müssen die Nutzer die Möglichkeit haben, über Links zu umfassenderen Erläuterungen – beispielsweise in der Datenschutzerklärung – zu wechseln, in denen ausgeführt wird, wie die App personenbezogene Daten verwendet, wer der für die Verarbeitung Verantwortliche ist und wo ein Nutzer seine Rechte geltend machen kann.

Dieser Ansatz kann mit der Verwendung von Symbolen und Bildern sowie von Video- und Audiodaten kombiniert werden und kontextbezogene Echtzeitmeldungen nutzen, wenn eine App auf das Adressbuch oder auf Fotos zugreift.[44] Diese Symbole müssen aussagekräftig sein (d. h. klar, selbsterklärend und eindeutig). Naturgemäß kommt in diesem Zusammenhang auch dem Hersteller des Betriebssystems wesentliche Mitverantwortung im Hinblick auf die Unterstützung der Nutzung solcher Symbole zu.

App-Entwickler verfügen über hervorragende Kenntnisse in der Programmierung und Konzeption komplexer Benutzeroberflächen für kleine Displays, und die Datenschutzgruppe fordert die Branche dazu auf, diese Kreativität für die Bereitstellung weiterer innovativer Lösungen für die wirksame Unterrichtung von Nutzern mobiler Endgeräte zu nutzen. Um sicherzustellen, dass die Informationen tatsächlich für Nutzer ohne technischen oder rechtlichen Hintergrund verständlich sind, empfiehlt die Datenschutzgruppe (in Übereinstimmung mit dem FTC-Bericht) dringend, Verbrauchertests für ausgewählte Informationsstrategien durchzuführen.[45]

3.8 Rechte der betroffenen Person

Nach den Artikeln 12 und 14 der Datenschutzrichtlinie müssen App-Entwickler und andere für die Verarbeitung Verantwortliche den Nutzern im Ökosystem mobiler Apps ermöglichen, ihre Rechte auf Auskunft, Berichtigung und Löschung sowie das Recht auf Widerspruch gegen die Datenverarbeitung wahrzunehmen. Wenn ein Nutzer seinen Auskunftsanspruch geltend macht, muss der für die Verarbeitung Verantwortliche dem Nutzer Informationen über die verarbeiteten Daten und über die Quelle dieser Daten bereitstellen. Wenn der für die Verarbeitung Verantwortliche auf der Grundlage der gesammelten Daten automatisierte

[43] Stellungnahme 10/2004 der Artikel-29-Datenschutzgruppe zu einheitlicheren Bestimmungen über Informationspflichten (Juli 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.

[44] Beispiel: Das auf iPhones verwendete Warnsymbol für die Verarbeitung von Geolokalisierungsdaten.

[45] FTC-Bericht (siehe Fußnote 6), S. 16.

Entscheidungen trifft, muss er den Nutzer auch über die diesen Entscheidungen zugrunde liegende Logik informieren. Dies kann etwa der Fall sein, wenn aufgrund finanzieller oder gesundheitsbezogener Daten oder sonstiger Profildaten die Leistungsfähigkeit oder das Verhalten des Nutzers bewertet werden. Auf Aufforderung des Nutzers muss der für die Verarbeitung Verantwortliche die Berichtigung, Löschung oder Sperrung personenbezogener Daten ermöglichen, wenn diese Daten unvollständig oder unrichtig sind oder wenn die Verarbeitung der Daten unrechtmäßig ist.

Damit die Nutzer die Verarbeitung ihrer personenbezogenen Daten kontrollieren können, müssen Apps die Nutzer klar und gut sichtbar über das Bestehen dieser Auskunfts- und Korrekturmechanismen informieren. Die Artikel-29-Datenschutzgruppe empfiehlt die Konzeption und Implementierung einfacher, aber sicherer Online-Auskunftswerkzeuge. Auskunftswerkzeuge sollten vorzugsweise entweder in der eigentlichen App oder durch Bereitstellung eines Links zu einer Online-Funktion verfügbar sein, über die für die Nutzer sofort ersichtlich ist, welche ihrer Daten verarbeitet werden, und über die die Nutzer die jeweils erforderlichen Erläuterungen erhalten. Ähnliche Initiativen wurden von Online-Dienstleistern durchgeführt (z. B. unterschiedliche „Dashboards“ zur Darstellung erfasster Informationen oder sonstige Auskunftsmechanismen).

Die Notwendigkeit einer einfachen Online-Auskunft ist besonders groß bei Apps, die umfangreiche Nutzerprofile verarbeiten (z. B. bei sozialen Apps, Netzwerk- und Nachrichten-Apps oder Apps, die sensible oder finanzielle Daten verarbeiten). Die Auskunft sollte natürlich nur erteilt werden, wenn die Identität der betroffenen Person festgestellt wurde, um die Weitergabe personenbezogener Daten an Dritte zu verhindern. Diese Verpflichtung zur Prüfung der Identität sollte jedoch nicht zu einer zusätzlichen, übermäßigen Erfassung personenbezogener Daten über die betroffene Person führen. In vielen Fällen könnte eine Authentifizierung anstelle einer (vollständigen) Identifizierung ausreichen.

Außerdem sollten die Nutzer jederzeit die Möglichkeit haben, ihre Einwilligung einfach und unaufwendig zu widerrufen. Eine betroffene Person kann ihre Einwilligung für die Datenverarbeitung auf verschiedenen Wegen und aus verschiedenen Gründen widerrufen. Die Option für den Widerruf der Einwilligung sollte vorzugsweise über die vorstehend genannten, leicht zugänglichen Mechanismen verfügbar sein. Es muss möglich sein, Apps zu deinstallieren und gleichzeitig sämtliche personenbezogenen Daten von den Servern des/der für die Verarbeitung Verantwortlichen zu entfernen. Um den Nutzern zu ermöglichen, ihre Daten durch den App-Entwickler löschen zu lassen, hat der Hersteller des Betriebssystems die wichtige Aufgabe, eine Meldung an den App-Entwickler zu senden, wenn ein Nutzer die App deinstalliert. Eine solche Meldung könnte über die Programmierschnittstelle erfolgen. Wenn ein Nutzer eine App deinstalliert hat, besitzt der Entwickler der betreffenden App grundsätzlich keine Rechtsgrundlage mehr

für die weitere Verarbeitung der diesen Nutzer betreffenden personenbezogenen Daten und muss entsprechend sämtliche Daten löschen. Ein App-Entwickler, der bestimmte Daten aufbewahren möchte (beispielsweise um eine erneute Installation der App zu vereinfachen), muss während der Deinstallation eine gesonderte Einwilligung einholen und den Nutzer ersuchen, einer festgelegten zusätzlichen Speicherfrist zuzustimmen. Die einzige Ausnahme von dieser Regel sind möglicherweise bestehende rechtliche Verpflichtungen zur Speicherung gewisser Daten für spezifische Zwecke (z. B. steuerrechtliche Verpflichtungen im Zusammenhang mit Finanztransaktionen).[46]

3.9 Speicherfristen

App-Entwickler müssen die Speicherung der mit einer App erfassten Daten und die damit verbundenen Datenschutzrisiken abwägen. Die spezifischen Zeitrahmen hängen vom Zweck der App und von der Relevanz der Daten für den Endnutzer ab. Eine Kalender- oder Tagebuch-App oder eine App zum Tauschen von Fotos würde beispielsweise die Wahl der Speicherfrist dem Endnutzer überlassen, während es für eine Navigations-App ausreichen kann, nur die letzten zehn besuchten Standorte zu speichern. App-Entwickler sollten auch Überlegungen zu den Daten von Nutzern anstellen, die die App längere Zeit nicht verwendet haben. Diese Nutzer könnten ihr mobiles Endgerät verloren haben oder zu einem anderen Endgerät gewechselt haben, ohne auf dem ursprünglichen Gerät alle Apps aktiv zu deinstallieren. App-Entwickler sollten daher im Voraus einen Zeitraum der Inaktivität festlegen, nach dessen Ablauf das Konto als erloschen behandelt wird, und sicherstellen, dass der Nutzer über diesen Zeitraum unterrichtet wird. Bei Ablauf dieses Zeitraums sollte der für die Verarbeitung Verantwortliche dem Nutzer einen Warnhinweis senden und ihm die Möglichkeit geben, personenbezogene Daten abzurufen. Wenn der Nutzer auf den Warnhinweis nicht reagiert, sollten die den Nutzer und die App-Nutzung betreffenden personenbezogenen Daten unwiderruflich anonymisiert oder gelöscht werden. Die Erinnerungsfrist hängt vom Zweck der App und dem Standort der gespeicherten Daten ab. Wenn Daten betroffen sind, die auf dem Gerät selbst gespeichert sind (z. B. die Höchstpunktzahl bei einem Spiel), können die Daten aufbewahrt werden, solange die App installiert ist. Wenn Daten betroffen sind, die nur einmal im Jahr verwendet werden (z. B. Informationen über ein Skigebiet), könnte die Erinnerungsfrist bei 15 Monaten liegen.

[46] Im Zusammenhang mit sämtlichen Diensten der Informationsgesellschaft (u. a. mit Apps) erinnert die Datenschutzgruppe daran, dass die europäische Verpflichtung zur Vorratsspeicherung von Daten (Richtlinie 2006/24/EG) für diese Dienste nicht gilt und daher nicht als Rechtsgrundlage für die fortgesetzte Verarbeitung von Daten über App-Nutzer herangezogen werden kann, nachdem diese Nutzer die App gelöscht haben. Die Datenschutzgruppe nutzt diese Gelegenheit, um zu betonen, dass Verkehrsdaten besonders risikobehaftet sind und als solche spezielle Vorsichts- und Sicherheitsmaßnahmen erfordern. Dies wurde bereits im Bericht der Datenschutzgruppe über die Durchsetzung der Richtlinie über die Vorratsspeicherung von Daten (WP172) unterstrichen, in dem alle relevanten Beteiligten a ufgefordert wurden, angemessene Sicherheitsmaßnahmen durchzuführen.

3.10 Kinder

Kinder sind begeisterte App-Nutzer, entweder auf eigenen oder auf gemeinsam genutzten Endgeräten (z. B. den Geräten ihrer Eltern oder Geschwister oder in Bildungseinrichtungen), und es gibt offensichtlich einen großen und vielseitigen Markt für Apps, die auf Kinder ausgerichtet sind. Gleichzeitig haben Kinder jedoch nur ein geringes oder keinerlei Verständnis und Wissen in Bezug auf den Umfang und die Sensibilität der Daten, auf die Apps zugreifen können, oder den Umfang der Weitergabe von Daten an Dritte zu Werbezwecken.

Die Datenschutzgruppe hat die Thematik der Verarbeitung von Daten von Kindern in der Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern behandelt und geht in diesem Abschnitt nur auf einige appspezifische Risiken und Empfehlungen ein.[47]

App-Entwickler und andere für die Verarbeitung Verantwortliche sollten die Altersgrenzen für die Definition von Kindern und Minderjährigen in den nationalen Rechtsvorschriften beachten, bei denen die Einwilligung der Eltern für die Datenverarbeitung eine Voraussetzung für die rechtmäßige Datenverarbeitung durch Apps ist.[48]

Wenn die Einwilligung rechtmäßig von einem Minderjährigen eingeholt werden kann und die App für die Nutzung durch ein Kind oder einen Minderjährigen bestimmt ist, sollte der für die Verarbeitung Verantwortliche beachten, dass ein Minderjähriger die Bedeutung der Datenverarbeitung vielleicht nur eingeschränkt erfasst und nur in beschränktem Umfang entsprechend sensibilisiert ist. Aufgrund der allgemeinen Schutzbedürftigkeit von Kindern und unter Berücksichtigung der Tatsache, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen, sollten für die Verarbeitung Verantwortliche, die Kinder als Zielgruppe ansprechen, die Grundsätze der Datenminimierung und der Zweckbindung besonders strikt beachten. Konkret sollten für die Verarbeitung Verantwortliche Daten von Kindern weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeiten, da dies über das Verständnis eines Kindes hinausgehen und damit die Grenzen der rechtmäßigen Verarbeitung überschreiten würde.

Die Datenschutzgruppe teilt die Bedenken, die die FTC in ihrem Bericht über mobile Apps für Kinder zum Ausdruck gebracht hat.[49]

---

[47] Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) (WP 160, 11. Februar 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_de.pdf.

[48] In den EU-Mitgliedstaaten liegt diese Altergrenze zwischen 12 und 18 Jahren.

[49] FTC-Bericht *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Februar 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf: *„Die FTC hat ein vielseitiges Spektrum von Apps für Kinder ermittelt, die von Hunderten verschiedener Entwickler erstellt wurden. Auf den App-Vertriebsplattformen hat sie Informationen über die Praktiken zur Verarbeitung und Weitergabe von Daten durch diese Apps jedoch allenfalls in geringem Umfang gefunden."*

App-Entwickler sollten in Zusammenarbeit mit App-Stores und Herstellern von Betriebssystemen und Endgeräten die relevanten Informationen auf einfache Weise und in altersgerechter Sprache bereitstellen. Die für die Verarbeitung Verantwortlichen sollten konkret auch jegliche Erfassung von Daten unterlassen, die die Eltern oder Familienmitglieder des minderjährigen Nutzers betreffen, zum Beispiel Finanzinformationen oder Informationen zu speziellen Datenkategorien (etwa medizinische Daten).

4 Schlussfolgerungen und Empfehlungen

Zahlreiche auf einem intelligenten mobilen Endgerät verfügbare Daten sind personenbezogene Daten. Der geltende Rechtsrahmen in diesem Bereich besteht in der Datenschutzrichtlinie in Verbindung mit der spezifischen Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation. Diese Vorschriften gelten unabhängig vom Standort des App-Entwicklers oder des App-Store für jede App, die an App-Nutzer in der EU vertrieben wird.

Die Fragmentierung des App-Ökosystems, das breite Spektrum technischer Möglichkeiten für den Zugriff auf Daten, die auf mobilen Endgeräten gespeichert sind oder von diesen erstellt werden, und die mangelnde Kenntnis der einschlägigen Rechtsvorschriften unter den Entwicklern führen zu einer Reihe ernsthafter Datenschutzrisiken für App-Nutzer. Diese Risiken reichen von einer mangelnden Transparenz und einem fehlenden Problembewusstsein der App-Nutzer bis hin zu unzureichenden Sicherheitsmaßnahmen, ungültigen Einwilligungsmechanismen, der Tendenz zur Datenmaximierung und einer ungenauen Festlegung der Verarbeitungszwecke.

Zwischen den Datenschutzverpflichtungen der verschiedenen an der Entwicklung, der Verbreitung und der Konzeption der technischen Möglichkeiten von Apps beteiligten Parteien bestehen Überschneidungen. Die meisten Schlussfolgerungen und Empfehlungen sind an App-Entwickler gerichtet (da die Entwickler am stärksten Einfluss darauf haben, wie die Verarbeitung erfolgt und wie Informationen in einer App dargestellt werden). Um die höchsten Standards für den Datenschutz und den Schutz der Privatsphäre zu erreichen, müssen die App-Entwickler jedoch häufig mit anderen Akteuren im App-Ökosystem zusammenarbeiten, z. B. mit den Herstellern von Betriebssystemen und Endgeräten, den App-Stores und Dritten wie z. B. Analysedienstleistern und Online-Werbenetzen.

App-Entwickler müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung der Daten von Nutzern und über Nutzer kennen und erfüllen;
- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Vertragsschließung mit Auftragsverarbeitern kennen und erfüllen (beispielsweise

wenn sie die Erfassung und Verarbeitung personenbezogener Daten extern an Entwickler, Programmierer oder beispielsweise Cloud-Speicheranbieter vergeben);
- eine Einwilligung einholen, bevor die App beginnt, Informationen vom Endgerät zu lesen oder auf dem Gerät zu speichern (d. h. vor Installation der App). Eine solche Einwilligung muss ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erteilt werden;
- eine differenzierte Einwilligung für jede Datenart einholen, auf die die App zugreift – zumindest für die Kategorien Standort, Kontakte, eindeutige Gerätekennung, Identität der betroffenen Person, Identität des Telefons, Kreditkarten- und Zahlungsdaten, Telefonie und SMS, Browserverlauf, E-Mail, Authentifizierungsdaten für soziale Netzwerke und biometrische Daten;
- sich bewusst sein, dass eine Einwilligung keine übermäßige oder unverhältnismäßige Datenverarbeitung legitimiert;
- vor der Installation der App genau festgelegte und verständlich formulierte Zwecke für die Datenverarbeitung bereitstellen und dürfen diese Zwecke nicht ohne eine erneute Einwilligung ändern; sie umfassende Informationen bereitstellen, wenn die Daten für die Zwecke Dritter, z. B. Werbung oder Analyse, verwendet werden;
- den Nutzern ermöglichen, ihre Einwilligung zu widerrufen und die App zu deinstallieren und gegebenenfalls Daten löschen;
- den Grundsatz der Datenminimierung beachten, d. h., sie dürfen nur die Daten erfassen, die für die Durchführung der gewünschten Funktion unbedingt erforderlich sind;
- in allen Phasen der Konzeption und der Implementierung der App die erforderlichen organisatorischen und technischen Maßnahmen ergreifen, um den Schutz der von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten (siehe Abschnitt 3.6 dieser Stellungnahme (Privacy by Design));
- einen einzigen Ansprechpartner für die App-Nutzer benennen;
- eine lesbare, verständliche und leicht zugängliche Datenschutzerklärung bereitstellen, die die Nutzer zumindest darüber informiert,
  - wer sie sind (Identität und Kontaktdaten),
  - welche genauen Kategorien personenbezogener Daten die App erfassen und verarbeiten soll,
  - warum diese Verarbeitung erforderlich ist (genaue Zwecke),
  - ob die Daten an Dritte weitergegeben werden (nicht nur eine allgemeine Erklärung, sondern eine spezifische Beschreibung, an wen die Daten weitergegeben werden),
  - welche Rechte die Nutzer in Bezug auf den Widerruf der Einwilligung und die Löschung von Daten haben;
- den Nutzern ermöglichen, ihre Rechte auf Auskunft, Berichtigung und Löschung sowie das Recht auf Widerspruch gegen die Datenverarbeitung auszuüben, und die Nutzer über die entsprechenden Mechanismen informieren;

- eine angemessene Speicherfrist für die mit der App erfassten Daten festlegen und von vornherein einen Zeitraum der Inaktivität festlegen, nach dessen Ablauf das Konto als erloschen behandelt wird;
- in Bezug auf für Kinder bestimmte Apps die Altersgrenzen für die Definition von Kindern und Minderjährigen in den jeweils geltenden nationalen Rechtsvorschriften beachten; sie müssen unter strikter Beachtung der Grundsätze der Datenminimierung und der Zweckbindung den am stärksten eingeschränkten Ansatz für die Datenverarbeitung wählen. Die Daten von Kindern dürfen sie weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeiten; außerdem dürfen sie über die Kinder keine Daten über deren Verwandten und/oder Freunde erfassen.

Die Datenschutzgruppe empfiehlt, dass App-Entwickler

- die einschlägigen Leitlinien in Bezug auf spezifische Sicherheitsrisiken und -maßnahmen sorgfältig prüfen;
- die Nutzer gemäß den Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation proaktiv über Verletzungen des Schutzes personenbezogener Daten informieren;
- die Nutzer über ihre Überlegungen hinsichtlich der Verhältnismäßigkeit der Daten, die auf dem betreffenden Gerät erfasst werden oder auf die zugegriffen wird, sowie über die Speicherfristen für die Daten und die durchgeführten Sicherheitsmaßnahmen unterrichten;
- Werkzeuge entwickeln, mit denen die Nutzer die Speicherfristen für ihre personenbezogenen Daten anhand ihrer spezifischen Präferenzen und Umstände anpassen können, anstatt vordefinierte Speicherfristen vorzugeben;
- in ihren für europäische Nutzer bestimmten Datenschutzerklärungen relevante Informationen angeben;
- einfache, aber sichere Online-Auskunftswerkzeuge ohne eine zusätzliche übermäßige Erfassung personenbezogener Daten konzipieren und implementieren;
- gemeinsam mit den Herstellern von Betriebssystemen und Endgeräten ihre Kreativität für die Bereitstellung innovativer Lösungen für die angemessene Unterrichtung von Nutzern mobiler Endgeräte nutzen, beispielsweise durch ein System von Mehrebenen-Informationshinweisen kombiniert mit aussagekräftigen Symbolen.

App-Stores müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung der Daten von Nutzern und über Nutzer kennen und erfüllen;
- die Informationspflichten der App-Entwickler durchsetzen (u. a. die Unterrichtung der Nutzer über die Arten von Daten, auf die die App zugreifen kann, über die Zwecke dieses Datenzugriffs und darüber, ob die Daten an Dritte weitergegeben werden);

- besondere Aufmerksamkeit auf Apps für Kinder verwenden, um eine unrechtmäßige Verarbeitung der Daten von Kindern zu verhindern, und insbesondere die Verpflichtung durchsetzen, die relevanten Informationen auf einfache Weise und in altersgerechter Sprache bereitzustellen;
- ausführliche Informationen über die tatsächlich durchgeführten Kontrollen neu aufgenommener Apps bereitstellen, einschließlich der Kontrollen zur Bewertung in Bezug auf den Datenschutz und den Schutz der Privatsphäre.

Die Datenschutzgruppe empfiehlt, dass App-Stores

- in Zusammenarbeit mit den Herstellern von Betriebssystemen für die Nutzer Instrumente zur Kontrolle ihrer Daten entwickeln, zum Beispiel Symbole zur Darstellung des Zugriffs auf Daten, die sich auf dem mobilen Endgerät befinden oder vom Gerät erstellt werden;
- die Bewertung aller Apps in einem öffentlichen Reputationsmechanismus ermöglichen;
- einen datenschutzfreundlichen Mechanismus für eine Fern-Deinstallation einführen;
- den Nutzern Möglichkeiten für die Äußerung von Rückmeldungen bereitstellen, damit diese Datenschutz- und/oder Sicherheitsprobleme melden können;
- in Zusammenarbeit mit den App-Entwicklern die Nutzer proaktiv über Verletzungen des Schutzes personenbezogener Daten informieren;
- die App-Entwickler auf die Besonderheiten des europäischen Rechts hinweisen, bevor eine App in Europa angeboten wird, zum Beispiel auf die Einwilligungsanforderung und gegebenenfalls auf die Regelung der Übermittlung personenbezogener Daten in Nicht-EU-Länder.

Hersteller von Betriebssystemen und Endgeräten müssen

- ihre Programmierschnittstellen, Regeln für App-Stores und Benutzeroberflächen aktualisieren, um den Nutzern eine ausreichende Kontrolle zu ermöglichen, damit diese eine gültige Einwilligung für die von Apps verarbeiteten Daten erteilen können;
- in ihren Betriebssystemen Mechanismen für die Einholung einer Einwilligung beim ersten Start der App oder beim ersten Zugriff der App auf eine der Datenkategorien mit wesentlichen Datenschutzauswirkungen implementieren;
- die Grundsätze des eingebauten Datenschutzes (Privacy by Design) beachten, um eine heimliche Überwachung der Nutzer zu verhindern;
- eine sichere Datenverarbeitung gewährleisten;
- sicherstellen, dass vorinstallierte Apps bzw. deren Standardeinstellungen dem europäischen Datenschutzrecht entsprechen;
- einen differenzierten Zugriff auf Daten, Sensoren und Dienstleistungen ermöglichen, um sicherzustellen, dass die App-Entwickler nur auf die Daten zugreifen können, die für ihre Apps tatsächlich erforderlich sind;

- anwenderfreundliche und wirksame Mittel bereitstellen, mit denen die Nutzer ein Tracking durch Werbetreibende oder sonstige Dritte verhindern können. Die Standardeinstellungen müssen jegliches Tracking ausschließen;
- die Verfügbarkeit angemessener Mechanismen zur Aufklärung der Endnutzer darüber gewährleisten, was Apps tun können und auf welche Daten sie Zugriff haben;
- sicherstellen, dass bei der Unterrichtung der Endnutzer vor der Installation der App alle Datenkategorien, auf die zugegriffen wird, klar und verständlich genannt werden;
- eine sicherheitsfördernde Umgebung einführen und Hilfsmittel verwenden, die eine Verbreitung bösartiger Apps verhindern und eine einfache Installation/Deinstallation einzelner Funktionen ermöglichen.

Die Datenschutzgruppe empfiehlt, dass die Hersteller von Betriebssystemen und Endgeräten

- den Nutzern ermöglichen, Apps zu deinstallieren, und eine Meldung an den App-Entwickler senden (z. B. über die Programmierschnittstelle), um die Löschung der entsprechenden Nutzerdaten zu ermöglichen;
- systematisch regelmäßige Sicherheitsaktualisierungen anbieten und die Nutzer bei ihrer Anwendung unterstützen;
- sicherstellen, dass die Methoden und Funktionen für den Zugriff auf personenbezogene Daten Funktionen beinhalten, die auf die Implementierung differenzierter Einwilligungsanfragen abzielen;
- aktiv zur Entwicklung von Symbolen beitragen, mit denen die Nutzer auf die verschiedenen Datenverwendungen durch Apps hingewiesen werden, und die Einführung dieser Symbole unterstützen;
- klare Prüfpfade für die Geräte entwickeln, damit die Endnutzer klar sehen können, welche Apps auf Daten auf ihren Geräten zugegriffen haben, und damit die Endnutzer Informationen über die ausgehende Datenverkehrsmenge pro App im Verhältnis zum nutzerinitiierten Datenverkehr erhalten können.

Dritte müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten über Nutzer kennen und erfüllen;
- in Zusammenarbeit mit den App-Entwicklern und/oder App-Stores beim Lesen oder Schreiben von Daten auf mobilen Endgeräten die in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vorgeschriebene Einwilligungsanforderung erfüllen; App-Entwickler und/oder App-Stores haben dabei die wichtige Aufgabe, die Nutzer über die Zwecke der Datenverarbeitung zu informieren;
- dafür sorgen, dass keine Mechanismen zur Verhinderung von Tracking umgangen werden (wie derzeit häufig bei in Browsern implementierten „Do Not Track"-Mechanismen der Fall);

- soweit sie als Kommunikationsdienstleister Markengeräte verbreiten, eine gültige Einwilligung der Nutzer für vorinstallierte Apps sicherstellen und die entsprechende Verantwortung übernehmen, wenn sie an der Festlegung bestimmter Funktionen des Endgeräts und des Betriebssystems beteiligt sind; dazu können sie beispielsweise den Zugriff der Nutzer auf bestimmte Konfigurationsparameter beschränken oder (sicherheits- und funktionsbezogene) Aktualisierungen der Hersteller der Endgeräte oder der Betriebssysteme filtern;
- soweit sie als Werbetreibende tätig sind, ausdrücklich davon absehen, Werbung außerhalb der App einzublenden. Beispiele sind die Einblendung von Werbung durch Modifizierung der Browsereinstellungen oder die Platzierung von Symbolen auf dem Desktop des mobilen Endgeräts. Sie dürfen eindeutige Geräte- oder Teilnehmerkennungen nicht zum Zwecke des Tracking verwenden;
- dafür sorgen, dass die Daten von Kindern weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeitet werden. Sie müssen angemessene Sicherheitsmaßnahmen durchführen. Dazu gehören die sichere Übertragung und die verschlüsselte Speicherung von eindeutigen Gerätekennungen und Kennungen der App-Nutzer sowie sonstigen personenbezogenen Daten.

Die Datenschutzgruppe empfiehlt, dass Dritte

- einfache, aber sichere Online-Auskunftswerkzeuge ohne eine zusätzliche übermäßige Erfassung personenbezogener Daten konzipieren und implementieren und
- nur die Daten erfassen und verarbeiten, die sich tatsächlich auf den Kontext beziehen, in dem die Nutzer diese Daten bereitstellen.

Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsdatenverarbeiter (WP 204)

Angenommen am 19. April 2013

Inhaltsverzeichnis

DIE DATENSCHUTZGRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

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

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

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

hat folgendes Arbeitsdokument angenommen:

1. Hintergrund

1.1. Vorschriften der Europäischen Union für den internationalen Datentransfer

In der Richtlinie ist festgelegt, dass die Übermittlung von Daten in Drittländer nach strengen Regeln erfolgen muss, um sicherzustellen, dass für die betroffenen Personen auch bei der Übermittlung ihrer Daten in Länder außerhalb der Europäischen Union (im Folgenden „EU") ein angemessenes Schutzniveau gewährleistet ist.

Gemäß Artikel 26 Absatz 2 der Richtlinie *„[…] kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau […] gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes […] der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben."*

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

Folglich sind von dem für die Verarbeitung Verantwortlichen ausreichende Garantien für die übermittelten Daten – beispielsweise durch die Annahme von Vertragsklauseln – abzugeben, wenn das Land des Datenimporteurs kein angemessenes Schutzniveau gewährleistet.

Auf dieser Grundlage und mit dem Ziel, die Einhaltung der Richtlinie 95/46/EG bei der Übermittlung von Daten in Länder außerhalb der EU zu fördern, hat die Europäische Kommission Standardvertragsklauseln angenommen, mit denen Übermittlungen zwischen den für die Verarbeitung Verantwortlichen – Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 und Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 – sowie zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern – Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 – geregelt werden sollen.

1.2. Verbindliche unternehmensinterne Datenschutzregelungen für die für die Verarbeitung Verantwortlichen

Nach Auffassung der Artikel-29-Datenschutzgruppe sollten Unternehmen angesichts der Notwendigkeit einheitlicher Datenschutzregelungen die Möglichkeit erhalten, verpflichtende interne Vorschriften, die so genannten verbindlichen unternehmensinternen Datenschutzregelungen (im Folgenden „BCR“ – Binding Corporate Rules), anzunehmen, in denen Vorgaben für die Übermittlung personenbezogener Daten festgelegt werden, die ursprünglich von dem Unternehmen in seiner Funktion als dem für die Verarbeitung Verantwortlichen innerhalb des betreffenden Unternehmens verarbeitet wurden. Die Datenschutzbehörden der EU haben Leitlinien entwickelt, in denen festgelegt ist, was in den BCR[2] geregelt werden soll.

Außerdem ist zu berücksichtigen, dass Standardvertragsklauseln lediglich einen pauschalen Lösungsansatz bieten, die jeweiligen BCR jedoch individuell auf die besonderen Bedürfnisse des betreffenden Unternehmens zugeschnitten werden müssen. Während Standardvertragsklauseln in der Regel ohne bestimmte Vorgaben für die Umsetzung festgelegt werden, wird bei BCR vorausgesetzt, dass das Unternehmen innerhalb der Unternehmensgruppe bereits über ausreichende und wirksame Datenschutzregelungen verfügt oder dass es die notwendigen Maßnahmen einführt, um zu gewährleisten, dass die vorhandenen Systeme die BCR-Anforderungen erfüllen.

Seit einigen Jahren werden die BCR für die für die Verarbeitung Verantwortlichen mit zunehmendem Erfolg eingesetzt. Das Annahmeverfahren konnte nicht nur dank der größeren Erfahrung von Datenschutzbehörden und Unternehmen, son-

[2] Siehe Arbeitsdokumente WP 153, WP 154 und WP 155, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_de.htm.

dern auch durch das Verfahren der gegenseitigen Anerkennung erheblich verkürzt werden. Außerdem wird von multinationalen Unternehmen immer wieder betont, dass die BCR gut zu der pragmatischen Vorgehensweise passen, die sie bei der Einhaltung von Vorschriften verfolgen. Unterstützt werden die BCR auch von der Europäischen Kommission, die diese in ihren am 25. Januar 2012 veröffentlichten Vorschlag für die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[3] aufgenommen hat.

1.3. Verbindliche unternehmensinterne Datenschutzregelungen für Auftragsverarbeiter

Um der Ausweitung von Datenverarbeitungstätigkeiten – insbesondere dem Entstehen neuer Geschäftsmodelle für die internationale Verarbeitung personenbezogener Daten – Rechnung zu tragen, nahm die Europäische Kommission im Jahr 2010 eine Reihe neuer Standardvertragsklauseln für die Übermittlung von Daten zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern an. Die im Jahr 2010 festgelegten Standardvertragsklauseln enthalten besondere Bestimmungen, wonach unter bestimmten Bedingungen sowie unter der Voraussetzung, dass ausreichende Garantien für die übermittelten personenbezogenen Daten geboten werden, die Auslagerung von Verarbeitungstätigkeiten an Unterauftragsverarbeiter zulässig ist.

Die Aufgabe, mithilfe der oben beschriebenen vorhandenen Instrumente zur Regelung internationaler Datenübermittlungen kontinuierlich ein angemessenes Schutzniveau zu gewährleisten, erweist sich insbesondere angesichts der wachsenden Zahl und Komplexität internationaler Datentransfers (bedingt z. B. durch Cloud-Computing, Globalisierung, Datenzentren, soziale Netzwerke usw.) als schwierig.

Zwar stellen die Standardvertragsklauseln allem Anschein nach ein wirksames Instrument für die Übermittlung überschaubarer Datenmengen von in der EU ansässigen Datenexporteuren an Datenimporteure in Ländern außerhalb der EU dar, doch fordert die Outsourcing-Industrie seit langem ein neues Rechtsinstrument, mit dem ein einheitlicher Rahmen für den Datenschutz in diesem Wirtschaftszweig geschaffen wird und etwaige bereits eingeführte unternehmensinterne Regelungen offiziell anerkannt werden. Mit einem solchen neuen Rechtsinstrument könnten größere Datenübermittlungen von Auftragsverarbeitern an Unterauftragsverarbeiter, die Teil desselben Unternehmens sind und im Auftrag und auf Anweisung des für die Verarbeitung Verantwortlichen handeln, wirksam geregelt werden. Angesichts des wachsenden Interesses der Industrie an einem solchen

[3] Siehe Artikel 42 des Vorschlags für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

Instrument wurden von der Datenschutzgruppe im Jahr 2012 ein Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter[4] sowie ein Antragsformular für die Vorlage verbindlicher unternehmensinterner Datenschutzregelungen für Auftragsverarbeiter[5] angenommen. Die Einführung verbindlicher unternehmensinterner Datenschutzregelungen für Auftragsverarbeiter wurde von der Datenschutzgruppe am 5. Dezember 2012[6] bestätigt.

2. Definition und Rechtsfragen

2.1. Anwendungsbereich dieses Instruments und Definitionen

Die BCR für Auftragsverarbeiter sollen als unterstützendes Instrument zur Regelung internationaler Übermittlungen personenbezogener Daten dienen, die ursprünglich von einem Auftragsverarbeiter im Auftrag und nach den Anweisungen[7] eines für die Verarbeitung Verantwortlichen in der EU verarbeitet wurden und im Unternehmen des Auftragsverarbeiters unterverarbeitet werden.

Daher sind die BCR für Auftragsverarbeiter als Anhang dem zwischen dem externen für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter geschlossenen Vertrag über die Auftragsverarbeitung (in diesem Arbeitsdokument als Dienstgütevereinbarung bezeichnet) beizufügen, der nach Artikel 17 der EU-Richtlinie 95/46/EG vorgeschrieben ist und insbesondere die Anweisungen des für die Verarbeitung Verantwortlichen enthält. Die BCR für Auftragsverarbeiter sind als ausreichende Garantien des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen (Artikel 26 Absatz 2 der EU-Richtlinie 95/46/EG) anzusehen, die dem für die Verarbeitung Verantwortlichen die Einhaltung der EU-Datenschutzvorschriften ermöglichen. Unternehmen aus der Unternehmensgruppe des Auftragsverarbeiters müssen sich zur Einhaltung der Grundsätze, die in den BCR für Auftragsverarbeiter festgelegt sind, verpflichten und sind bei Verstößen gegen die BCR für Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen haftbar.

---

[4] Siehe WP 195, angenommen am 6. Juni 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_de.pdf.

[5] Siehe Antrag auf Genehmigung verbindlicher unternehmensinterner Datenschutzregelungen für die Übermittlung personenbezogener Daten für Datenverarbeitungstätigkeiten, angenommen am 17. September 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_application_form_en.doc.

[6] Siehe Pressemitteilung vom 21. Dezember 2012, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf.

[7] Ein für die Verarbeitung verantwortlicher Dritter beauftragt ein Auslagerungsunternehmen, das internationale Übermittlungen dieser Daten an Unternehmen seiner Unternehmensgruppe vornimmt, welche eine Unterverarbeitung durchführen.

An dieser Stelle ist jedoch der Hinweis wichtig, dass der für die Verarbeitung Verantwortliche – ungeachtet der Tatsache, dass die EU-Datenschutzbehörden den Inhalt der BCR für die Auftragsverarbeiter einer Unternehmensgruppe beurteilen, um die Einhaltung aller im Arbeitsdokument WP 195 festgelegten Anforderungen sicherzustellen – verpflichtet ist, ausreichende Garantien für die Daten zu bieten, die in seinem Auftrag und nach seinen Anweisungen in den Unternehmen der Unternehmensgruppe des Auftragsverarbeiters übermittelt und verarbeitet werden.

Die Datenschutzgruppe weist darauf hin, dass das Ziel der BCR für Auftragsverarbeiter nicht darin besteht, die Pflichten der für die Verarbeitung Verantwortlichen auf die Auftragsverarbeiter zu verlagern. Die Pflichten der Auftragsverarbeiter und der für die Verarbeitung Verantwortlichen im Zusammenhang mit der Datenübermittlung ins Ausland bleiben bestehen (wie im Beschluss 2010/87/EU der Kommission über Standardvertragsklauseln festgelegt), allerdings müssen einige Instrumente im Hinblick auf die Besonderheiten von Übermittlungen innerhalb einer Unternehmensgruppe (eine für alle Mitglieder der Gruppe geltende Verpflichtung anstelle mehrerer Verträge) sowie im Hinblick auf die Besonderheiten der BCR (Instrumente für die Rechenschaftspflicht, wie Audits, Schulungsprogramme, Datenschutzbeauftragte usw.) angepasst werden.

Durch die BCR für Auftragsverarbeiter sollen ferner die Rechte der betroffenen Personen gestärkt werden, indem ausdrücklich festgelegt wird, dass Auftragsverarbeiter verpflichtet sind, den für die Verarbeitung Verantwortlichen die relevanten Informationen vorzulegen, die diese zur Einhaltung ihrer Verpflichtungen gegenüber den betroffenen Personen benötigen. Offenkundig bieten die BCR für Auftragsverarbeiter eine zusätzliche Gewähr dafür, dass die Auftragsverarbeiter sich dazu verpflichten, den für die Verarbeitung Verantwortlichen die maßgeblichen Informationen vorzulegen.

Während der Auftragsverarbeiter entsprechend den im Arbeitsdokument WP 107[8] festgelegten gegenseitigen Anerkennungs- und Kooperationsverfahren einen Antrag stellen muss, damit seine BCR für Auftragsverarbeiter in der EU als angemessene Garantien für internationale Datenübermittlungen anerkannt werden, sind die für die Verarbeitung Verantwortlichen nach wie vor gehalten, auf der Grundlage der BCR für Auftragsverarbeiter, die Bestandteil der von den für die Verarbeitung Verantwortlichen geleisteten Garantien sind, bei den zuständigen Datenschutzbehörden die Genehmigung von Datenübermittlungen an die verschiedenen Unternehmen ihrer Dienstleistungsanbieter (Auftragsverarbeiter, Unterauftragsverarbeiter, Datenzentren usw.) zu beantragen.

[8] Siehe Arbeitsdokument WP 107, angenommen am 14. April 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_de.pdf.

2.2. Datenübermittlung und Weiterübermittlung

2.2.1. Datenübermittlungen innerhalb der Unternehmensgruppe des Auftragsverarbeiters

Da nach den Vorgaben des Arbeitsdokuments WP 195 Daten nur dann von anderen Mitgliedern der Unternehmensgruppe des Auftragsverarbeiters unterverarbeitet werden können, wenn der für die für die Verarbeitung Verantwortliche zuvor hierüber unterrichtet wurde[9] und vorab seine schriftliche Einwilligung erteilt hat, sorgen die BCR für Auftragsverarbeiter für Transparenz gegenüber dem für die Verarbeitung Verantwortlichen und gewährleisten, dass dieser die Kontrolle über die Daten behält, die von Unternehmen der Unternehmensgruppe des Auftragsverarbeiters in seinem Auftrag und nach seinen Anweisungen verarbeitet werden.

Die Parteien der Dienstevereinbarung können je nach ihren spezifischen Anforderungen selbst entscheiden, ob eine generelle vorherige Einwilligung des für die Verarbeitung Verantwortlichen, die zu Beginn der Erbringung des Dienstes erteilt wird, ausreicht oder ob für jede neue Unterverarbeitung eine erneute Einwilligung erforderlich ist. Wird eine generelle Einwilligung erteilt, so sollte der für die Verarbeitung Verantwortliche über alle beabsichtigten Änderungen, die die Hinzuziehung weiterer Unterauftragnehmer oder den Ersatz von Unterauftragnehmern betreffen, so rechtzeitig unterrichtet werden, dass er in der Lage ist, Einwendungen gegen die Änderung zu erheben oder vom Vertrag zurückzutreten, bevor die Daten an den neuen Unterauftragsverarbeiter weitergeleitet werden.

Das Unternehmen eines Auftragsverarbeiters, das BCR für Auftragsverarbeiter eingeführt hat, ist nicht verpflichtet, mit allen Unterauftragsverarbeitern im eigenen Unternehmen Verträge zur Regelung von Datenübermittlungen zu schließen, da die BCR für Auftragsverarbeiter Garantien für Daten bieten, die im Auftrag und nach Anweisung des für die Verarbeitung Verantwortlichen übermittelt und verarbeitet werden.

2.2.2. Weiterübermittlung an externe Unterauftragsverarbeiter

Neben den oben genannten Regelungen für Übermittlungen innerhalb der Unternehmensgruppe des Auftragsverarbeiters (Transparenz, Einwilligung des für die Verarbeitung Verantwortlichen) kann ein Mitglied der Unternehmensgruppe des Auftragsverarbeiters seine Pflichten gemäß der Dienstevereinbarung (Artikel 17 der Richtlinie) an einen externen Unterauftragsverarbeiter (außerhalb der Unternehmensgruppe) nur im Wege einer schriftlichen Vereinbarung mit dem externen

[9] Angaben zu den Hauptbestandteilen (Beteiligte, Länder, Sicherheit, Garantien im Falle der Datenübermittlung ins Ausland sowie die Möglichkeit, eine Kopie des angewandten Vertrags zu erhalten). Ausführliche Angaben, z. B. die Namen der Unterauftragsverarbeiter, könnten beispielsweise in einem öffentlichen digitalen Verzeichnis zugänglich gemacht werden.

Unterauftragsverarbeiter übertragen, die einerseits die Gewähr dafür bietet, dass ein ausreichender Schutz im Einklang mit den Artikeln 16 und 17 der Richtlinie 95/46/EG gewährleistet ist, und andererseits dem externen Unterauftragsverarbeiter die gleichen Pflichten auferlegt, die auch das Mitglied der Unternehmensgruppe des Auftragsverarbeiters nach der Dienstevereinbarung und den Abschnitten 1.3, 1.4, 3 und 6 des Arbeitsdokuments WP 195[10] erfüllen muss. Sofern die BCR für Auftragsverarbeiter nicht für Datenübermittlungen an externe Unterauftragsverarbeiter (außerhalb der Unternehmensgruppe) gelten, ist außerdem ein angemessener Schutz solcher Datenübermittlungen im Einklang mit den Artikeln 25 und 26 der Richtlinie 95/46/EG zu gewährleisten.

2.3. Überlegungen zur Verbindlichkeit der BCR für Auftragsverarbeiter

Auftragsverarbeiter tragen den Erfordernissen ihrer Datenverarbeitungstätigkeiten auf der Grundlage unterschiedlicher rechtlicher und kultureller Hintergründe und unterschiedlicher Geschäftsphilosophien und -praktiken Rechnung. Die Erfahrung mit den BCR für die für die Verarbeitung Verantwortlichen verdeutlicht, dass fast alle multinationalen Unternehmen dieses Problem unterschiedlich angehen. Neben anderen Aspekten gibt es jedoch ein wichtiges Merkmal, das alle Systeme aufweisen müssen, wenn sie als Garantie für die Übermittlung von Daten für Datenverarbeitungstätigkeiten in Drittländer angeführt werden sollen: die Verbindlichkeit der unternehmensinternen Vorschriften für Auftragsverarbeiter, sowohl im Innenverhältnis als auch im Außenverhältnis (rechtliche Durchsetzbarkeit der Vorschriften).

2.3.1. Verbindlichkeit unternehmensinterner Datenschutzregelungen für Auftragsverarbeiter innerhalb des Unternehmens[11]

Hier ist zu unterscheiden zwischen dem Problem der Einhaltung der Vorschriften einerseits und dem Problem ihrer rechtlichen Durchsetzbarkeit andererseits.

Die Bewertung der „Verbindlichkeit“ unternehmensinterner Datenschutzregelungen für Auftragsverarbeiter setzt eine Bewertung ihrer externen und ihrer internen rechtlichen Verbindlichkeit voraus.

Die interne Verbindlichkeit der Vorschriften bedeutet in diesem Zusammenhang, dass die Mitglieder des Unternehmens des Auftragsverarbeiters und alle Mitarbeiter des Unternehmens gezwungen sind, die unternehmensinternen Datenschutzregelungen einzuhalten. Zu den Elementen derartiger Regelungen können unter anderem Disziplinarmaßnahmen bei Verstößen gegen die Vorschriften zählen,

[10] Op. cit., Ziff. 6.

[11] Die Annahme eines Verhaltenskodex ist ein Schritt, den Unternehmen nicht unbedacht vornehmen, weil sie erhebliche Risiken birgt und für Unternehmen, die gegen ihren eigenen Kodex verstoßen, sogar rechtliche Folgen haben kann.

ferner die individuelle und wirksame Information der Mitarbeiter oder die Aufstellung spezieller Schulungsprogramme für Mitarbeiter und Unterauftragnehmer usw. All diese Elemente, auf die auch in Abschnitt 4 eingegangen wird, könnten mit dazu beitragen, dass sich die Personen im Unternehmen des Auftragsverarbeiters zur Einhaltung dieser Vorschriften verpflichtet fühlen.

Was die Mitglieder der Unternehmensgruppe des Auftragsverarbeiters angeht, ist es nicht Sache der Datenschutzgruppe, vorzuschreiben, auf welche Weise die Unternehmen garantieren, dass alle Unternehmensteile wirksam an die Vorschriften gebunden werden oder sich ihnen verpflichtet fühlen; bestimmte Beispiele sind jedoch weithin bekannt, z. B. interne Verhaltenskodizes, die zusätzlich durch unternehmensinterne Vereinbarungen[12] gestützt werden. Die Unternehmen müssen sich jedoch bewusst sein, dass diejenigen, die die Genehmigung ihrer BCR für Datenverarbeiter als angemessene Garantien des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen (Artikel 26 Absatz 2 der EU-Richtlinie 95/46/EG) beantragen, gegenüber den Datenschutzbehörden nachweisen müssen, dass diese BCR für Auftragsverarbeiter in der gesamten Unternehmensgruppe bindend sind.

Die unternehmensinterne Verbindlichkeit der Datenschutzregelungen muss klar und so beschaffen sein, dass dadurch die Einhaltung der Vorschriften außerhalb der EU garantiert werden kann, üblicherweise unter der Verantwortung der EU-Hauptniederlassung, des in der EU für den Datenschutz zuständigen Unternehmensteils oder des Auftragsverarbeiters des EU-Datenexporteurs, die die erforderlichen Maßnahmen treffen müssen, um zu garantieren, dass alle Unternehmensteile ihre Unterverarbeitungstätigkeiten an die Vorschriften in den BCR anpassen.[13]

Es gibt in der Praxis fast immer ein in der EU ansässiges Mitglied der Unternehmensgruppe, das ausreichende Garantien bietet und den Antrag für die BCR des Auftragsverarbeiters bei der federführenden Datenschutzbehörde stellt. Befindet sich die Hauptniederlassung des Unternehmens nicht in der EU, sollte sie diese Zuständigkeiten an einen in der EU ansässigen Unternehmensteil, sofern vorhanden, delegieren. Es ist zweckmäßig, dass derjenige, der die Garantien tatsächlich übernimmt, für die wirksame Einhaltung der Vorschriften und die Durchsetzung der Garantien verantwortlich bleibt. Es kann jedoch auch eine andere Regelung anerkannt werden, bei der die Verantwortung zum Beispiel beim Auftragsverarbeiter des EU-Datenexporteurs liegt. Siehe hierzu die Abschnitte 4.6 und 4.7 zu Haftung und Gerichtsstand.

[12] Es ist zu beachten, dass in einigen Mitgliedstaaten nur Verträge als verbindlich angesehen werden. Daher ist eine Beratung vor Ort erforderlich, wenn anstelle von Verträgen andere rechtliche Mittel eingesetzt werden sollen.

[13] Nach dem internationalen Gesellschaftsrecht können angegliederte Unternehmen Verhaltenskodizes gegeneinander durchsetzen, wenn Verstöße gegen vertragsähnliche Vereinbarungen sowie Falschdarstellungen oder Fahrlässigkeit geltend gemacht werden.

2.3.2. Unternehmensinterne Datenschutzregelungen für Auftragsverarbeiter und ihre Verbindlichkeit für externe Unterauftragsverarbeiter der Daten

Vergibt der Auftragsverarbeiter mit Einwilligung des für die Verarbeitung Verantwortlichen Unteraufträge, die den Pflichten der Dienstevereinbarung (Artikel 17 der Richtlinie) unterliegen, an einen externen Unterauftragsverarbeiter, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich. Siehe hierzu Abschnitt 2.2.2 zu Weiterübermittlungen.

2.3.3. Rechtliche Durchsetzbarkeit der unternehmensinternen Datenschutzregelungen

2.3.3.1. Rechtliche Durchsetzbarkeit der unternehmensinternen Datenschutzregelungen durch die betroffenen Personen (Drittbegünstigtenrechte)

Betroffene Personen, die in den Anwendungsbereich der BCR für Auftragsverarbeiter fallen, müssen durch die Aufnahme einer Drittbegünstigungsklausel in die BCR, die entweder durch einseitige Verpflichtungen (möglichst nach einzelstaatlichem Recht) oder aufgrund vertraglicher Vereinbarungen zwischen den Mitgliedern der Unternehmensgruppe des Auftragsverarbeiters bindend ist, den Status von Drittbegünstigten erhalten.

Auf jeden Fall ist betroffenen Personen das Recht einzuräumen, die Einhaltung der Datenschutzregelungen gegenüber dem für die Verarbeitung Verantwortlichen durchzusetzen; dies kann durch Einreichen einer Beschwerde bei der Datenschutzbehörde oder bei dem Gericht erfolgen, das für den für die Verarbeitung Verantwortlichen in der EU zuständig ist (siehe Erläuterung in Abschnitt 4.6).

Sind die betroffenen Personen jedoch nicht in der Lage, Ansprüche gegen den für die Verarbeitung Verantwortlichen[14] geltend zu machen, so können sie rechtliche Schritte gegen den Auftragsverarbeiter auch bei der Datenschutzbehörde oder bei dem Gericht einleiten, das (i) für die EU-Hauptniederlassung des Auftragsverarbeiters oder (ii) für das in der EU für den Datenschutz zuständige Mitglied der Unternehmensgruppe des Auftragsverarbeiters oder (iii) für den Auftragsverarbeiter des EU-Datenexporteurs zuständig ist.

Besteht diese Möglichkeit nicht (beispielsweise weil der Auftragsverarbeiter keine Niederlassung in der EU hat), sind die betroffenen Personen berechtigt, vor dem Gericht an ihrem Wohnort Beschwerde einzulegen. Sieht das innerstaatliche

[14] Dies kann dann der Fall sein, wenn der für die Verarbeitung Verantwortliche faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des für die Verarbeitung Verantwortlichen übernommen; in letzterem Fall kann die betroffene Person ihre Rechte gegenüber dem Rechtsnachfolger geltend machen.

Recht jedoch eine für die betroffenen Personen günstigere Lösung vor (etwa nach dem Verbraucher- oder Arbeitsrecht), so wäre diese anwendbar.

In manchen Fällen ist die rechtliche Durchsetzbarkeit einer Drittbegünstigungsklausel in einseitigen Erklärungen eindeutig, in anderen Mitgliedstaaten ist die Lage dagegen unklarer und einseitige Erklärungen könnten für sich alleine unzureichend sein. Sollten einseitige Erklärungen nicht als Gewährleistung rechtlich durchsetzbarer Drittbegünstigtenrechte gelten können, muss das Unternehmen entsprechende vertragliche Vereinbarungen treffen. Solche Vereinbarungen können in allen Mitgliedstaaten privatrechtlich durchgesetzt werden.[15]

Mit der Drittbegünstigungsklausel soll die Durchsetzbarkeit folgender Grundsätze, die in den BCR festgelegt sind, gewährleistet werden:

- Pflicht des Auftragsverarbeiters zur Einhaltung der BCR und der Anweisungen des für die Verarbeitung Verantwortlichen bezüglich der Datenverarbeitung sowie der Sicherheits- und Vertraulichkeitsmaßnahmen entsprechend der Dienstevereinbarung (WP 195, Abschnitt 1.1);
- Drittbegünstigung für Betroffene (WP 195, Abschnitt 1.3);
- Pflicht des Auftragsverarbeiters zur Leistung von Schadenersatz und zur Abhilfe bei Verstößen gegen die BCR (WP 195, Abschnitt 1.5);
- die Beweislast trägt das Unternehmen, nicht die betroffene Person (WP 195, Abschnitt 1.7);
- die BCR sind für die betroffenen Personen leicht zugänglich (WP 195, Abschnitt 1.8);
- Beschwerdeverfahren für die BCR (WP 195, Abschnitt 2.2);
- Pflicht zur Zusammenarbeit mit den Datenschutzbehörden (WP 195, Abschnitt 3.1) und Pflicht zur Zusammenarbeit mit dem für die Verarbeitung Verantwortlichen (WP 195, Abschnitt 3.2);
- Datenschutzgrundsätze (WP 195, Abschnitt 6.1);
- Liste der Unternehmen des Auftragsverarbeiters, die an die BCR gebunden sind (WP 195, Abschnitt 6.2);
- Transparenz in Fällen, in denen das einzelstaatliche Recht der Einhaltung der BCR durch den Auftragsverarbeiter entgegensteht (WP 195, Abschnitt 6.3).

Vertragliche Vereinbarungen müssen nicht komplex oder umfangreich sein. Sie dienen lediglich als Instrumente, um den betroffenen Personen in denjenigen Ländern Drittbegünstigtenrechte zu bieten, in denen zweifelhaft ist, ob mit einseiti-

[15] Heute ist es in allen Mitgliedstaaten möglich, Drittbegünstigtenrechte in einem Vertrag zu gewähren. Siehe hierzu frühere Erfahrungen mit Standardvertragsklauseln und Drittbegünstigten.

gen Erklärungen ein ähnliches Ergebnis erreicht werden kann. Manchmal kann dieses Ziel durch die Aufnahme einer einfachen Klausel in bestehende Verträge zwischen den Mitgliedern der Unternehmensgruppe des Auftragsverarbeiters erreicht werden.

2.3.3.2. Rechtliche Durchsetzbarkeit der unternehmensinternen Datenschutzregelungen durch den für die Verarbeitung Verantwortlichen

Die BCR für Auftragsverarbeiter dienen als Garantie für internationale Datenübermittlungen, die der Auftragsverarbeiter seinem Kunden (dem für die Verarbeitung Verantwortlichen) bietet; dabei ist in erster Linie der für die Verarbeitung Verantwortliche gegenüber den Datenschutzbehörden und den betroffenen Personen dafür zuständig, den Schutz personenbezogener Daten sicherzustellen, die in Länder außerhalb der EU übermittelt werden. Daher müssen die BCR für Auftragsverarbeiter verbindlichen Charakter gegenüber dem für die Verarbeitung Verantwortlichen erhalten, indem in der Dienstevereinbarung ausdrücklich hierauf verwiesen wird.

Darüber hinaus, und um die BCR für Auftragsverarbeiter in eindeutiger Form mit der Dienstevereinbarung zu verknüpfen, die mit jedem Kunden (für die Verarbeitung Verantwortlichen) unterzeichnet wird, ist dafür zu sorgen, dass in der Dienstevereinbarung Folgendes geregelt bzw. enthalten ist:

– bei der Übermittlung besonderer Kategorien personenbezogener Daten muss der für die Verarbeitung Verantwortliche dafür Sorge tragen, dass die betroffenen Personen vor der Übermittlung davon in Kenntnis gesetzt worden sind oder in Kenntnis gesetzt werden, dass ihre Daten möglicherweise in ein Drittland übermittelt werden, das keinen ausreichenden Datenschutz bietet;

– des Weiteren die Verpflichtung des für die Verarbeitung Verantwortlichen, die betroffenen Personen über Auftragsverarbeiter außerhalb der EU und über die BCR für Auftragsverarbeiter in Kenntnis zu setzen. Der für die Verarbeitung Verantwortliche muss den betroffenen Personen auf Verlangen eine Kopie der BCR für Auftragsverarbeiter und der Dienstevereinbarung (ohne dass sensible und vertrauliche Geschäftsinformationen offengelegt werden) zugänglich machen;

– eindeutige Angaben zu Vertraulichkeits- und Sicherheitsmaßnahmen oder Verweis hierauf mittels elektronischem Link;

– eindeutige Beschreibung der Anweisungen und der Datenverarbeitung;

– genaue Angaben in der Dienstevereinbarung dazu, ob die Unterverarbeitung von Daten innerhalb oder außerhalb der Unternehmensgruppe des Auftragsverarbeiters erfolgen darf und ob die Einwilligung des für die Verarbeitung Verantwortlichen in grundsätzlicher Form erteilt wurde oder ob sie für jede Unterverarbeitung erneut zu erteilen ist.

Auch wenn die Datenschutzbehörden, die die BCR bewerten, nicht unbedingt die Vorlage einer solchen Dienstevereinbarung verlangen, so sind mit dem Antrag grundsätzlich eine Zusammenfassung sowie Auszüge aus dieser Vereinbarung einzureichen, in denen erläutert wird, wie die Durchsetzbarkeit der BCR für Auftragsverarbeiter durch die für die Verarbeitung Verantwortlichen gewährleistet wird.

Darüber hinaus enthalten die BCR eine Drittbegünstigungsklausel zugunsten des für die Verarbeitung Verantwortlichen, welche die gerichtlichen Rechtsbehelfe und Schadenersatzansprüche gegenüber allen Mitgliedern der Unternehmensgruppe des Auftragsverarbeiters einschließt und mit der sichergestellt werden soll, dass dieser zur Durchsetzung der BCR berechtigt ist.

2.3.3.3. Rechtliche Durchsetzbarkeit der unternehmensinternen Datenschutzregelungen durch die Datenschutzbehörden

Reicht ein Auftragsverarbeiter einen Antrag auf Anerkennung seiner BCR für Auftragsverarbeiter in der EU als angemessene Garantien des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen (Artikel 26 Absatz 2 der EU-Richtlinie 95/46/EG) ein, ist hieraus eindeutig abzuleiten, dass die Unternehmensgruppe des Auftragsverarbeiters sich damit gegenüber den Datenschutzbehörden in der EU zur Einhaltung der angeführten Garantien (in diesem Fall der BCR für Auftragsverarbeiter) verpflichtet. Es ist jedoch Aufgabe des für die Verarbeitung Verantwortlichen, die erforderliche nationale Genehmigung für die internationale Datenübermittlung einzuholen, wobei diese klar von der Anerkennung der BCR als Instrument, das ausreichende Garantien für Datenübermittlungen bietet, zu unterscheiden ist. Die BCR für Auftragsverarbeiter, die auf EU-Ebene bereits „anerkannt" (nicht „genehmigt") wurden, werden von dem für die Verarbeitung Verantwortlichen als die vorgesehenen angemessenen Garantien für internationale Datenübermittlungen angeführt.

Soweit die Datenschutzbehörden nach Artikel 28 der EU-Richtlinie 95/46/EG *„[…] beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen"*, bedeutet dies, dass sie unter anderem verpflichtet sind, Datenübermittlungen zu überwachen und die Garantien für Datenübermittlungen außerhalb der EU zu beurteilen.

Um diesen Verpflichtungen nachzukommen, werden die Datenschutzbehörden mit Untersuchungsbefugnissen, wirksamen Einwirkungsbefugnissen in ihrem Hoheitsgebiet sowie mit dem Klagerecht ausgestattet; diese Befugnisse können eingesetzt werden, um gegen einen Auftragsverarbeiter vorzugehen, der die BCR nicht einhält.

Ferner kann eine Verletzung der BCR für Auftragsverarbeiter durch ein Mitglied der Unternehmensgruppe des Auftragsverarbeiters (oder durch die gesamte Gruppe) dazu führen, dass die Genehmigung für die betreffende Datenübermittlung aufgehoben wird, die dem für die Verarbeitung Verantwortlichen auf der Grundlage der BCR für Auftragsverarbeiter erteilt wurde. Eine solche Aufhebung kann nicht rückwirkend erfolgen.

2.3.4. Für die Mitglieder der Unternehmensgruppe geltende zwingende Anforderungen nach nationalem Recht

Die BCR sollten eine eindeutige Bestimmung enthalten, nach der ein Mitglied der Unternehmensgruppe des Auftragsverarbeiters, wenn es Grund zu der Annahme hat, dass es durch die geltenden oder künftigen Rechtsvorschriften möglicherweise daran gehindert ist, die Anweisungen einzuhalten, die es von dem für die Verarbeitung Verantwortlichen erhalten hat, oder seine Pflichten nach den BCR oder der Dienstevereinbarung zu erfüllen, dies unverzüglich folgenden Stellen mitzuteilen hat:

– dem für die Verarbeitung Verantwortlichen, der berechtigt ist, die Datenübermittlung auszusetzen und/oder die Dienstevereinbarung zu kündigen,

– der EU-Hauptniederlassung des Auftragsverarbeiters oder dem in der EU für den Datenschutz zuständigen Mitglied oder den zuständigen Datenschutzbeauftragten/Datenschutzabteilungen, und

– der Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist.

Außerdem ist der Auftragsverarbeiter verpflichtet, den für die Verarbeitung Verantwortlichen über alle rechtlich bindenden Aufforderungen einer Strafverfolgungsbehörde zur Weitergabe personenbezogener Daten zu informieren, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen. Der Aufforderung zur Weitergabe sollte zunächst nicht nachgekommen werden. Stattdessen sind die Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist, sowie die Datenschutzbehörde, die für die BCR federführend ist, von dieser Aufforderung in Kenntnis zu setzen.

Es muss jedoch sichergestellt werden, dass die Weitergabe personenbezogener Daten an Strafverfolgungsbehörden auf einer dem geltenden Recht entsprechenden Rechtsgrundlage erfolgt, da die in Abschnitt 6.3 des Arbeitsdokuments WP 195 festgelegten Anforderungen der BCR für Auftragsverarbeiter lediglich ein Informationsverfahren vorsehen (siehe oben), das die Weitergabe nicht *per se* legitimiert. Bei Rechtskollisionen ist auf die für diesen Bereich geltenden internationalen Verträge und Vereinbarungen zu verweisen.

3. Wesentlicher Inhalt der verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter

3.1. Wesentlicher Inhalt und Ausführlichkeit

Die Datenschutzgrundsätze der Richtlinie müssen in den BCR für Auftragsverarbeiter weiterentwickelt und ausgeführt werden, so dass sie auf praktische und realistische Weise in die Verarbeitungstätigkeiten integriert werden können, die von dem Unternehmen in Drittländern durchgeführt werden, und von den im Unternehmen für den Datenschutz zuständigen Personen verstanden und wirksam angewandt werden können.

In Abschnitt 6 des Arbeitsdokuments WP 195 wird dieser Inhalt ausführlicher erläutert.

Während in die BCR lediglich eine allgemeine Beschreibung der Datenübermittlungen aufgenommen werden kann, sind im Rahmen des einzelstaatlichen Genehmigungsverfahrens bei den zuständigen Datenschutzbehörden ausführlichere Angaben zu den spezifischen Datenübermittlungen eines bestimmten für die Verarbeitung Verantwortlichen vorzulegen. Die BCR müssen ausreichend detailliert gehalten sein, so dass die Datenschutzbehörden beurteilen können, ob die angeführten Garantien für die Datenverarbeitung und die Unterverarbeitung, die in Drittländern von einem Mitglied der Unternehmensgruppe des Auftragsverarbeiters durchgeführt werden, angemessen sind.

3.2. Aktualisierung der BCR

Die Artikel-29-Datenschutzgruppe ist sich dessen bewusst, dass Unternehmen sich verändernde Organisationen sind, deren Unternehmensteile und Praktiken sich häufig ändern können, so dass die im Namen und nach den Anweisungen der für die Verarbeitung Verantwortlichen durchgeführten Datenübermittlungen und natürlich auch die in den BCR festgelegten Vorschriften nicht dauerhaft mit den Gegebenheiten zu dem Zeitpunkt übereinstimmen können, zu dem diese als angemessene Schutzmaßnahmen anerkannt wurden.

Deshalb können die BCR für Auftragsverarbeiter geändert werden (z. B. zur Anpassung an eine Änderung der gesetzlichen Regelungen oder der Unternehmensstruktur); sie müssen jedoch eine Pflicht zur Meldung solcher Änderungen an alle Mitglieder der Unternehmensgruppe, an die Datenschutzbehörden und an die für die Verarbeitung Verantwortlichen enthalten.

Betrifft eine Änderung die Verarbeitungsbedingungen, so sollte der für die Verarbeitung Verantwortliche hierüber so rechtzeitig informiert werden, dass er die

Möglichkeit hat, Einwendungen gegen die Änderungen zu erheben oder von dem Vertrag zurückzutreten, bevor die Änderung vorgenommen wird (z. B. Mitteilung über beabsichtigte Änderungen, die die Hinzuziehung weiterer Unterauftragnehmer oder den Ersatz von Unterauftragnehmern betreffen, bevor die Daten dem neuen Unterauftragsverarbeiter übermittelt werden).

Unter folgenden Voraussetzungen sind Aktualisierungen der BCR für Auftragsverarbeiter oder der Liste der Mitglieder, die an die BCR für Auftragsverarbeiter gebunden sind, ohne neuen Antrag bei der Datenschutzbehörde möglich:

i) Es wird eine Person benannt, die eine stets aktualisierte Liste der Gruppenmitglieder und der Unterauftragsverarbeiter führt, die an der Datenverarbeitungstätigkeit des für die Verarbeitung Verantwortlichen mitwirken; diese Liste ist dem für die für die Verarbeitung Verantwortlichen, den betroffenen Personen und den Datenschutzbehörden zugänglich zu machen.

ii) Diese Person verfolgt und dokumentiert alle Aktualisierungen der Vorschriften, leitet die notwendigen Informationen systematisch an den für die Verarbeitung Verantwortlichen weiter und erteilt den Datenschutzbehörden auf Anfrage diesbezügliche Auskünfte.

iii) Einem neuen Mitglied der Unternehmensgruppe dürfen personenbezogene Daten erst dann übermittelt werden, wenn dieses neue Mitglied an die BCR für Auftragsverarbeiter gebunden ist und in der Lage ist, die Einhaltung der Vorschriften zu gewährleisten.

iv) Signifikante Änderungen der BCR für Auftragsverarbeiter oder der Mitgliederliste müssen den zuständigen Datenschutzbehörden, die den für die Verarbeitung Verantwortlichen die Genehmigung für Datenübermittlungen erteilen, jährlich mit einer kurzen Begründung der Änderungen gemeldet werden.

Die Aktualisierung der Vorschriften ist in dem Sinne zu verstehen, dass sich möglicherweise Arbeitsverfahren geändert haben und die Vorschriften an die geänderten Gegebenheiten anzupassen sind.

4. Einhaltung und Durchsetzung der Vorschriften

Neben den Vorschriften, die wesentliche Grundsätze des Datenschutzes betreffen, müssen verbindliche unternehmensinterne Datenschutzregelungen für den Auftragsverarbeiter außerdem Folgendes enthalten:

4.1. Bestimmungen, die eine möglichst umfassende Einhaltung der Vorschriften garantieren

Mit Hilfe der Datenschutzregelungen soll ein System geschaffen werden, das die Beachtung und Umsetzung der Vorschriften innerhalb und außerhalb der Europäischen Union garantiert. Die Einführung unternehmensinterner Datenschutzgrundsätze durch die Hauptniederlassung ist lediglich als erster Schritt anzusehen, um ausreichende Garantien im Sinne von Artikel 26 Absatz 2 der Richtlinie bieten zu können. Das antragstellende Unternehmen muss außerdem nachweisen können, dass die diesbezüglichen Grundsätze den Mitarbeitern bekannt sind und von ihnen verstanden und in der ganzen Unternehmensgruppe wirksam angewandt werden und dass die Mitarbeiter eine geeignete Schulung erhalten haben und jederzeit Zugriff auf die relevanten Informationen (einschließlich der BCR) haben, zum Beispiel im Intranet. Für die Aufsicht und die Sicherstellung der Einhaltung ernennt das Unternehmen einen geeigneten Stab, der von der oberen Leitungsebene unterstützt wird.

4.2. Audits

In den Vorschriften müssen regelmäßige Datenschutzaudits und/oder eine externe Überwachung durch interne oder externe akkreditierte Auditoren festgelegt werden, die dem Datenschutzbeauftragten/der Datenschutzabteilung bzw. dem Aufsichtsrat der Muttergesellschaft direkt Bericht erstatten. Auf Verlangen sind diese Audits dem für die Verarbeitung Verantwortlichen zugänglich zu machen.[16]

Ferner ist in den BCR für Auftragsverarbeiter festzulegen, dass den Datenschutzbehörden, die für den für die Verarbeitung Verantwortlichen zuständig sind, auf Antrag Zugang zu den Ergebnissen der Audits zu gewähren ist und dass ihnen die Berechtigung einzuräumen ist, bei Bedarf – sofern dies rechtlich möglich ist – selbst ein Datenschutzaudit durchzuführen. Dies dürfte vor allem dann der Fall sein, wenn die im vorstehenden Absatz vorgesehenen Audits – aus welchen Gründen auch immer – nicht verfügbar sind, wenn sie die für eine normale Weiterverfolgung der von den Datenschutzbehörden erteilten Genehmigung erforderlichen Angaben nicht enthalten oder wenn die Dringlichkeit der Lage eine direkte Beteiligung der Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist, angeraten erscheinen lässt.

Solche Audits werden nach den einschlägigen Gesetzen und Vorschriften durchgeführt, die ungeachtet der Überprüfungsbefugnisse der einzelnen Datenschutzbehörden auf die Untersuchungsbefugnisse von Datenschutzbehörden Anwendung

[16] Diese Audits müssen umfassend angelegt sein und auf jeden Fall auf bestimmte in diesem Arbeitsdokument bereits aufgeführte Einzelheiten eingehen, zum Beispiel die Weiterübermittlung auf der Grundlage von Standardvertragsklauseln (siehe Abschnitt 2.2.2.) oder die Entscheidungen hinsichtlich der zwingenden Anforderungen nach nationalen Rechtsvorschriften, die zu Konflikten mit den verbindlichen unternehmensinternen Datenschutzregelungen führen könnten (siehe Abschnitt 3.3.3.).

finden. Grundsätzlich werden solche Audits unter Beachtung der Vertraulichkeit und der Geschäftsgeheimnisse durchgeführt und sind strikt auf die Feststellung der Einhaltung der unternehmensinternen Datenschutzregelungen beschränkt.

Außerdem muss aus den BCR für Auftragsverarbeiter hervorgehen, dass jeder Auftragsverarbeiter oder Unterauftragsverarbeiter, der die Daten eines bestimmten, für die Verarbeitung Verantwortlichen verarbeitet, sich bereit erklärt, auf Verlangen dieses für die Verarbeitung Verantwortlichen seine Datenverarbeitungseinrichtungen im Hinblick auf diejenigen Datenverarbeitungstätigkeiten prüfen zu lassen, die mit dem betreffenden für die Verarbeitung Verantwortlichen in Zusammenhang stehen. Dieses Audit wird von dem für die Verarbeitung Verantwortlichen oder einem Prüfgremium durchgeführt, dessen Mitglieder unabhängig agieren, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind; das Prüfgremium wird von dem für die Verarbeitung Verantwortlichen ausgewählt, gegebenenfalls in Absprache mit der für ihn zuständigen Datenschutzbehörde.

Dem Antrag ist eine Beschreibung des Auditsystems beizufügen. Darin ist zum Beispiel anzugeben,

– welche Abteilung innerhalb des Unternehmens über den Auditplan/das Auditprogramm entscheidet,

– welche Abteilung das Audit durchführt,

– wann das Audit durchgeführt wird (regelmäßig oder auf besonderen Antrag der Datenschutzabteilung),

– welchen Umfang das Audit hat (z. B. Anwendungen, IT-Systeme, Datenbanken, in denen personenbezogene Daten verarbeitet werden, oder Weiterübermittlungen, Beschlüsse im Hinblick auf zwingende Anforderungen nach nationalem Recht, die den BCR für Auftragsverarbeiter entgegenstehen, Überprüfung der Vertragsklauseln, auf deren Grundlage Daten außerhalb der Unternehmensgruppe des Auftragsverarbeiters (an für die Verarbeitung Verantwortliche oder Auftragsverarbeiter) übermittelt werden, Abhilfemaßnahmen usw.),

– wer die Auditergebnisse erhält.

4.3. Bearbeitung von Beschwerden

Der Auftragsverarbeiter der Unternehmensgruppe muss sich in den BCR für Auftragsverarbeiter verpflichten, eigens eine Kontaktstelle für betroffene Personen einzurichten.

Alle Mitglieder, die an die BCR für Auftragsverarbeiter gebunden sind, müssen sich verpflichten, die Beschwerde oder Anfrage unverzüglich dem für die Ver-

arbeitung Verantwortlichen zuzuleiten; sie selbst sind nicht verpflichtet, die Beschwerde oder Anfrage zu bearbeiten (sofern mit dem für die Verarbeitung Verantwortlichen keine anderslautenden Vereinbarungen getroffen wurden).

Nur in Fällen, in denen der für die Verarbeitung Verantwortliche faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, muss der Auftragsverarbeiter Beschwerden bearbeiten.

Werden Beschwerden durch den Auftragsverarbeiter bearbeitet (sofern dies mit dem für die Verarbeitung Verantwortlichen vereinbart ist oder der für die Verarbeitung Verantwortliche faktisch oder rechtlich nicht mehr besteht), muss dies durch eine klar benannte Abteilung oder Person geschehen, die bei der Wahrnehmung ihrer Aufgaben hinreichend unabhängig ist.

In diesen Fällen ist die betroffene Person darüber zu informieren,

– wo die Beschwerde einzureichen ist,
– in welcher Form sie einzureichen ist,
– wie lange die Bearbeitung der Beschwerde dauern wird,
– welche Folgen die Ablehnung der Beschwerde hat,
– welche Folgen die Anerkennung der Beschwerde hat,
– welche Rechtsbehelfe der betroffenen Person zur Verfügung stehen, wenn sie mit der Behandlung ihrer Beschwerde nicht zufrieden ist (Einlegung eines Rechtsbehelfs bei Gericht/der Datenschutzbehörde).

4.4. Pflicht zur Zusammenarbeit mit dem für die Verarbeitung Verantwortlichen

In den BCR für Auftragsverarbeiter muss ausdrücklich festgelegt sein, dass alle Mitglieder der Unternehmensgruppe und die Beschäftigten die Anweisungen des für die Verarbeitung Verantwortlichen bezüglich der Datenverarbeitung sowie die Sicherheits- und Vertraulichkeitsmaßnahmen entsprechend der Dienstevereinbarung (Artikel 17 der Richtlinie) befolgen müssen.

Ferner müssen die BCR die Auftragsverarbeiter oder Unterauftragsverarbeiter unmissverständlich dazu verpflichten, mit dem für die Verarbeitung Verantwortlichen zusammenzuarbeiten und ihn bei der Einhaltung der Datenschutzvorschriften zu unterstützen (z. B. bei der Erfüllung seiner Pflicht, die Rechte der betroffenen Personen zu wahren oder ihre Beschwerden zu bearbeiten oder auf eine Untersuchung oder Anfrage der Datenschutzbehörden zu reagieren). Dies hat binnen einer angemessenen Frist und in dem Umfang zu geschehen, in dem dies in angemessener Weise möglich ist.

4.5. Pflicht zur Zusammenarbeit mit den Datenschutzbehörden

Wie im Arbeitsdokument WP 12 ausgeführt, ist der Umfang der Unterstützung und Hilfe, die betroffenen Personen geboten werden, eines der wichtigsten Merkmale, mit dem die Angemessenheit eines Systems der Selbstkontrolle bewertet werden kann: *„Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, dass der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben."*

Dies ist durchaus ein wichtiges Merkmal der BCR für Auftragsverarbeiter: In den Datenschutzregelungen muss in eindeutiger Form festgelegt sein, dass alle Mitglieder der Unternehmensgruppe des Auftragsverarbeiters zur Zusammenarbeit mit den Datenschutzbehörden, die für den betreffenden für die Verarbeitung Verantwortlichen zuständig sind, verpflichtet sind und Einzelpersonen somit die institutionelle Unterstützung erhalten, die im Arbeitsdokument WP 12 angesprochen wird.

Außerdem muss eine eindeutige Verpflichtung vorliegen, dass das Unternehmen als Ganzes und jeder Unternehmensteil für sich die Stellungnahme der zuständigen Datenschutzbehörde zu allen Problemen der Auslegung und Anwendung dieser BCR für Auftragsverarbeiter einhalten wird.

Vor einer Stellungnahme kann die zuständige Datenschutzbehörde die Meinung des Unternehmens, der betroffenen Personen, der jeweiligen für die Verarbeitung Verantwortlichen und der Datenschutzbehörden einholen, die gegebenenfalls im Rahmen des in diesem Arbeitsdokument vorgesehenen koordinierten Verfahrens[17] beteiligt sind. Die Stellungnahme der Behörde kann veröffentlicht werden.

Zusätzlich zu den einschlägigen nationalen Bestimmungen kann eine ernsthafte und/oder anhaltende Weigerung des Unternehmens, mit der zuständigen Datenschutzbehörde zusammenzuarbeiten oder deren Stellungnahme zu befolgen, dazu führen, dass die dem für die Verarbeitung Verantwortlichen erteilte Genehmigung zur Datenübermittlung entweder durch die Datenschutzbehörde selbst oder durch die nach den nationalen Rechtsvorschriften dazu befugte Behörde ausgesetzt oder aufgehoben wird. Die unmittelbare Konsequenz einer solchen Aussetzung oder Aufhebung besteht darin, dass der betreffende für die Verarbeitung Verantwortliche den angemessenen Schutz der übermittelten Daten auf andere Weise gewährleisten muss, zum Beispiel durch die Unterzeichnung der Standardvertragsklauseln 2010/87/EU, oder dass er für diese Datenübermittlungen entsprechend den geltenden nationalen Rechtsvorschriften bei den zuständigen Datenschutzbehörden einen neuen Antrag stellen muss.

[17] Siehe Kapitel 5.

4.6. Haftung

4.6.1. Allgemeines Recht auf Rechtsbehelfe und gegebenenfalls Entschädigung

In den Datenschutzregelungen ist anzugeben, dass die Drittbegünstigtenrechte der betroffenen Personen und die Rechtsbehelfe des für die Verarbeitung Verantwortlichen die gerichtlichen Rechtsbehelfe und Schadenersatzansprüche (im Falle der betroffenen Personen sind nicht nur materielle, sondern auch immaterielle Schäden zu berücksichtigen) einschließen.

Als Ergänzung dieses allgemeinen Rechts müssen die Vorschriften auch Bestimmungen über Haftung und Gerichtsstand enthalten, die deren Wahrnehmung in der Praxis erleichtern.

4.6.2. Vorschriften zur Haftung

4.6.2.1. Vorschriften zur Haftung für betroffene Personen

Als Drittbegünstigte sind betroffene Personen berechtigt, die BCR gegenüber den Mitgliedern der Unternehmensgruppe des Auftragsverarbeiters durchzusetzen, die gegen die BCR verstoßen haben.

In den BCR für Auftragsverarbeiter muss zudem festgelegt werden, welches Mitglied der Unternehmensgruppe – (i) die EU-Hauptniederlassung oder (ii) das in der EU für den Datenschutz zuständige Mitglied des Auftragsverarbeiters oder (iii) der Auftragsverarbeiter des EU-Datenexporteurs (z. B. die Vertragspartei des für die Verarbeitung Verantwortlichen in der EU) – verpflichtet ist, die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU (die gegen die BCR oder die Dienstevereinbarung verstoßen haben) oder für Vertragsverletzungen (siehe hierzu Abschnitt 2.2.2) externer Unterauftragsverarbeiter außerhalb der EU zu übernehmen und Abhilfe zu schaffen sowie gegebenenfalls Schadenersatz zu leisten. Entscheidet sich das Unternehmen für die dritte Option (Auftragsverarbeiter des EU-Datenexporteurs), so muss es der federführenden Datenschutzbehörde gegenüber darlegen, warum kein Unternehmen benannt werden konnte, das für die gesamte Unternehmensgruppe haftbar ist.

Statt des Mitglieds der Unternehmensgruppe außerhalb der EU oder des externen Unterauftragnehmers außerhalb der EU, das bzw. der den Verstoß gegen die BRC begangen hat, erklärt sich das benannte Mitglied der Unternehmensgruppe zur Übernahme der Haftung bereit, als ob die Verletzung von ihm in dem Mitgliedstaat begangen wurde, in dem es niedergelassen ist.

Zum Ausschluss der eigenen Haftung kann dieses Mitglied sich nicht darauf berufen, dass der Verstoß gegen seine Pflichten durch einen (internen oder externen) Unterauftragsverarbeiter (der Unternehmensgruppe) begangen wurde.

Sofern kein Mitglied der Unternehmensgruppe in der EU niedergelassen ist, übernimmt die außerhalb der EU befindliche Hauptniederlassung der Unternehmensgruppe diese Haftung.

4.6.2.2. Vorschriften zur Haftung für den für die Verarbeitung Verantwortlichen

In den BCR für Auftragsverarbeiter muss festgelegt sein, dass alle für die Verarbeitung Verantwortlichen berechtigt sind, die BCR für Auftragsverarbeiter gegen jedes Mitglied der Unternehmensgruppe des Auftragsverarbeiters durchzusetzen, das gegen die BCR verstößt. Der für die Verarbeitung Verantwortliche ist außerdem befugt, die schriftliche Vereinbarung (siehe hierzu Abschnitt 2.2.2) gegen externe Unterauftragsverarbeiter durchzusetzen, die gegen diese Vereinbarung verstoßen.

Ferner hat der für die Verarbeitung Verantwortliche im Falle eines Verstoßes durch ein nicht in der EU niedergelassenes Unternehmen des Auftragsverarbeiters oder durch einen externen, nicht in der EU niedergelassenen Unterauftragsverarbeiter das Recht, die BCR für Auftragsverarbeiter gegenüber dem Unternehmen des Auftragsverarbeiters[18] durchzusetzen, das die Pflicht zur Leistung von Schadenersatz und zur Abhilfe bei Verstößen gegen die BCR, die Dienstevereinbarung oder die mit den externen Unterauftragsverarbeitern geschlossenen schriftlichen Vereinbarungen anerkannt hat.

Das Unternehmen verpflichtet sich in seinem Antrag auf Genehmigung der BCR für Auftragsverarbeiter dazu, dass der Unternehmensteil, der die Haftung für Handlungen anderer Mitglieder außerhalb der EU, die an die BCR für Auftragsverarbeiter gebunden sind, und für externe Unterauftragsverarbeiter außerhalb der EU übernommen hat, über ausreichende Mittel verfügt, um den entstandenen Schaden zu ersetzen.

4.6.2.3. Beweislast

Aus den BCR für Auftragsverarbeiter muss zudem Folgendes hervorgehen: Wenn eine betroffene Person oder der für die Verarbeitung Verantwortliche nachweisen kann, dass sie bzw. er geschädigt wurde, und anhand von Tatsachennachweisen belegt, dass der Schaden wahrscheinlich wegen des Verstoßes gegen die

[18] Die EU-Hauptniederlassung des Auftragsverarbeiters oder das in der EU für den Datenschutz zuständige Mitglied der Unternehmensgruppe des Auftragsverarbeiters oder der Auftragsverarbeiter des EU-Datenexporteurs (siehe Arbeitsdokument WP 195, Abschnitt 1.5).

BCR für Auftragsverarbeiter (oder die Dienstevereinbarung oder die in Abschnitt 2.2.2 erwähnten schriftlichen Verträge) entstanden ist, muss dasjenige Mitglied der Unternehmensgruppe, das die Haftung übernommen hat, nachweisen, dass der Verstoß, durch den der Schaden verursacht wurde, nicht durch das außerhalb der EU ansässige Mitglied der Unternehmensgruppe oder den externen Unterauftragsverarbeiter verursacht wurde, oder dass ein solcher Verstoß nicht stattfand.

Kann das Unternehmen, das die Haftung übernommen hat, nachweisen, dass die schadensbegründende Handlung nicht dem außerhalb der EU ansässigen Mitglied der Unternehmensgruppe zuzurechnen ist, so ist es selbst von der Haftung befreit.

4.7. Vorschrift zum Gerichtsstand

Wie in Abschnitt 4.6.2. oben ausgeführt, muss das Unternehmen auch akzeptieren, dass betroffene Personen berechtigt sind, Verfahren gegen das Unternehmen einzuleiten, wenn sie nicht in der Lage sind, Ansprüche gegen den für die Verarbeitung Verantwortlichen[19] geltend zu machen, und den Gerichtsstand (Datenschutzbehörde oder Gericht) wie folgt zu wählen:

a) bei den zuständigen Datenschutzbehörden,

b) am Gerichtsstand des in der EU niedergelassenen Mitglieds der Unternehmensgruppe des Auftragsverarbeiters am Herkunftsort der Übermittlung,

c) am Gerichtsstand der EU-Hauptniederlassung des Auftragsverarbeiters,

d) am Gerichtsstand des in der EU für den Datenschutz zuständigen Mitglieds der Unternehmensgruppe des Auftragsverarbeiters oder,

e) sofern kein Mitglied der Unternehmensgruppe in der EU niedergelassen ist, sind die betroffenen Personen und der für die Verarbeitung Verantwortliche berechtigt, bei den Datenschutzbehörden oder bei den Gerichten an ihrem Wohn-/Niederlassungsort Beschwerde einzulegen. Befindet sich der Wohn-/Niederlassungsort der betroffenen Person oder des für die Verarbeitung Verantwortlichen außerhalb der EU und legt diese bzw. dieser eine Beschwerde bei einem Gericht in einem Drittland ein, so sind die zuständigen Datenschutzbehörden in der EU über ein solches Verfahren und seinen Ausgang zu informieren.

[19] Dies kann der Fall sein, wenn der für die Verarbeitung Verantwortliche faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des für die Verarbeitung Verantwortlichen übernommen; in letzterem Fall kann die betroffene Person ihre Rechte gegenüber dem Rechtsnachfolger geltend machen.

Bei einem gut funktionierenden System – dazu gehören die möglichst umfassende Einhaltung der Vorschriften in der gesamten Unternehmensgruppe, regelmäßige Audits, die effiziente Behandlung von Beschwerden, Zusammenarbeit mit Datenschutzbehörden usw. – erscheint der Gang zum Gericht unwahrscheinlich, kann jedoch nicht grundsätzlich ausgeschlossen werden. Erst die Erfahrung mit diesen Instrumenten wird zeigen, ob diese Einschätzung zutreffend ist.

Es gelten die in der Richtlinie und in den nationalen Rechtsvorschriften enthaltenen einschlägigen Grundsätze und Regelungen zum Gerichtsstand.

4.8. Transparenz

Unternehmen, die BCR für Auftragsverarbeiter einsetzen, müssen nachweisen können, dass für die betroffenen Personen alle im Rahmen der BCR eingegangenen Verpflichtungen, deren Einhaltung diese Personen als Drittbegünstigte durchsetzen können, leicht zugänglich sind. Auf der Website des Unternehmens sind die BCR für Auftragsverarbeiter daher so zu veröffentlichen, dass sie für die betroffenen Personen leicht zugänglich sind, oder es ist dort zumindest ein Dokument mit allen Informationen (und nicht nur eine Zusammenfassung der Informationen) zu veröffentlichen, das die in Abschnitt 2.3.3.1 aufgeführten Drittbegünstigtenrechte enthält.

Was den für die Verarbeitung Verantwortlichen betrifft, ist durch die Dienstevereinbarung gewährleistet, dass die BCR für Auftragsverarbeiter Bestandteil des Vertrags sind. Die BCR für Auftragsverarbeiter werden der Dienstevereinbarung als Anlage beigefügt oder es wird auf die BCR – mit einer Möglichkeit für den elektronischen Zugriff – verwiesen.

5. Schlussfolgerung

Die Datenschutzgruppe ist der Auffassung, dass die in diesem Dokument vorgelegten Leitlinien dazu beitragen können, die Anwendung von Artikel 26 Absatz 2 der Richtlinie in Bezug auf die BCR für Auftragsverarbeiter zu vereinfachen. Außerdem soll dadurch eine gewisse Vereinfachung der Arbeit internationaler Unternehmen erreicht werden, die im Auftrag der für die Verarbeitung Verantwortlichen auf weltweiter Basis routinemäßig personenbezogene Daten verarbeiten und austauschen.

Der Inhalt dieses Arbeitsdokuments sollte nicht als das letzte Wort der Artikel-29-Datenschutzgruppe zu diesem Thema verstanden werden, sondern als ein fundierter erster Schritt, mit dem die Verwendung von BCR für Auftragsverarbeiter auf der Grundlage eines Systems der Selbstkontrolle und der Zusammenarbeit zwischen den Behörden gefördert werden soll. Dies schließt auch die Möglichkeit

nicht aus, auf andere Instrumente für die Übermittlung personenbezogener Daten ins Ausland zurückzugreifen, beispielsweise die Standardvertragsklauseln oder gegebenenfalls die Grundsätze des sicheren Hafens.

Weitere Beiträge interessierter Kreise und Fachleute auf der Grundlage der Erfahrungen mit dem Einsatz dieser Arbeitsunterlage sind willkommen. Möglicherweise wird die Datenschutzgruppe dieses Thema vor dem Hintergrund der gewonnenen Erfahrungen erneut überprüfen.

Brüssel, den 19. April 2013

Für die Datenschutzgruppe
Der Vorsitzende
Jacob Kohnstamm

Stellungnahme 05/2013 zu intelligenten Grenzen (WP 206)

Angenommen am 6. Juni 2013

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

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

gestützt auf Artikel 29, Artikel 30 Absatz 1 Buchstabe c und Artikel 30 Absatz 3 der genannten Richtlinie sowie gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

Einleitung

Am 28. Februar 2013 legte die Kommission Vorschläge für ein Einreise-/Ausreisesystem (EES) und ein Registrierungsprogramm für Reisende (RTP) für den Schengen-Raum vor, die zusammen als Vorschläge für „intelligente Grenzen" bezeichnet werden. Außerdem wurde ein Vorschlag für erforderliche Änderungen des Schengener Grenzkodex vorgelegt.

Der Vorschlag für ein Einreise-/Ausreisesystem umfasst ein System zur zentralen Speicherung der Ein- und Ausreisedaten von Drittstaatsangehörigen, die für Kurzaufenthalte im Schengen-Raum zugelassen sind, unabhängig davon, ob sie einer Visumpflicht für ein Schengen-Visum unterliegen. Anstatt die Reisepässe bei der Einreise in den Schengen-Raum und der Ausreise aus dem Schengen-Raum abzustempeln, werden Daten über die Identität des Besuchers sowie über Dauer und Zweck des Aufenthalts bei der Einreise in das System eingegeben und bei der Ausreise überprüft, um sicherzustellen, dass der Drittstaatsangehörige die höchstens zulässige Aufenthaltsdauer nicht überschritten hat. Da das EES ein zentrales System darstellt, ist bei der Prüfung der EES-Daten unerheblich, über welche Grenzübergangsstelle der Drittstaatsangehörige aus dem Schengen-Raum ausreist. In erster Linie soll mit dem System verhindert werden, dass Drittstaatsangehörige, die ursprünglich mit einem gültigen Visum oder für einen zulässigen Zweck für einen Kurzaufenthalt (maximal 90 Tage innerhalb eines Zeitraums von 180 Tagen) eingereist sind, die zulässige Aufenthaltsdauer im Schengen-Raum überziehen. Der Vorschlag für ein EES umfasst ein System, in dem zunächst personenbezogene Daten erfasst werden, die zur Identifizierung von Personen benö-

tigt werden. (Diese Daten werden im Wortlaut des Vorschlags nur als „alphanumerische Daten" bezeichnet.) Nach drei Jahren sollen auch „biometrische Daten" erfasst werden. Nach zwei Jahren soll geklärt werden, ob Strafverfolgungsbehörden und Drittstaaten Zugang zu den im System gespeicherten Informationen erhalten sollten.

Der Vorschlag für ein Registrierungsprogramm für Reisende (RTP) umfasst ein Programm zur Registrierung von Reisenden, die häufig in den Schengen-Raum einreisen (Vielreisende), beispielsweise Geschäftsreisende. Drittstaatsangehörige können den Status als registrierte Vielreisende beantragen, um die Grenzabfertigung zu beschleunigen. Grundlage des RTP bilden ein Zentralregister mit biometrischen Daten sowie ein an die Reisenden ausgehändigtes „Token", auf dem eine individuelle Kennnummer gespeichert ist.

Die Artikel-29-Datenschutzgruppe wiederholt die Bedenken, die sie bereits bei Veröffentlichung der Mitteilung über intelligente Grenzen in ihrem Schreiben an Kommissarin Malmström geäußert hat[1]. Die Datenschutzgruppe hat hinsichtlich der Vorschläge aus datenschutzrechtlicher Sicht unverändert Vorbehalte. Insbesondere hat die Datenschutzgruppe ernsthafte Zweifel daran, dass das Einreise-/Ausreisesystem den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit entspricht und dass die Beeinträchtigungen des Rechts auf den Schutz personenbezogener Daten gemäß Artikel 8 der EU-Charta der Grundrechte gerechtfertigt sind.

Diese Stellungnahme konzentriert sich hauptsächlich auf das Einreise-/Ausreisesystem und geht darüber hinaus auf einige spezifische Datenschutzbelange des Registrierungsprogramms für Reisende ein. Hauptziel der Stellungnahme ist die Untersuchung des Einreise-/Ausreisesystems unter dem Aspekt der Notwendigkeit und der Verhältnismäßigkeit und die entsprechende Möglichkeit der Rechtfertigung einer Verletzung der Privatsphäre. Im zweiten Teil der Stellungnahme werden einige spezifische Datenschutzbelange beider Vorschläge behandelt.

Teil I: Einreise-/Ausreisesystem – Prüfung der Notwendigkeit

Mit dem EES würde vor allen Dingen eine neue, sehr umfangreiche Datenbank geschaffen. Daher müssen die Eingriffe in das Recht auf Privatsphäre gemäß Artikel 8 der EU-Charta der Grundrechte gerechtfertigt werden.

1. Hintergrund – Ziele und Kontext

Die Datenschutzgruppe hat bereits anerkannt, dass eine integrierte Verwaltung der EU-Außengrenzen notwendig ist und dass die Verbesserung der Steuerung

[1] Schreiben der Datenschutzgruppe an Kommissarin Malmström zu intelligenten Grenzen, 12.6.2012, Ref. Ares (2012) 707810 – 13.6.2012.

von Migrationsströmen und die Vermeidung der irregulären Migration rechtmäßige Zwecke darstellen.[2] Der Mehrwert eines EES zur Erreichung dieser Ziele reicht jedoch nicht aus, um die Notwendigkeit des EES sowie seine Verhältnismäßigkeit hinsichtlich der Auswirkungen auf die Grundrechte, einschließlich des Rechts auf Datenschutz und auf Privatsphäre, zu begründen. Eingriffe in das Privatleben sind dann zulässig, wenn sie „in einer demokratischen Gesellschaft notwendig" sind. Bei einem bloßen Mehrwert ist die geforderte Notwendigkeit in diesem Kontext nicht gegeben.

Bei der Bewertung der Verhältnismäßigkeit sollte auch der Anwendungsbereich des EES berücksichtigt werden. Wie viele Grenzübertritte in den Schengen-Raum würden tatsächlich über das EES abgefertigt? Laut der Folgenabschätzung der Kommission sind 73,5 % der Reisenden an Schengen-Grenzübergangsstellen entweder EU-Bürger oder Berechtigte gemäß der Richtlinie 2004/38/EG.[3] Die restlichen 26,5 % umfassen Visuminhaber und Nicht-Visuminhaber. Dabei wird jedoch nicht klar, ob es sich um Besucher mit kurzer Aufenthaltsdauer handelt oder ob in diesen Zahlen Inhaber von Visa für lange Aufenthalte oder Inhaber sonstiger Aufenthaltserlaubnisse enthalten sind, die nicht in den Anwendungsbereich des EES fallen. Das EES wird also nur einen relativ kleinen Prozentanteil (wenn auch eine sehr große Zahl) von Grenzübertritten betreffen. Dies wirft die Frage auf, ob die Einrichtung einer solch großen Datenbank gemessen am Umfang des zu bewältigenden Problems verhältnismäßig wäre. Zudem ist der verfolgte Zweck – die Unterbindung des Problems, dass die zulässige Aufenthaltsdauer überzogen wird – einer der Hauptzwecke einer weiteren großen EU-Datenbank, des Visa-Informationssystems (VIS). Dieser Zweck wird in Erwägungsgrund 5 der VIS-Verordnung deutlich zum Ausdruck gebracht: „Das VIS sollte auch die Identifizierung von Personen, die die Voraussetzungen für die Einreise in das Hoheitsgebiet der Mitgliedstaaten oder den dortigen Aufenthalt nicht bzw. nicht mehr erfüllen, […] unterstützen". In der Folgenabschätzung wird nichts darüber ausgesagt, warum das VIS für die Erfüllung dieses Zweckes nicht ausreichend sein sollte.

In diesem Zusammenhang ist der Umfang des Problems der Überziehung der zulässigen Aufenthaltsdauer zu berücksichtigen, das mit dem EES (ergänzend zum VIS) bewältigt werden soll. Nach Schätzungen des Projekts „Clandestino" liegt die Zahl der Personen, die die zulässige Aufenthaltsdauer überziehen (sogenannte „Overstayer"), in der EU zwischen 1,8 und 3,9 Millionen.[4] Verlässliche Zahlen sind nicht verfügbar, und die Feststellung, dass diesbezüglich ein erhebliches Problem bestehe, gründet sich allein auf eine verbreitete Ansicht. Es ist natür-

[2] Schreiben der Datenschutzgruppe an Kommissarin Malmström zu intelligenten Grenzen, 12.6.2012 Ref. Ares (2012) 707810 – 13.6.2012.

[3] Impact Assessment accompanying the document *Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, SWD(2013) 47 final, S. 12.

[4] Ebenda, S. 12.

lich problematisch, eine große Datenbank auf der Grundlage derart unsicherer Belege zu erstellen. Die Datenschutzgruppe betont jedoch, dass dies kein Grund sein kann, eine Datenbank einzurichten, die zunächst die statistischen Daten zu beschaffen versucht, um die Existenz dieser Datenbank vielleicht im Nachhinein zu rechtfertigen.

Der Zweck und die Methodik dieser Analyse bestehen darin, die Eignung, Notwendigkeit und Verhältnismäßigkeit des Einreise-/Ausreisesystems sowie mögliche Alternativen zu diesem System zu untersuchen. Um zu beurteilen, ob das EES der Anforderung der Notwendigkeit entspricht, müssen zunächst die zugrunde liegenden Ziele des Systems untersucht und unter Berücksichtigung des allgemeinen politischen Kontexts betrachtet werden.

Wenn die Ziele des Vorschlags im Kontext betrachtet werden, können die Notwendigkeit und die Verhältnismäßigkeit anhand von drei Fragen geprüft werden:

- Ist das EES geeignet, ein rechtmäßiges Ziel zu erreichen?
- Ist ein EES – angesichts seiner Auswirkungen auf Grundrechte wie z. B. das Recht auf Datenschutz und auf Privatsphäre – notwendig, um dieses rechtmäßige Ziel zu erreichen?
- Sind bereits bestehende Alternativen verfügbar, mit denen das gleiche rechtmäßige Ziel ohne entsprechende Beeinträchtigung von Grundrechten (u. a. der Rechte auf Datenschutz und auf Schutz der Privatsphäre) erreicht werden kann?

1.1 Ziele des EES

Die Datenschutzgruppe nimmt zur Kenntnis, dass das EES laut Aussage der Kommission vier politische Ziele verfolgt:

1) Verbesserung der Effizienz der Kontrollen an den Schengen-Grenzen: Das derzeitige System mit Stempeln zur Ermittlung der Dauer zulässiger Kurzaufenthalte ist umständlich und zeitaufwendig. Mit dem Einreise-/Ausreisesystem entfallen Probleme aufgrund der Uneinheitlichkeit oder Unleserlichkeit von Stempeln in Reisedokumenten sowie aufgrund (möglicher) Betrugsfälle.

2) Bekämpfung der Überziehung der zulässigen Aufenthaltsdauer im Schengen-Raum: Das Einreise-/Ausreisesystem ermöglicht eine automatische Meldung in den Fällen, in denen ein Drittstaatsangehöriger zum Ende seiner zulässigen Aufenthaltsdauer den Schengen-Raum nicht verlassen hat. Das derzeitige Stem-

pelsystem ermöglicht eine Berechnung der zulässigen Aufenthaltsdauer nur auf der Grundlage der Stempel, d. h. an den Schengen-Grenzen oder wenn ein Drittstaatsangehörige aus einem anderen Grund in einem Mitgliedstaat mit Behörden in Kontakt kommt. Wenn eine Person unauffällig bleibt, gibt es keine Möglichkeit festzustellen, dass die Aufenthaltsdauer überzogen wurde. (In Anbetracht der Informationen, die im VIS bereits über Personen registriert sind, die Kurzzeit- oder Transitvisa benötigen, können solche Personen jedoch als echte Minderheit angesehen werden.)

3) Fundierte Politikgestaltung: Durch die Bereitstellung genauerer Daten über Einreisen in die EU, über das Ursprungsland der Reisenden und über Überziehungen der zulässigen Aufenthaltsdauer wird eine bessere Politikgestaltung ermöglicht, beispielsweise für gezieltere neue Visaerleichterungs- und -befreiungsabkommen.

4) Einfachere Rückführungen: Durch das Einreise-/Ausreisesystem sind irreguläre Migranten, deren Daten bei der Einreise im EES erfasst werden, weiterhin für die Zwecke der Rückführung identifizierbar; in dieser Hinsicht ergänzt das EES das VIS. Damit entfällt das Problem, das sich ansonsten ergeben kann, wenn Drittstaatsangehörige nach der Einreise in den Schengen-Raum ihre Reisedokumente vernichten.

1.2 Hintergrund

Die Ziele des EES sind vor dem bestehenden politischen Hintergrund zu bewerten. Bei der Beantwortung der Frage, ob das EES die gesetzten Ziele erreichen kann, ist zu berücksichtigen, dass das EES die EU-Politik für Migration und Mobilität ergänzen soll. Der Hintergrund ist wichtig, weil er Aufschluss über die den Vorschlägen zugrunde liegenden Motivationen und Probleme gibt und weil sich aus der Berücksichtigung des Hintergrundes potenzielle Alternativen ergeben, mit denen ähnliche Ziele erreicht werden könnten. Der wichtigste Aspekt des politischen Hintergrunds ist die Bekämpfung der illegalen (irregulären) Migration und die Notwendigkeit der Förderung politischer Strategien für eine wirksame Rückführung. Ein zweiter politischer Faktor ist das Bedürfnis nach einer fundierteren Politikgestaltung zur Bekämpfung der irregulären Migration und des Menschenhandels sowie nach einer angemessenen Mobilitätspolitik, d. h. nach der Klärung der Frage, in welchen Ländern und Regionen Visumerleichterungen und Visumbefreiungen für den Zugang zur EU gewährt werden sollten.

Bekämpfung der illegalen Migration und wirksame Rückführung

Natürlich bestehen starke politische Motivationen zur Bekämpfung der illegalen Migration, einschließlich der Überziehung der zulässigen Aufenthaltsdauer.

Im Stockholmer Programm[5] sind Prioritäten der Mitgliedstaaten für die Bekämpfung der illegalen Migration und für eine wirksame Rückführung festgelegt. Die Mitgliedstaaten messen der Einrichtung des EES zur Ergänzung bestehender Systeme für die integrierte Grenzverwaltung unter Einhaltung der Datenschutzregelungen hohe Priorität zu. Ähnliche Schwerpunkte verfolgt der „Fahrplan" zur Bekämpfung illegaler Migration, der im Dokument „EU-Aktion gegen Migrationsdruck – Eine strategische Antwort"[6] der dänischen Ratspräsidentschaft vereinbart wurde.

Hinsichtlich der Bekämpfung der illegalen Migration betont das Stockholmer Programm die Bedeutung einer wirksamen Rückführung. Das EES sollte auch im Zusammenhang mit der Rückübernahmepolitik der EU und mit den allgemeinen Problemen bei der Durchführung von Rückführungsentscheidungen untersucht werden. 2010 wurden auf insgesamt 540 000 Ausweisungsanordnungen hin 226 000 Rückführungen wirksam durchgeführt.[7]

Fundierte Politikgestaltung

Eines der Ziele des EES besteht darin, Fakten für die Entscheidungsfindung im Zusammenhang mit der Mobilitätspolitik der EU bereitzustellen, d. h. im Hinblick auf eine Öffnung der EU für die visumfreie Einreise aus weiteren Drittstaaten.

Im VIS werden ähnliche statistische Daten in Bezug auf Personen verfügbar sein, die Schengen-Visa beantragen oder Inhaber von Schengen-Visa sind.

Die Rolle, die das EES in einem solchen Vorhaben spielen kann, ist auch im Kontext und im Vergleich mit der Hauptmethodik der EU bei einschlägigen Entscheidungen zu betrachten – dem Gesamtansatz für Migration und Mobilität (GAMM)[8]. Der GAMM stellt einen Rahmen und spezifische operative Werkzeuge (insbesondere die Mobilitätspartnerschaft) bereit, um Drittstaaten in Überlegungen in den Bereichen Steuerung der Migration, Rückführung/Rückübernahme, Kapazitätsaufbau zur Steuerung von Migrationsströmen, Förderung spezifischer rechtmäßiger Migrationskanäle oder Bewertung des potenziellen Kandidatenstatus für verbesserte Chancen im Hinblick auf eine Mobilität in Richtung der EU einzubeziehen.

---

[5] *Das Stockholmer Programm – ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger*, ABl. 2010/C/115/01, Abschnitte 5.1 und 6.1.6.

[6] *EU-Aktion gegen Migrationsdruck – Eine strategische Antwort*, Ratsdokument 8714/12.

[7] Mitteilung der Kommission an das Europäische Parlament und den Rat – Intelligente Grenzen: Optionen und weiteres Vorgehen, KOM(2011) 680 endgültig, S. 4.

[8] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – *Gesamtansatz für Migration und Mobilität*, KOM(2011) 743 endgültig.

2. Prüfung der Notwendigkeit

Frage 1: Ist das EES geeignet, seine rechtmäßigen Ziele zu erreichen?

2.1 Ziel: höhere Effizienz bei der Grenzabfertigung

Die Kommission hat argumentiert, dass das EES zu einer effizienteren Grenzabfertigung führen würde; Kontrollen würden erleichtert, wenn vielfältige Stempel durch konsistente Einträge in einer Datenbank ersetzt würden. Da dies nur dann zutrifft, wenn die Daten der jeweiligen Person nicht ohnehin im SIS oder im VIS gespeichert sind (d. h. in Datenbanken, auf die Grenzschutzbeamte bei Grenzkontrollen routinemäßig und einfach Zugriff haben), ist fraglich, dass die Abfertigung von Warteschlangen dadurch beschleunigt würde, insbesondere da die Grenzschutzbeamten bei der ersten Einreise einer Person in den Schengen-Raum zunächst umfangreiche Daten in das System eingeben müssten.

Ferner wurde argumentiert, dass das EES eine einheitliche Methode für die Berechnung einer kurzen Aufenthaltsdauer bereitstellen würde und dass die Berechnung daher nicht mehr aufgrund unterschiedlicher Einreisestempel erfolgen müsse. Infolge der einheitlichen Einträge im EES entfielen Zweifelsfälle, die sich angesichts einer Vielzahl verschiedener – zum Teil unleserlicher – Einreisestempel ergeben könnten. Außerdem würden Stempelfälschungen bekämpft. Es stellt sich allerdings die Frage, warum das VIS nicht stärker auch für diesen Zweck eingesetzt werden sollte. Die Nützlichkeit einheitlicher zentraler Einträge wäre natürlich von der Datenqualität abhängig, d. h. davon, dass zunächst korrekte Daten in das System eingegeben werden und dass die Daten am Ende der Speicherfrist oder nach etwaigen Änderungen der Gegebenheiten bei den Reisenden gelöscht würden.

2.2 Ziel: Bekämpfung der Überziehung der zulässigen Aufenthaltsdauer

i. Notwendigkeit wirksamer Ausreisekontrollen, um unberechtigte Meldungen einer Überziehung der zulässigen Aufenthaltsdauer zu vermeiden

Die Datenschutzgruppe möchte betonen, dass das Einreise-/Ausreisesystem eine einwandfrei funktionierende Ausreisekomponente umfassen muss, um wirksamer gegen Überziehungen der zulässigen Aufenthaltsdauer vorgehen zu können. Wenn die Ausreisekontrollen nicht vollständig und korrekt protokolliert werden, stellt das System unberechtigterweise eine Überziehung der zulässigen Aufenthaltsdauer fest. Entsprechend können unbescholtene Reisende grundlos verfolgt werden. Dies ist insbesondere an den Landgrenzen wichtig, an denen Ausreisekontrollen aufgrund der Menge und der Vielzahl der genutzten Verkehrsmittel anscheinend problematisch sind. Gemäß dem Stockholmer Programm sollte bei

der Einführung eines EES „[b]esondere Aufmerksamkeit […] auf die Landgrenzen gerichtet werden, und vor der Anwendung sollten die Auswirkungen auf die Infrastruktur und die Grenzen analysiert werden“;[9] dies lässt darauf schließen, dass bekannt ist, dass die Schaffung eines wirksam funktionierenden Systems an Landgrenzen für das Funktionieren des Systems entscheidend ist und mit großen Herausforderungen verbunden sein kann.

Die Datenschutzgruppe merkt an, dass es anscheinend keine internationalen Beispiele für vergleichbare Ausreisekontrollsysteme gibt, die an Landgrenzen eingesetzt werden. In der Folgenabschätzung der Kommission wird auf die Probleme bei der Einführung der Ausreisekomponente des amerikanischen Programms VISIT verwiesen. In diesem Zusammenhang wird festgestellt: „Das amerikanische Department of Homeland Security (DHS, Ministerium für Innere Sicherheit) hat angegeben, dass die Einführung der Technologie aufgrund der hohen Kosten, des hohen Personalbedarfs und der Zahl der Möglichkeiten, aus den Vereinigten Staaten auszureisen, insbesondere über die Landgrenzen, noch mehrere Jahre erfordern wird.“[10] Die Kommission hält dieser Argumentation in der Folgenabschätzung entgegen, dass derartige Einführungsprobleme im Schengen-Raum nicht auftreten würden, da „an allen Grenzkontrollstellen in beiden Richtungen eine vollständige und ausgereifte Architektur besteht und ausreichende personelle Ressourcen verfügbar sind.“[11] Diese Einschätzung steht im Widerspruch zu Bedenken, die zuvor im Stockholmer Programm formuliert wurden, und offenbar liegen der Kommission keine Nachweise vor, die den wirksamen Einsatz eines Ausreisekontrollsystems vergleichbarer Größe und Struktur an einer Landgrenze belegen würden.

ii. Ausmaß des Problems der Überziehung der zulässigen Aufenthaltsdauer

Das Ausmaß der tatsächlichen Überziehung der zulässigen Aufenthaltsdauer, das mit dem EES möglicherweise bekämpft werden kann, muss ebenfalls in Frage gestellt werden.

In der Folgenabschätzung wird angemerkt, dass „allgemeine Übereinstimmung darüber besteht“[12], dass das größte Risiko einer Überziehung der zulässigen Aufenthaltsdauer bei Personen gegeben ist, die für einen Kurzaufenthalt rechtmäßig zugelassen sind. Im Zusammenhang mit der Bekämpfung der Überziehung der zulässigen Aufenthaltsdauer ist anzumerken, dass alle Informationen zum Visumstatus visumpflichtiger Drittstaatsangehöriger sowie Fingerabdrücke und sonsti-

[9] *Das Stockholmer Programm*, ABl. 2010/C/115/01, Abschnitt 5.1, C/115/27.

[10] Impact Assessment accompanying the document *Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, SWD(2013) 47 final, S. 14.

[11] Ebenda, S. 15.

[12] Ebenda, S. 13.

ge Informationen gemäß der VIS-Verordnung und nach dem Grenzkodex bereits im VIS vorhanden sind und dass Grenzschutzbeamte und viele andere Behörden (Einwanderungsbehörden, Asylbehörden und Behörden, die für Kontrollen von Ausländern im Hoheitsgebiet zuständig sind) routinemäßig auf das VIS zugreifen.

Das EES beschränkt sich per Definition zwangsläufig auf Kurzaufenthalte. Aber Besucher mit kurzer Aufenthaltsdauer sind natürlich nicht die einzigen Drittstaatsangehörigen, die die Schengen-Grenzen überschreiten. Insoweit ist festzustellen, dass Drittstaatsangehörige, die Berechtigte gemäß der Richtlinie 2004/38/EG und Inhaber der entsprechenden Aufenthaltskarte sind, sowie Inhaber von Aufenthaltskarten, die unter die Ausnahmebestimmung von Artikel 2 Absatz 15 des Schengener Grenzkodex fallen, vom Anwendungsbereich des Systems ausgenommen sind.

Stellen Personen, die für einen langen Aufenthalt zugelassen sind, kein Risiko für eine Überziehung der zugelassenen Aufenthaltsdauer dar? Es besteht die Gefahr einer allgemeinen Annahme, dass „hochwertige" Migranten wie Inhaber einer „Blue Card" oder Forscher kein Einwanderungsrisiko darstellen. Studenten gehören jedoch ebenfalls der Kategorie der Ausländer mit langem Aufenthalt an und werden hinsichtlich der Überziehung der zugelassenen Aufenthaltsdauer häufig als Risiko eingestuft.

Eine Überziehung der zugelassenen Aufenthaltsdauer kann auch eine Folge des Missbrauchs abgeleiteter Rechte gemäß der Richtlinie 2004/38/EG sein. Drittstaatsangehörige, die ihren Anspruch auf abgeleitete Rechte verlieren, beispielsweise durch Beendigung der Beziehung mit dem betreffenden EU-Bürger nach einer kurzen Zeit, können eigentlich nur ermittelt werden, wenn sie ihre Aufenthaltskarte zurückgeben.

Die Datenschutzgruppe möchte sich nicht dafür aussprechen, dass Drittstaatsangehörige dieser Kategorien ebenfalls durch eine umfangreiche Datenbank erfasst werden sollen. Diese Beispiele wurden angeführt, um zu verdeutlichen, dass das Problem der Überziehung der zulässigen Aufenthaltsdauer so umfassend sein könnte, dass es durch das EES nicht zu bewältigen wäre. Das EES wäre nur ein Element für die Bewältigung dieses Gesamtproblems.

iii. Das Problem der Überziehung der zulässigen Aufenthaltsdauer wird durch die Ermittlung einer solchen Überziehung nicht gelöst

Die Datenschutzgruppe möchte zudem betonen, dass die Ermittlung einer Überziehung der zulässigen Aufenthaltsdauer keinen Selbstzweck darstellt. Das EES kann für sich genommen die Überziehung der zulässigen Aufenthaltsdauer nicht unterbinden. Personen, die vorsätzlich die zulässige Aufenthaltsdauer überziehen,

werden möglicherweise durch das höhere Aufdeckungsrisiko abgeschreckt. Diese abschreckende Wirkung wird jedoch durch die fehlenden Begleitmaßnahmen zur Ergreifung solcher Personen geschwächt. Es besteht ein größeres Risiko, dass unbescholtene Reisende durch Meldungen einer Überziehung der zulässigen Aufenthaltsdauer im EES unverhältnismäßig beeinträchtigt werden – beispielsweise durch die Verlängerung der Speicherfrist oder die Notwendigkeit, Daten löschen zu lassen, wie in Teil II dieser Stellungnahme erörtert.

2.3 Ziel: Unterstützung der wirksamen Rückführung

Das EES wird die Identifizierung der irregulären Migranten erleichtern, die ihre Reisedokumente vernichten und durch das VIS nicht identifiziert werden können. Dies wirft zwei Fragen auf. Erstens: Wie viel wird das EES zur Überprüfung der Identität beitragen, wenn das VIS für die Durchführung dieser Funktion für Inhaber von Schengen-Visa bereits vorhanden ist? Das EES wird zur Überprüfung der Identität von irregulären Migranten beitragen, die nicht visumpflichtig waren. Da bei Ländern mit Visumbefreiung ein geringeres Einwanderungsrisiko gesehen wird, ist fraglich, wie viele EES-Einträge tatsächlich für die Identitätsüberprüfung von potenziell rückgeführten Personen benötigt werden.

Der Beitrag des EES zur Identitätsüberprüfung kann die Rückübernahmeproblematik nur teilweise lösen. Es ist nicht garantiert, dass eine Person, deren Identität überprüft wurde, von dem Drittland tatsächlich akzeptiert wird.[13] Es liegen nur wenige zuverlässige Daten darüber vor, wie viele Rückführungen über die EU-Rückübernahmeabkommen erreicht werden. Die von der Kommission für die Evaluierung der Rückübernahmeabkommen durchgeführte Erhebung ergab eine Bewilligungsquote zwischen 50 % und 80 % für Anträge auf Rückübernahme eigener Staatsangehöriger. Dem Bericht zufolge lassen sich jedoch keine zuverlässigen Rückschlüsse auf die tatsächliche Zahl der Rückführungen ziehen.[14] Wenn bei den EU-Rückübernahmeabkommen eine Diskrepanz zwischen der Bewilligungsquote und den tatsächlichen Rückführungen besteht, dürfte die Situation bei bilateralen Vereinbarungen noch viel unberechenbarer sein. Wie in dieser Stellungnahme bereits weiter oben festgestellt, besteht in der EU eine große Diskrepanz zwischen Ausweisungsanordnungen und durchgeführten Rückführungen. Und wie die Datenschutzgruppe schon in ihrem Schreiben zur Mitteilung über intelligente Grenzen angemerkt hat, lässt dies anscheinend darauf schließen, dass ein allgemeines Problem eher bei der tatsächlichen Rückführung illegaler Migranten (einschließlich Overstayern) besteht als bei der Identifizierung dieser Migranten. Selbst wenn man berücksichtigt, dass einige Rückführungen aus Gründen der Nichtzurückweisung oder aus sonstigen Menschenrechtsgrün-

[13] Anmerkung des Meijers-Ausschusses in der Stellungnahme zu intelligenten Grenzen, Ref.: CM1307, S. 2.

[14] Mitteilung der Kommission an das Europäische Parlament und den Rat – Evaluierung der EU-Rückübernahmeabkommen, KOM(2011) 76 endgültig, S. 5.

den nicht durchgeführt werden können, ist diese Diskrepanz zu groß, als dass sie ausschließlich auf ein Problem der Identitätsüberprüfung zurückgeführt werden könnte. Es wird davor gewarnt, das EES als Lösung für Probleme bei der Rückführung nicht identifizierter Overstayer zu betrachten.

2.4 Ziel: Bessere Datenlage für fundierte Politikgestaltung

Es würden zwar gewisse nützliche Daten über Migrationsströme gewonnen. Vergleichbare Daten über visumpflichtige Drittstaatsangehörige werden aber auch aus dem VIS verfügbar sein.

Frage 2: Ist ein EES – gemessen an seinen Auswirkungen auf Grundrechte (u. a. das Recht auf Datenschutz und das Recht auf Privatsphäre) – notwendig, um diese rechtmäßigen Ziele zu erreichen?

Nach der Analyse im Zusammenhang mit Frage 1 erscheint zweifelhaft, dass das EES die erhoffte Wirksamkeit bei der Erreichung der erklärten Ziele haben kann. Doch selbst wenn das EES einen wesentlichen Mehrwert bieten würde, fragt sich aus rechtlicher Sicht, ob dies die Verletzung der Privatsphäre gemäß Artikel 8 der EU-Charta rechtfertigen könnte. Die Datenschutzgruppe vertritt nachdrücklich die Ansicht, dass der Mehrwert des EES im Hinblick auf die Erreichung seiner Ziele die Anforderung der Notwendigkeit nicht erfüllt und dass die entsprechende Beeinträchtigung bestehender Rechte gemäß Artikel 8 der EU-Charta nicht gerechtfertigt wäre. Sie ist ferner der Auffassung, dass der Mehrwert des EES in Bezug auf die einzelnen Ziele nicht im Verhältnis zum Ausmaß seiner Auswirkungen auf die Grundrechte steht. Diese Auffassung wird im Folgenden erläutert:

Höhere Effizienz bei der Grenzabfertigung: Es besteht ein Mehrwert in der Einheitlichkeit der Einreise-/Ausreisedaten. Dieser Mehrwert hängt jedoch von der Qualität der Daten im System ab.

Eine Datenbank mit schlechter Datenqualität geht für unbescholtene Reisende mit einem sehr hohen Risiko unverhältnismäßiger Sanktionen einher. Zudem ist es offensichtlich unverhältnismäßig, eine umfangreiche Datenbank mit personenbezogenen Daten zu erstellen, nur um Warteschlangen schneller abfertigen zu können.

Die Kosten des EES (Entwicklungskosten von 183 Mio. EUR und jährliche Betriebskosten von 88 Mio. EUR – zusätzlich zu den Betriebskosten anderer Systeme wie z. B. SIS II und VIS) sind ein Faktor, der bei den Überlegungen zu den Vorteilen einer schnelleren Grenzabfertigung ebenfalls berücksichtigt werden sollte. Sind Investitionen auf dieser Ebene wirklich kosteneffizient?

Mögliche Bekämpfung der Überziehung der zulässigen Aufenthaltsdauer: Ein gewisser Mehrwert besteht darin, dass Informationen über die Anwesenheit von Overstayern im Schengen-Raum durch das EES leichter verfügbar sind. Dieser Mehrwert wird jedoch erheblich dadurch beeinträchtigt, dass das EES das Problem nicht in vollem Umfang angehen kann. Noch gravierender fällt ins Gewicht, dass die reine Ermittlung einer Überziehung der zulässigen Aufenthaltsdauer noch kein Mittel für die Ergreifung der Overstayer darstellt. Die Auswirkungen einer Einführung dieses zusätzlichen Instruments sind für sich genommen nicht hinreichend, um die geforderte Notwendigkeit feststellen zu können.

Zudem hat die Datenschutzgruppe ernsthafte Bedenken dahin gehend, dass unberechtigte oder unverhältnismäßige Einreiseverbote ausgesprochen werden könnten, weil das EES Überziehungen der zulässigen Aufenthaltsdauer meldet. Die Gruppe begrüßt, dass in der Folgenabschätzung eingeräumt wird: „Wenn das Einreise-/Ausreisesystem eine Überziehung der zulässigen Aufenthaltsdauer meldet, sollte dies für den Drittstaatsangehörigen nicht automatisch zu einer Verhaftung, einer Rückführung oder einer Sanktion führen."[15] Die Datenschutzgruppe betont, dass Einreiseverbote oder Ausweisungsanordnungen stets auf einer individuellen Bewertung aller Umstände eines Falles beruhen müssen und dass ein wirksamer Rechtsbehelf verfügbar sein sollte.

Überprüfung der Identität irregulärer Migranten und Unterstützung einer wirksamen Rückführung: Ein gewisser Mehrwert besteht in den Daten, die das EES für die Identifizierung irregulärer Migranten bereitstellt. Dieser Mehrwert wird jedoch stark dadurch beeinträchtigt, dass mit ähnlichen Daten aus dem VIS voraussichtlich eine größere Zahl von Overstayern erfasst ist und dass die Identitätsüberprüfung an sich kein Mittel für eine wirksame Rückführung ist.

Fundierte Politikgestaltung: Die Datenschutzgruppe hält es für unverhältnismäßig, die Einführung einer großen Datenbank mit personenbezogenen Daten damit zu rechtfertigen, dass eines der Ziele die Erstellung besserer statistischer Daten für die Politikgestaltung ist. Für diese Auffassung spricht auch, dass viele ähnliche Daten aus dem VIS verfügbar sein werden und dass der Gesamtansatz für Migration und Mobilität Alternativen für eine informierte Politikgestaltung in diesem Bereich bietet.

Zugang für Strafverfolgungsbehörden und Drittstaaten: Die Datenschutzgruppe stellt fest, dass der Zugang von Strafverfolgungsbehörden auf die Informationen im EES nach zwei Jahren bewertet wird. Eine solche Bewertung würde offensichtlich eine neue Folgenabschätzung unter Berücksichtigung der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit erfordern. Beunruhigend sind

[15] Impact Assessment accompanying the document *Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, SWD(2013) 47 final, S. 19.

jedoch Anzeichen dafür, dass der Vorschlag einen Zugang der Strafverfolgungsinstanzen offenbar ohnehin voraussetzt. Dies ist etwa daraus zu schließen, dass technische Vorbereitungen für den Zugang von Strafverfolgungsbehörden getroffen werden (Erwägungsgrund 11). Wenn von vornherein davon ausgegangen wird, dass die Strafverfolgungsbehörden Zugang erhalten, werden die Eingriffe später umso umfassender sein. Die Datenschutzgruppe wiederholt ihren grundsätzlichen Einwand, dass Strafverfolgungsbehörden nicht routinemäßig Zugriff zu einer Verwaltungsdatenbank erhalten sollten, die personenbezogene Daten unbescholtener Reisender enthält.

Auch aus dem Umstand, dass der Vorschlag der Kommission von vornherein die Verpflichtung zur Abnahme von zehn Fingerabdrücken vorsieht, geht eindeutig hervor, dass die Kommission den Strafverfolgungsbehörden letztlich Zugang gewähren möchte. Zur Identifizierung eines Drittstaatsangehörigen zu Zwecken der Ein- oder Ausreise oder zur Identifizierung auf der Straße bei Zweifeln hinsichtlich einer Überziehung der zulässigen Aufenthaltsdauer wären maximal vier Fingerabdrücke (zwei von jeder Hand, ähnlich dem in europäischen Ländern verwendeten ePass) ausreichend. Daher entspricht der Vorschlag der Kommission nicht den Anforderungen der Grundsätze der Datenminimierung und des eingebauten Datenschutzes (Privacy by Design) – die die Kommission im Rahmen der laufenden Datenschutzreform selbst befürwortet. Der einzige vorstellbare Grund dafür, von vornherein zehn Fingerabdrücke von Drittstaatsangehörigen zu erfassen und zu speichern, besteht in der Erstellung einer Datenbank, die dafür geeignet ist, nach Fingerabdrücken zu suchen, wenn ein Drittstaatsangehöriger nicht persönlich anwesend ist (d. h. für Zwecke der Strafverfolgung).

Frage 3: Sind bereits bestehende Alternativen verfügbar, mit denen die gleichen rechtmäßigen Ziele ohne die gleichen Auswirkungen auf Grundrechte (u. a. das Recht auf Datenschutz und auf Privatsphäre) erreicht werden können?

Für die Auffassung, dass das EES die Anforderung der Notwendigkeit nicht erfüllen kann, spricht auch, dass Alternativen zur Erreichung der erklärten Ziele bestehen. Aus dem Abschnitt über den politischen Kontext in dieser Stellungnahme geht hervor, dass ein EES nur ein einzelnes Werkzeug aus einem breiten Spektrum von Ansätzen zur Bekämpfung illegaler Migration sein kann.

In der Folgenabschätzung der Kommission heißt es: „Für eine Verringerung der Zahl der Overstayer oder im Hinblick auf Möglichkeiten zur Identifizierung oder Ermittlung von Overstayern sind auch andere Initiativen zur Bekämpfung der irregulären Migration […] nicht von Bedeutung.“[16] Dies bezog sich direkt auf das

[16] Ebenda, S. 21.

Ratsdokument „EU-Aktion gegen Migrationsdruck – Eine strategische Antwort", aber selbst in diesem engen Kontext muss diese Aussage als politische Meinungsäußerung hinterfragt werden.

Mit dem EES würden einige Fälle ermittelt, in denen die zulässige Aufenthaltsdauer überzogen wurde; die dieser Problematik zugrunde liegenden Ursachen würden jedoch nicht bekämpft. Das System verfügt für sich genommen über keinerlei Mittel zur Verringerung der Zahl der Overstayer; es hat bestenfalls eine leichte abschreckende Wirkung. Andererseits bestehen bereits Instrumente, die in ganzheitlicher Weise zur Bekämpfung der Überziehung der zulässigen Aufenthaltsdauer eingesetzt werden.

Die Richtlinie über Sanktionen gegen Arbeitgeber illegaler Migranten[17] ist ein solches Instrument. Die illegale Beschäftigung ist als ein Faktor bekannt, der illegale Migration fördert, und Overstayer werden aufgrund ihres mangelnden Rechtsstatus zwangsläufig illegal beschäftigt. Die Richtlinie über Sanktionen gegen Arbeitgeber illegaler Migranten stellt einen Mechanismus zur Bekämpfung des illegalen Beschäftigungssektors bereit und bietet außerdem einen Rahmen, in dem Mitgliedstaaten Kontrollen bei Arbeitgebern durchführen können, die im Verdacht stehen, illegale Migranten zu beschäftigen. Insoweit ist eine Möglichkeit gegeben, Overstayer ausfindig zu machen.

Anstrengungen zum Ausbau legaler Migrationsrouten in die Europäische Union bieten ebenfalls eine Alternative zur illegalen Überziehung der zulässigen Aufenthaltsdauer. Informations- und Sensibilisierungswerkzeuge wie das Einwanderungsportal können potenziellen Migranten helfen, die echten Chancen und Herausforderungen in Verbindung mit einer Migration in die EU zu verstehen. Außerdem können sie Alternativen zu einer Überziehung der zulässigen Aufenthaltsdauer aufzeigen. Durch die Förderung einer freiwilligen Rückführung und durch Reintegrationsprojekte erhalten einige Overstayer, die in ihre Heimat zurückkehren möchten, eine realistische Option. Alle diese politischen Initiativen berücksichtigen den umfassenderen Hintergrund der Überziehung der zulässigen Aufenthaltsdauer und funktionieren ohne ein EES.

Die Datenschutzgruppe ist der Auffassung, dass der Gesamtansatz für Migration und Mobilität einen politischen Rahmen und praktische Werkzeuge für die Erreichung einiger der erklärten politischen Ziele des EES bietet, insbesondere für die Notwendigkeit einer fundierten Politikgestaltung. Eine fundierte Politikgestaltung kann durch die geografischen Prioritäten und Werkzeuge des GAMM erreicht werden. Wie können Daten eines EES die Politikgestaltung beeinflussen, wenn auf politischer Ebene bereits beschlossen wurde, die Partnerschaftsanstren-

[17] Richtlinie 2009/52/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über Mindeststandards für Sanktionen und Maßnahmen gegen Arbeitgeber, die Drittstaatsangehörige ohne rechtmäßigen Aufenthalt beschäftigen, ABl. L/168/24.

gungen in der ersten Phase durch die Mobilitätspartnerschaft auf europäische Nachbarländer zu konzentrieren und weiter entfernt liegende Schwerpunktländer gleichzeitig über das Werkzeug des GAMM im Auge zu behalten? Aufgrund der operativen Erfahrungen von Mobilitätspartnerschaften oder infolge politischer Dialoge im Rahmen des GAMM eröffnet der GAMM auch die Möglichkeit, die Eignung und die Bereitschaft eines Landes zur Übernahme der Verantwortung für eine Visumbefreiung viel fundierter zu bewerten.

Die Datenschutzgruppe hat den Eindruck, dass es viel aussichtsreichere Alternativen zur Verhinderung der Überziehung einer zulässigen Aufenthaltsdauer und zur Gestaltung der EU-Politik im Hinblick auf eine Visumliberalisierung gibt als die Erfassung von Reisenden in einem EES. Insbesondere wird ein erheblicher Teil der ermittelten Probleme offenbar bereits durch das VIS bekämpft. Insoweit ist festzustellen, dass bestehende Alternativen wie das VIS nicht vollständig genutzt werden.

Die Datenschutzgruppe akzeptiert, dass die bestehende Problematik durch die einzelnen Alternativen möglicherweise nicht vollständig gelöst wird. Sie ist angesichts der vorstehend erläuterten Analyse jedoch der Ansicht, dass das EES keine verhältnismäßige oder legitime Reaktion zur Erreichung der identifizierten Ziele darstellt.

Teil II: Spezifische Datenschutzbelange hinsichtlich EES und RTP

Erfassung biometrischer Daten

Die Erfassung biometrischer Daten ist im EES-Vorschlag von vornherein fest vorgesehen und wird nicht nach einem bestimmten Zeitraum neu bewertet. Es ist enttäuschend, dass die Erfassung biometrischer Daten keiner Bewertung unterzogen wird. Wie bereits in ihrem Schreiben an Kommissarin Malmström angemerkt, ist die Datenschutzgruppe der Ansicht, dass biometrische Daten erst nach einer Bewertung des Systems erfasst werden sollten. Diese Bewertung sollte durchgeführt werden, nachdem das System einige Jahre lang in Betrieb war, und könnte eine faktische Grundlage für die Entscheidung bilden, ob die Ziele auch ohne die Erfassung biometrischer Daten erreicht werden könnten.

Artikel 20: Speicherfrist

Die Datenschutzgruppe betont, dass die Daten so lange gespeichert werden sollten, wie für die Erreichung eines rechtmäßigen Zweckes erforderlich. Daher werden die EES-Einträge im Allgemeinen sechs Monate lang gespeichert. (Dies ist der maximale Zeitraum, in dem ein Drittstaatsangehöriger für einen Kurzaufent-

halt von bis zu 90 Tagen einreisen kann.) Bei Overstayern beträgt die Speicherfrist fünf Jahre. Es werden keine Belege für die Notwendigkeit dieser Verlängerung der Speicherfrist angeführt. Eine pauschale Speicherfrist von fünf Jahren für Overstayer ist unverhältnismäßig.

Artikel 21: Bestimmung zur Löschung von Daten

Nach dieser Bestimmung liegt die Beweislast für die Beschaffung und Vorlage von Nachweisen zur Löschung von Daten oder Meldungen von Overstayern aus dem EES bei der betroffenen Person, wenn sie zwischenzeitlich eine Aufenthaltsberechtigung erworben hat, wenn sie durch ein unvorhersehbares Ereignis gezwungen war, die Aufenthaltsdauer zu verlängern, oder wenn die Daten fehlerhaft sind. Insbesondere wenn die betroffene Person eine Aufenthaltsberechtigung im Rahmen eines anderen nationalen Programms, einer EU-Richtlinie oder der Richtlinie 2004/38/EG erworben hat, ist ihr möglicherweise nicht bewusst, dass sie die Löschung der Daten aus dem EES beantragen muss. Derartige Änderungen der Gegebenheiten könnten häufig vorkommen und zu erheblichen Problemen in Form unberechtigter Meldungen führen. Es ist ratsam, dass die betroffene Person zu dem Zeitpunkt, zu dem sie die alternative Aufenthaltsberechtigung für den Mitgliedstaat erwirbt, durch einen geeigneten Mechanismus über diese Anforderung informiert wird. Der Vorschlag sollte um einen Erwägungsgrund erweitert werden, durch den die Mitgliedstaaten auf diese Problematik aufmerksam gemacht werden.

Die vorgeschlagene Regelung könnte im Fall von Drittstaatsangehörigen, die eine Aufenthaltsgenehmigung gemäß der Richtlinie 2004/38/EG beantragen, ein schwerwiegendes Problem darstellen. Diese Personen sind derzeit verpflichtet, ihren Reisepass gemäß dem Schengener Grenzkodex abstempeln zu lassen, bis sie im Rahmen der Richtlinie eine Aufenthaltskarte erhalten. Diese Drittstaatsangehörigen werden infolgedessen im EES auf der gleichen Grundlage erfasst wie andere Reisende. Dies kann jedoch Folgen haben, die weit über die Erfassung von Stempeln im Reisepass der betreffenden Personen hinausgehen können (einschließlich der unberechtigten Meldung einer Überziehung der zulässigen Aufenthaltsdauer und einer Speicherung über einen Zeitraum von fünf Jahren). Wenn dem Antrag dieser Personen auf eine Aufenthaltskarte später stattgegeben wird, müssen die Daten im EES gelöscht werden, wobei die Verpflichtung für eine entsprechende Antragsstellung bei den Drittstaatsangehörigen liegt. Da die Berechtigten gemäß der Richtlinie 2004/38/EG einen Sonderstatus besitzen, der – wie die Kommission bereits anerkannt hat[18] – geschützt werden muss, möchte

[18] Impact Assessment accompanying the document *Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, SWD(2013) 47 final, S. 19 – Die Maßnahmen zum Schutz der Rechte von Reisenden – einschließlich des Rechts auf einen wirksamen Rechtsbehelf – müssen die privilegierte Stellung von Nicht-EU-Familienangehörigen von EU-Bürgern berücksichtigen, deren Recht auf Einreise und Aufenthalt gemäß der Richtlinie 2004/38/EG vom Recht des jeweiligen EU-Bürgers abhängt.

die Datenschutzgruppe insbesondere darauf hinweisen, dass diese Gruppe von unberechtigten Meldungen einer Überziehung der zulässigen Aufenthaltsdauer unverhältnismäßig betroffen sein kann.

Artikel 27: Übermittlung von Daten an Drittstaaten im Rahmen einer Rückübernahme

Der Meijers-Ausschuss hat bereits Bedenken hinsichtlich der „umfassenden Ermessensbefugnisse der nationalen Behörden der Mitgliedstaaten in Bezug auf die Übermittlung personenbezogener Daten aus dem EES an Drittstaaten“[19] im Kontext der Rückübernahme gemäß Artikel 27 der vorgeschlagenen Verordnung geäußert. Einer der Gründe für eine Übermittlung ist Artikel 26 Absatz 1 Buchstabe d der Richtlinie 95/46/EG. Es ist fraglich, ob die Rückführung eines Overstayers „für die Wahrung eines wichtigen öffentlichen Interesses […] erforderlich“ ist und ob die Übermittlung von EES-Daten für die Erreichung dieses Ziels verhältnismäßig ist. Es muss noch weiter geklärt werden, welche Schutzmechanismen bestehen, wenn Daten an Drittstaaten mit offensichtlich unzureichenden Datenschutzstandards übermittelt werden. Außerdem ist anzumerken, dass in der Erklärung der Kommission für das Ratsprotokoll bei der Annahme der Schlussfolgerungen des Rates zur Rückübernahme anerkannt wird, dass „die EU-Rückübernahmeabkommen im Einklang mit der Grundrechtecharta durchzuführen sind“.[20] Welche Schutzmechanismen bestehen, um sicherzustellen, dass die Behörden der Mitgliedstaaten diesen Anforderungen entsprechen?

Eine ähnliche Bestimmung ist in Artikel 31 der VIS-Verordnung enthalten. Es wäre ratsam, abzuwarten, wie diese Bestimmung in der Praxis umgesetzt wird.

Spezifische Schutzmechanismen

Die Datenschutzgruppe merkt an, dass keine spezifischen Schutzmechanismen angestrebt wurden, obwohl ein offensichtlicher Bedarf besteht: Die EES-Architektur sieht in Artikel 19 vor, dass alle einzelnen Nutzer einen Zugang zur zentralen Datenbank mit Daten aller Drittstaatsangehörigen haben, die für einen Kurzaufenthalt im Schengen-Raum zugelassen wurden. Wenn der Grundsatz „Kenntnis nur wenn nötig“ angewandt würde, wäre als Voraussetzung für die Konsultation personenbezogener Daten im EES entweder erforderlich, dass die betroffene Person in der Liste der identifizierten Overstayer enthalten ist (Artikel 10 Absatz 2) oder dass die Behörde mit einem für einen Kurzaufenthalt im Schengen-Raum zugelassenen Drittstaatsangehörigen in direktem Kontakt steht. Die Datenschutzgruppe vertritt die Ansicht, dass angesichts der verfügbaren Ressourcen der Aufsichtsbehörden (Artikel 37 und 38) oder der tatsächlichen Mög-

[19] Stellungnahme des Meijers-Ausschusses zu den Vorschlägen für intelligente Grenzen, CM 1307, S. 4.

[20] Ratsdokument 11260/11, Anhang II.

lichkeit, die gemäß Artikel 30 geführten Aufzeichnungen zu kontrollieren, Bestimmungen zu spezifischen Datenschutzmechanismen für das EES und für das RTP eingeführt werden sollten.

Begriffsbestimmungen

Die Datenschutzgruppe hat Bedenken hinsichtlich der folgenden Begriffsbestimmungen im EES-Vorschlag:

Ein „Overstayer" ist definiert als Person, die „die Bedingungen für den Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten nicht oder nicht mehr erfüllt". Die Formulierung „nicht […] erfüllt" kann so ausgelegt werden, dass sie einen illegalen Migranten bezeichnet und nicht einen Overstayer. Ein „Overstayer" sollte definiert werden als eine Person, die „die Bedingungen für den Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten nicht mehr erfüllt".

„Biometrische Daten" sind als Fingerabdruckdaten definiert.

Die Definitionen der Begriffe „Identifizierung" (1:n-Abgleich) und „Verifizierung" (1:1-Abgleich) sind nur in Bezug auf Suchabfragen unter Verwendung von Fingerabdruckdaten (oder allgemeinen biometrischen Daten) sinnvoll.

Die Definition des Begriffs „alphanumerische Daten" muss – zumindest in einem Erwägungsgrund – klarstellen und spezifizieren, dass die in Artikel 11 genannten alphanumerischen Daten personenbezogene Daten bezeichnen, insoweit sie Informationen über eine bestimmte oder bestimmbare natürliche Person (die betroffene Person) enthalten, und dass die Begriffsbestimmung gemäß Artikel 2 Buchstabe a der Richtlinie 95/46/EG gilt – mit allen erforderlichen Folgen hinsichtlich der Rechtmäßigkeit der Verarbeitung solcher Daten. Zudem wird vorgeschlagen, nach den Worten „im EES" in der ersten Zeile von Artikel 12 die Formulierung „oder in anderen Systemen wie dem VIS oder dem SIS" hinzuzufügen.

Registrierungsprogramm für Reisende

Die Datenschutzgruppe hat Bedenken, dass eine weitere zentrale biometrische Datenbank eingerichtet würde. Sie ist der Ansicht, dass ein System vorzuziehen wäre, das ausschließlich die biometrischen Daten in Pässen nutzt, um die Erstellung einer weiteren Datenbank zu vermeiden.

Es ist wahrscheinlich, dass auch europäische Bürger in die Datenbank aufgenommen würden. Der Grund dafür wäre, dass die Teilnahme an RTP-Programmen in Drittländern – zumindest derzeit – die Teilnahme an nationalen Programmen erfordert (z. B. das amerikanische Programm „Global Entry"). Daher würde eine biometrische Datenbank europäischer Reisender eingerichtet werden.

Diskriminierungsrisiken

Es sollte sichergestellt werden, dass bei dem RTP transparente Prüfkriterien für die Einstufung von Reisenden mit einem „geringen Risikoprofil" verwendet werden. Die Gefahren der Diskriminierung bei der Unterscheidung zwischen Reisenden mit „geringem" und „hohem Risikoprofil" (die aufgrund dieser Einstufung quasi ohne Beweise als schuldig betrachtet würden) sollten vermieden werden.

Schlussfolgerung

Diese Stellungnahme stellt in Frage, dass das EES seine erklärten Ziele wirksam erreichen kann. Selbst unter der Annahme, dass das EES einen wesentlichen Mehrwert bietet, kommt die Stellungnahme zu dem Schluss, dass der Mehrwert des EES für die Erreichung seiner erklärten Ziele nicht dem Anspruch der Notwendigkeit entspricht, um so die Eingriffe in die Rechte gemäß Artikel 8 der EU-Charta zu rechtfertigen. Des Weiteren ist anzumerken, dass der Mehrwert des EES in Bezug auf die einzelnen Ziele nicht im Verhältnis zum Ausmaß seiner Auswirkungen auf die Grundrechte stehen würde und dass Alternativen für die Erreichung der Ziele verfügbar sind.

Brüssel, den 6. Juni 2013

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

V. Internationale Konferenz der Datenschutzbeauftragten

35. Konferenz vom 23. – 26. September 2013 in Warschau, Polen

Entschließung zur Profilbildung

Nach der Erörterung der Frage zur Profilbildung während der geschlossenen Sitzung auf ihrer 34. Internationalen Konferenz in Uruguay und nach Anhörung verschiedener Experten aus dem öffentlichen und dem privaten Bereich während dieser geschlossenen Sitzung;

In Anerkennung der vielen nützlichen Anwendungen von großen Datenmengen und der Vorteile, die umfangreiche Datensammlungen für unterschiedliche Teile der Gesellschaft, sowohl für Unternehmen und Regierungen als auch für gemeinnützige Organisationen, mit sich bringen könnten;

Unter gleichzeitiger Berücksichtigung, dass die Sammlung personenbezogener Informationen in großen Datenbanken und deren anschließende Nutzung Gefahren für den Schutz personenbezogener Daten und der Privatsphäre darstellen;

In Anbetracht der Tatsache, dass sich die Risiken noch erhöhen, wenn verschiedene Datensätze ohne angemessene Berücksichtigung des Schutzes dieser Daten und des Zwecks, für den sie ursprünglich gesammelt wurden, kombiniert werden;

Unter Hinweis auf die allgemeinen Grundsätze des Datenschutzes und der Privatsphäre;

Unter erneuter Bestätigung der im Jahr 2012 angenommenen Erklärung von Uruguay über die Profilbildung;

fordert die 35. Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre von allen die Profilbildung nutzenden Parteien:

1. Eine klare Bestimmung der Notwendigkeit und des praktischen Nutzens eines bestimmten Profilbildungsvorgangs und die Gewährleistung angemessener Schutzmaßnahmen vor dem Beginn der Profilbildung.

2. Die Begrenzung, im Einklang mit den Grundsätzen des Privacy-by-Design, der Vermutung und der Menge der gesammelten Daten auf das für den beabsichtigten rechtmäßigen Zweck erforderliche Maß, und die Gewährleistung, soweit angemessen, dass die Daten für den vorgesehenen Zweck hinreichend auf dem neuesten Stand und korrekt sind.

3. Die Gewährleistung, dass die Profile und die zugrunde liegenden Algorithmen einer ständigen Überprüfung unterliegen, um eine Verbesserung der Ergebnisse und die Verringerung falsch-positiver oder falsch-negativer Ergebnisse zu ermöglichen;

4. Die möglichst umfassende Unterrichtung der Gesellschaft über Profilbildungsvorgänge, einschließlich der Art und Weise, wie Profile zusammengeführt werden und der Zwecke, für die Profile genutzt werden, womit sichergestellt werden soll, dass die Einzelnen in der Lage sind, so weit wie möglich und so weit es angemessen ist, die Kontrolle über ihre eigenen personenbezogenen Daten zu behalten.

5. Die Gewährleistung, insbesondere in Bezug auf Entscheidungen, die bedeutende rechtliche Auswirkungen für die Einzelnen haben oder ihre Unterstützung oder ihren Status betreffen, dass die Einzelnen über ihr Recht auf Auskunft und Berichtigung unterrichtet werden und dass, soweit angemessen, menschliche Eingriffe vorgesehen sind, zumal angesichts der Zunahme der Vorhersagekraft von Profilen aufgrund effizienterer Algorithmen.

6. Die Sicherstellung, dass alle Profilbildungsvorgänge einer angemessenen Aufsicht unterliegen.

Außerdem rufen die Datenschutzbeauftragten die Regierungen der ganzen Welt dazu auf, die Offenheit zu gewährleisten und den Beteiligten Gelegenheit zu öffentlichen Stellungnahmen und Beiträgen bei allen Gesetzgebungsverfahren zu geben, die Profilbildungsvorgänge ins Werk setzen könnten.

Entschließung über digitale Bildung für alle

Eingedenk der wichtigsten geltenden internationalen Übereinkommen, von denen sich einige auf die grundlegenden Menschenrechte, den Datenschutz und den Schutz der Privatsphäre beziehen:

– Die Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948 – Artikel 25 und 26-3;

– Die Europäische Konvention zum Schutze der Menschen und Grundfreiheiten vom 4. November 1950 – Artikel 8;

– Die Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 – Artikel 241

– Der Internationale Pakt der Vereinten Nationen über wirtschaftliche, soziale und kulturelle Rechte vom 16. Dezember 1966, – Artikel 17;

– Die Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Europarat, 28 Januar 1981 und das Zusatzprotokoll zur Konvention 108;

– Die OECD-Richtlinien über den Datenschutz;

– Das Memorandum von Montevideo über den digitalen Ausschluss von Jugendlichen;

Eingedenk der internationalen Übereinkommen, die sich unmittelbar auf die Rechte von Kindern beziehen:

– Die Genfer Erklärung der Kinderrechte vom 26. September 1924;

– Die UN-Kinderrechtskonvention vom 20. November 1989;

– Das Europäische Übereinkommen über die Ausübung von Kinderrechten, Europarat, Nr. 160, vom 25. Januar 1996.

Eingedenk der folgenden, auf der 30. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre im Jahr 2008 angenommenen Entschließungen:

– Die Entschließung zum „Datenschutz in sozialen Netzwerkdiensten“;

– Die Entschließung zum „Schutz der Privatsphäre von Kindern im Internet“, die die Beauftragten zur Entwicklung der digitalen Erziehung, insbesondere für die Jüngsten, ermutigt.

Gestützt auf die Entschließung zu „Privacy by Design“, die auf der 32. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre im Jahre 2010 angenommen wurde;

Gestützt auf die „Empfehlung des Rates zum Schutz der Kinder im Internet“ der OECD vom 16. Februar 2012,

Eingedenk der Empfehlung R(2006)12 des Europarates an die Mitgliedstaaten, angenommen am 27. September 2006 durch das Ministerkomitee, zur Befähigung von Kindern zum Umgang mit den neuen Informations- und Kommunikationstechnologien, und der „Erklärung des Ministerkomitees zum Schutz der Würde, Sicherheit und Privatsphäre von Kindern im Internet“, angenommen am 20. Februar 2008;

Gestützt auf den Internationale Pakt der Vereinten Nationen über wirtschaftliche, soziale und kulturelle Rechte vom 16. Dezember 1966, – Artikel 13, der das Recht eines jeden auf Bildung anerkennt;

Eingedenk, dass die digitale Technologie heute zu einem Teil des täglichen Lebens geworden ist und vollständig in jeden Bereich unserer Existenz integriert ist: Soziale Beziehungen, Familie, Freunde, berufliche Tätigkeit, Konsum, kulturelle Aktivitäten, Freizeitaktivitäten; dass all diese Facetten nun mit dem digitalen Universum verwoben sind; dass dieses neue digitale Zeitalter die ganze Bevölkerung betrifft, unabhängig von Alter, Erfahrung und Standort.

In der Erkenntnis der Herausforderung, die Komplexität der digitalen Umgebung zu verstehen, da sich die Informationstechnologie rasch ändert, die an diesem Ecosystem beteiligten Akteure und das auf sie gegründete Geschäftsmodell. Deshalb sind die Nutzer und die politischen Entscheidungsträger nicht in der Lage, alle Risiken und alle Möglichkeiten für Innovation und Wirtschaftswachstum zu verstehen, die diese digitale Technologie bietet.

In der Einsicht, dass die digitale Technologie viele neue Herausforderungen in Bezug auf den Schutz der Daten und der Privatsphäre hervorruft und dass der rechtliche Rahmen allein nicht alle erforderlichen Antworten und Garantien zu geben vermag.

Die auf der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vertretenen Behörden erachten folgendes als dringend notwendig:

– **Die unverzügliche Förderung** des Wissens über die digitale Technologie, um es jedem Bürger, Konsumenten und Unternehmer zu ermöglichen, aktive, kreative und kritische Akteure zu werden, die über hinreichende Kenntnisse und ein ausreichendes Verständnis verfügen, um eine informierte Entscheidung über die Nutzung der von der digitalen Technologie angebotenen Möglichkeiten zu treffen;

– **Zusammenzuarbeiten**, in Verbindung mit allen wichtigen Beteiligten, da es hier um eine gemeinsame Verantwortung geht.

Demzufolge ruft die Entschließung die Mitglieder-Behörden dazu auf, mit allen betroffenen Beteiligten zusammenarbeiten, um:

– Die digitale Kompetenz zu **fördern** und eine Rolle bei der Ausbildung aller betroffenen Teile der Öffentlichkeit zu spielen, jeden Alters, um ihnen folgendes zu ermöglichen:

- Die zur Teilnahme an der digitalen Umgebung notwendigen Kenntnisse zu erwerben;

- Informierte und verantwortliche Akteure in der digitalen Umgebung zu werden; und

- Ihre Rechte wirksam zu nutzen und sich über ihre Pflichten bewusst zu sein.

– Ein gemeinsames Programm über die digitale Ausbildung **anzunehmen**, das auf 5 Grundprinzipien und auf 4 operationellen Zielen beruht.

Grundprinzipien:

1. Minderjährige sind im Hinblick auf die digitale Technologie besonders zu schützen;

2. Lebenslanges Training zum Thema digitale Technologie ist zu fördern;

3. Zwischen den Möglichkeiten und Risiken der digitalen Technologien ist ein angemessener Ausgleich zu suchen;

4. Die Entwicklung guter Bräuche und der Respekt für andere Nutzer sind zu fördern;

5. Kritisches Denken zu Risiken und Vorteilen der digitalen Technologie ist zu fördern.

Operationelle Ziele:

1. Förderung der Ausbildung zum Thema Datenschutz als Teil des Programms zum Erwerb digitaler Kompetenz;

2. Eine Rolle beim Training von Kontaktpersonen zu spielen durch die Organisation des „Trainings der Trainer" zum Schutz der Daten und der Privatsphäre oder hierzu beitragend;

3. Förderung von Berufen im Bereich der digitalen Technologien durch Förderung innovativer Sektoren, vor allem von Sektoren, die „Privacy by Design" entwickeln;

4. Formulierung von Empfehlungen und guten Praktiken zur Nutzung der neuen Technologien für die betroffene Öffentlichkeit (Kinder, Eltern, Lehrer, Unternehmen …).

Eine Arbeitsgruppe zur Umsetzung dieser operationellen Ziele wird eingerichtet.

Erläuternde Anmerkungen

In den letzten Jahren haben viele Datenschutzbehörden, die die wichtigsten regionalen Gebiete der Welt repräsentieren, ihre Erfahrungen ausgetauscht und wichtige Initiativen für das globale Bewusstsein von Kindern, Jugendlichen und im Bildungsbereich für den Datenschutz und die Privatsphäre ergriffen.

Diese Entschließung ist eine Fortsetzung der auf der 30. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre angenommenen Entschließung und zielt darauf ab, noch einen Schritt weiter zu gehen. Diese konkreten Vorschläge zielen auf die Förderung von Wissen über die digitale Technik und die Ausbildung aller betroffenen Teile der Öffentlichkeit, jeden Alters, ab. Dies soll allen Bürgern die Möglichkeit geben, sich zu informieren und verantwortungsvolle Akteure im digitalen Umfeld zu werden, ihre Rechte und Pflichten wirksam zu nutzen und sich über ihre Pflichten in diesem Universum bewusst zu werden. Daher ist eine groß angelegte Aktion erforderlich, die auf alle Teile der Öffentlichkeit abzielt.

Die Datenschutzbehörden könnten sich an ihre jeweiligen Regierungen wenden, um in weitem Umfang Maßnahmen (gesetzgeberischer Art oder in Zusammenarbeit mit allen wichtigen Akteuren, einschließlich der Zivilgesellschaft) auch auf internationaler Ebene zu ergreifen.

Die Datenschutzbehörden verpflichten sich zu langfristigem Handeln und regelmäßiger Bewertung der ergriffenen Maßnahmen, um eine effektive Fortsetzung der Empfehlungen dieser Entschließung sicherzustellen.

Entschließung über die Offenheit bei der Verarbeitung personenbezogener Daten

Unter Hinweis auf die „Entschließung über die Verbesserung der Bekanntmachung von Praktiken zum Datenschutz", die im Jahr 2003 auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre angenommen wurde.

Eingedenk dessen, dass sich das Ausmaß und der Umfang der erhobenen personenbezogenen Daten, die Fähigkeit zur Auswertung dieser Daten und die Nutzungsmöglichkeiten dieser Daten auf dramatische Weise erhöht haben.

Im Anbetracht dessen, dass Offenheit ein langjähriges Prinzip der fairen Information ist, das sich in mehreren internationalen Instrumenten widerspiegelt, einschließlich in den „Internationalen Standards zum Schutz der Privatsphäre" (die Erklärung von Madrid), die auf der 31. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre im Jahr 2009 angenommen wurden.

In der Erkenntnis, dass eine effektive Kommunikation von Vorgehensweisen und Praktiken einer Organisation in Bezug auf personenbezogene Daten wesentlich ist für die Einzelnen, um informierte Entscheidungen über die Art und Weise der Verwendung ihrer personenbezogenen Daten und zu treffen und Maßnahmen zum Schutz ihrer Privatsphäre und zur Durchsetzung ihrer Rechte zu ergreifen.

In der Erkenntnis, dass Transparenz in Bezug auf Vorgehensweisen und Praktiken von Regierungen in Bezug auf personenbezogene Daten entscheidend ist für die Schaffung und Erhaltung von Vertrauen, zur Förderung des Engagements der Bürger und zur Wahrung demokratischer Rechenschaft.

Die 35. Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre **beschließt** daher:

1. Bei den Organisationen, die personenbezogene Daten erheben, darauf zu drängen, die Zwecke zu erklären, zu denen die Daten gesammelt werden; die Identität der Organisation oder verantwortlichen Person preiszugeben und zu erklären, wie man sich mit ihnen in Verbindung setzt und wie man einen Antrag auf Zugang oder Korrektur der Daten stellen kann;

2. Bei den Organisationen darauf zu drängen, verständliche Informationen über ihre Vorgehensweise und Praktiken bezüglich der Datensammlung in deutlicher und einfacher Sprache und in einem leicht zugänglichen Format zu geben, wobei sie die Charakteristika der Einzelnen, auf die sich die Daten beziehen, und die Methode der Erhebung berücksichtigen;

3. Bei den Organisationen, Datenschutzbehörden, Behörden für den Schutz der Privatsphäre sowie bei den Regierungen darauf zu drängen, über die Nützlichkeit von Datenschutz-Gütesiegeln, Zertifizierungen und Vertrauenssiegeln als Mittel zur Information für die Nutzer und für mehr Wahlfreiheit nachzudenken;

   und

4. Bei den Regierungen darauf zu drängen, unter angemessener Berücksichtigung der nationalen Sicherheit, der öffentlichen Sicherheit und der öffentlichen Ordnung, zur Stärkung der demokratischen Rechenschaft und zur wirksamen Umsetzung des Grundrechts des Schutzes der Privatsphäre mehr Offenheit über ihre Datenerhebungspraktiken an den Tag zu legen.

Aus Zuständigkeitsgründen enthielt sich die US Federal Trade Commission bei der Abstimmung über diese Entschließung, soweit sie den öffentlichen Bereich betrifft.

Erläuternde Anmerkungen

Auf internationaler Ebene hat das Prinzip der Offenheit seine Wurzeln in den OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, die in den späten 1970er Jahren entwickelt wurden. Heute wird dieses Prinzip weitgehend in den Gesetzen über den Datenschutz und den Schutz der Privatsphäre auf der ganzen Welt widergespiegelt.

Die Menschen erwarten heute eine größere Rechenschaftspflicht und Transparenz auf Seiten der Organisationen des privaten Bereichs und ihrer Regierungen in Bezug auf die Art und Weise, wie diese personenbezogene Daten erheben, nutzen und offenlegen. Allerdings werden diese Erwartungen nicht immer berücksichtigt. Im Jahre 2013 nahmen neunzehn Behörden aus aller Welt an dem ersten Global Privacy Enforcement Network (GPEN) Datenschutz Sweep teil. Die teilnehmenden Behörden untersuchten in einem koordinierten Vorgehen Webseiten, um die Transparenz der Datenschutzpraktiken von Organisationen zu beurteilen.

Die Behörden fanden heraus, dass eine von fünf Sites keine Datenschutzerklärung aufwies oder dass diese in einem langen rechtlichen Hinweis über den Webseiten-Betreiber oder in den allgemeinen Geschäftsbedingungen verborgen war. Wenn Datenschutzerklärungen existierten, dann häufig nur in Form von Textbausteinen mit Formulierungen von rechtlichen Anforderungen, ohne den Nutzern klare und verständliche Informationen über die Art und Weise zu geben, wie ihre personenbezogenen Daten genutzt und offengelegt werden. Sie fanden auch heraus, dass in einer beträchtlichen Anzahl von Fällen die Sites entweder keine Kontaktinformationen auflisteten, mit deren Hilfe sich die Nutzer zusätzliche Informationen über die Praktiken der Organisation einholen könnten, oder dass die Kontaktdaten schwer zu finden waren.

Die jüngsten Enthüllung über Überwachungsprogramme von Regierungen lösten Forderungen nach mehr Offenheit in Bezug auf den Umfang dieser Programme, nach einer strengeren Aufsicht und einer größeren Rechenschaftspflicht bezüglich dieser Programme aus, sowie Forderungen nach einer stärkeren Transparenz seitens der Organisationen des privaten Bereichs, die verpflichtet sind, den Regierungen personenbezogene Daten zur Verfügung zu stellen. Die Enthüllungen haben ebenso Diskussionen über das angemessene Maß an Transparenz in Verbindung mit solchen Programmen unter Berücksichtigung der nationalen Sicherheit, der öffentlichen Sicherheit und der öffentlichen Ordnung ausgelöst.

Entschließung „Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht“

Die Konferenz ruft in Erinnerung, dass sie:

– bereits auf ihrer 27. Sitzung in Montreux die Vereinten Nationen aufgefordert hat, ein verbindliches Rechtsinstrument vorzubereiten, in dem die Rechte auf

Datenschutz und dem Schutz der Privatsphäre als einklagbare Menschenrechte klar und detailliert geregelt sind,

– auf ihrer 28. Sitzung in Montreal die Verbesserung der internationalen Zusammenarbeit beim Datenschutz und dem Schutz der Privatsphäre gefordert hat,

– auf ihrer 30. Sitzung in Straßburg eine Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz der personenbezogenen Daten verabschiedet hat,

– auf ihrer 31. Sitzung in Madrid internationale Standards zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre angenommen hat (Erklärung von Madrid),

– auf ihrer 32. Sitzung in Jerusalem die Regierungen zur Einberufung einer Regierungskonferenz aufgefordert hat, um ein verbindliches internationales Übereinkommen zum Schutz der Privatsphäre und der Daten zu erarbeiten, mit dem die Erklärung von Madrid umgesetzt wird,

und sie erinnert an die Wichtigkeit bestehender Instrumente im internationalen Recht, die Regelungen und Standards für den Schutz personenbezogener Daten vorsehen, insbesondere das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108).

Die 35. Internationale Konferenz stellt fest,

dass eine dringende Notwendigkeit für eine verbindliche internationale Vereinbarung zum Datenschutz besteht, das die Menschenrechte durch den Schutz der Privatsphäre, der personenbezogenen Daten und der Integrität von Netzwerken gewährleistet und die Transparenz der Datenverarbeitung erhöht, und dabei ein ausgewogenes Verhältnis im Hinblick auf Sicherheit, wirtschaftliche Interessen und freie Meinungsäußerung wahrt.

und beschließt

die Regierungen auffordern, sich für die Verabschiedung eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) einzusetzen, das auf den Standards, die von der Internationalen Konferenz entwickelt und gebilligt wurden, und auf den Bestimmungen im allgemeinen Kommentar Nr. 16 zum Pakt basieren sollte, um weltweit gültige Standards für

den Datenschutz und den Schutz der Privatsphäre zu schaffen, die im Einklang mit der Rechtsstaatlichkeit stehen.

Die Federal Trade Commission der USA enthielt sich bei der Abstimmung über diese Entschließung.

Erläuternde Anmerkungen

Die 35. Internationale Konferenz stellt fest, dass der im Jahre 1966 von der Generalversammlung der Vereinten Nationen angenommene und von 167 Staaten ratifizierte IPBPR bereits einen rechtlichen Rahmen für den Schutz der Privatsphäre bietet. Artikel 17 des IPBPR lautet:

1. Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
2. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Darüber hinaus bietet der allgemeine Kommentar Nr. 16 des IPBPR weitere Erläuterungen zu den datenschutzrechtlichen Bestimmungen unter Artikel 17. Dort heißt es, unter anderem, dass,

- die Erhebung und Speicherung personenbezogener Daten auf Computern, in Datenbanken oder anderen Geräten, sei es von öffentlichen oder privaten Stellen, gesetzlich geregelt werden müssen;
- die Staaten wirksame Maßnahmen ergreifen müssen um sicherzustellen, dass Informationen über das Privatleben einer Person nicht in die Hände von Personen gelangen, die nicht gesetzlich zum Erhalt, zur Verarbeitung und zur Nutzung dieser Informationen berechtigt sind;
- Nutzungen dieser Informationen zu Zwecken, die mit dem Pakt nicht vereinbar sind, verhindert werden müssen;
- die Einzelnen das Recht haben sollten, zu bestimmen, welche Informationen über sie gespeichert werden und für welche Zwecke, sowie das Recht, einen Antrag auf Berichtigung oder Löschung fehlerhafter Informationen zu stellen;
- jeder „Eingriff" in diese Rechte nur auf einer gesetzlichen Grundlage erfolgen darf, die mit dem Pakt im Einklang steht.

Diese Forderungen werden durch die Verpflichtung der speichernden Stelle zur Transparenz bei der Datenverarbeitung ergänzt, insbesondere in Bezug auf die Bereitstellung von Informationen, Korrektur und Löschung als wesentliche Datenschutzgrundsätze.

Entschließung zu Webtracking und Datenschutz

Web Tracking ermöglicht den Organisationen die Überwachung fast jeden einzelnen Aspekts des Nutzerverhaltens im Internet. Die Art von Information, die durch Tracking erhoben werden kann, (z. B. IP-Adressen, Gerätekennungen, etc.), kann zur Identifizierung eines bestimmten Betroffenen führen. Diese Fähigkeit eröffnet den Organisationen die Möglichkeit zur Entwicklung eines umfangreichen Profils über die Online-Aktivitäten eines identifizierbaren Betroffenen über einen längeren Zeitraum.

Daten über Nutzeraktivitäten, die von einem Computer oder einem anderen Gerät (z. B. einem Smartphone) während der Nutzung verschiedener Dienste der Informationsgesellschaft im Internet erhoben werden, werden zunehmend von unterschiedlichen Akteuren für verschiedene Zwecke kombiniert, korreliert und analysiert, die sich von karitativen bis zu kommerziellen Zwecken der unterschiedlichen Akteure erstrecken, die solche Dienstleistungen oder Teile davon anbieten. Die erzeugten Interessenprofile (oder „Nutzerprofile“) können mit Daten der „offline-Welt“ über fast jeden Aspekt des Privatlebens, einschließlich finanzieller Informationen wie auch Informationen, beispielsweise über Freizeitinteressen, gesundheitliche Probleme, politische Ansichten und/oder religiöse Meinungen angereichert werden.

Wir erkennen an, dass Tracking den Verbrauchern einige Vorteile wie Netzwerk-Management, Sicherheit und Betrugsprävention bietet und die Entwicklung neuer Produkte und Dienstleistungen erleichtern kann. Dennoch stellt Tracking ein ernsthaftes Risiko für die Privatsphäre der Bürger in einer Informationsgesellschaft dar, denn es droht, die wichtigsten datenschutzrechtlichen Grundsätze der Transparenz, Zweckbindung und individuelle Kontrolle zu untergraben.

Als Konsequenz hieraus sollten alle Beteiligten, einschließlich Regierungen, internationalen Organisationen und Anbietern von Informationsdiensten den Schutz der Privatsphäre beim Design, der Bereitstellung und Nutzung von Diensten der Informationsgesellschaft an die erste Stelle setzen.

Die Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre fordert daher alle Beteiligten auf, soweit es relevant und angebracht ist, folgendes zu unternehmen:

- Beachtung des Grundsatzes der Zweckbindung;
- Benachrichtigung und Kontrolle über die Verwendung von Tracking-Elementen, einschließlich Geräte- und Browser Fingerprinting;
- Verzicht auf die Nutzung unsichtbarer Tracking-Elemente zu anderen Zwecken als für Sicherheit / Betrugsaufdeckung oder Netzwerk-Managment;

- Verzicht auf die Ableitung eines Satzes an Informationselementen (Fingerabdrücke) für die alleinige Identifizierung und Verfolgung von Nutzern zu anderen Zwecken als für Sicherheit / Betrugsprävention oder Netzwerk-Management;

- Gewährleistung angemessener Transparenz über alle Arten von Web-Tracking-Verfahren, damit die Verbraucher eine informierte Wahl treffen können;

- Angebot einfach zu bedienender Werkzeuge, um den Nutzern angemessene Kontrolle über die Erhebung und Nutzung ihrer personenbezogenen Daten zu ermöglichen;

- Vermeidung des Trackings von Kindern und des Trackings auf an Kinder gerichtete Webseiten;

- Beachtung des Grundsatzes des Privacy-by-Design und Durchführung einer Datenschutz-Folgenabschätzung zu Beginn neuer Projekte;

- Verwendung von Techniken, die die Auswirkungen auf die Privatsphäre mindern, wie Anonymisierung / Pseudonymisierung;

- Förderung technischer Standards für eine bessere Nutzerkontrolle (z. B. ein wirksamer Do-Not-Track Standard).

Die Datenschutzbeauftragte der Republik Slowenien und die Französische Datenschutzbehörde enthielten sich bei der Abstimmung über diese Entschließung.

Entschließung zur Internationalen Koordinierung der Aufsichtstätigkeit

Unter Hinweis auf die Entschließungen der 29., 33. und 34. Konferenz, die

- die Datenschutzbehörden ermutigten, ihre Bemühungen um die Unterstützung der internationalen Zusammenarbeit weiterzuentwickeln und mit internationalen Organisationen zur Stärkung des Datenschutzes auf der ganzen Welt zusammen zu arbeiten, und

- die Annahme der Empfehlung der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zur grenzüberschreitenden Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen begrüßten;

Unter Hinweis darauf, dass die 33. Konferenz die Arbeitsgruppe zur internationalen Koordinierung der Aufsichtstätigkeit im Datenschutz als vorläufige Arbeitsgruppe einrichtete, die einen Rahmen zur Erleichterung der möglichen

Koordinierung entwickeln und auf der 34. Konferenz darüber berichten sollte; und

Unter Kenntnisnahme, dass die Arbeitsgruppe als Bericht ein Rahmenwerk mit sechs empfohlenen Koordinierungsgrundsätzen vorlegte; und

Unter weiterem Hinweis darauf, dass die 33. Konferenz beschloss, sicherzustellen, dass diejenigen, die sich für die Fragen zur Durchsetzung des Datenschutzes und zur Koordinierung interessieren, jedes Jahr wenigstens eine Gelegenheit für ein Treffen haben, und unter Kenntnisnahme der folgenden Treffen in Montreal und Washington DC;

Eingedenk der Tatsache, dass die jüngsten Fälle wieder gezeigt haben, wie sich die Praktiken globaler Konzerne, oder Sicherheitsverletzungen, die ihre Informationssysteme betreffen, schnell und nachteilig auf eine große Anzahl von Personen auf der ganzen Welt auswirken können;

Aufbauend auf bedeutsamen Fortschritten, die in den letzten Jahren auf regionaler und internationaler Ebene zum Ausbau von Übereinkommen für grenzüberschreitende Zusammenarbeit zur Durchsetzung von Datenschutzgesetzen erzielt wurden, wozu die Bemühungen der APEC, der in der Artikel 29-Datenschutzgruppe vertretenen Datenschutzbehörden, der OECD, des Europarats, des Netzwerks der frankophonen Behörden,des Ibero-Amerikanischen Netzwerks, und des GPEN gehören;

Schlussfolgernd, dass die verstärkte Koordinierung die Effektivität der Datenschutzbehörden in den Fällen steigern würde, die die Verarbeitung personenbezogener Daten in unterschiedlichen Rechtssystemen betreffen:

Beschließt die 35. Internationale Konferenz der Beauftragen für Datenschutz und Privatsphäre die weitere Förderung der Bemühungen um eine effektive Koordinierung von grenzüberschreitenden Untersuchungen und Durchsetzungen in entsprechenden Fällen, und insbesondere:

1. der Arbeitsgruppe zur internationalen Koordinierung der Aufsichtstätigkeit den **Auftrag** zur Zusammenarbeit mit anderen Netzwerken **zu erteilen**, damit sie einen gemeinsamen Ansatz für den grenzüberschreitenden Umgang mit Fällen und für die Koordinierung der Durchsetzung entwickelt; dies soll in einem multilateralen Rahmendokument festgehalten werden, das auf der 36. Konferenz angenommen werden soll. Dieser Ansatz soll auf dem auf der 34. Konferenz vorgestellten internationalen Koordinationsrahmen und auf der Arbeit des GPEN gründen und den Austausch von für die Durchsetzung relevanter Informationen zum Gegenstand haben, wozu auch gehört, wie diese Informationen von den Empfängern zu behandeln sind. Diese Arbeit soll nicht

die bestehenden nationalen und regionalen Bedingungen und Mechanismen für den Informationsaustausch ersetzen oder ähnliche Vereinbarungen anderer Netzwerke beeinträchtigen;

2. die Datenschutzbehörden **zu ermutigen**, konkrete Chancen zur Zusammenarbeit bei besonderen Ermittlungen mit grenzüberschreitenden Gesichtspunkten zu suchen;

3. die Entwicklung einer sicheren Informationsplattform **zu unterstützen**, die den Datenschutzbehörden einen „sicheren Raum" für den Austausch vertraulicher Informationen bietet, die ihnen ebenso die Initiierung und Durchführung koordinierter Durchsetzungsaktionen ermöglicht sowie andere internationale Mechanismen zur koordinierten Durchsetzung ergänzt und damit einen Mehrwert für die internationalen operationellen Rahmenwerke für die Durchsetzung bietet.

Erläuternde Anmerkungen

Diese Entschließung zielt darauf ab, auf frühere Entschließungen zur Förderung der Zusammenarbeit bei der grenzüberschreitenden Durchsetzung des Datenschutzes aufzubauen. Alle Mitglieder der Internationalen Konferenz sind eingeladen, sich an der Erreichung der Ziele dieser Entschließung zu beteiligen, deren Bestreben die Mobilisierung der bestehenden Mechanismen ist, auf ihnen aufzubauen und sie zu verbessern und ebenso die Sicherstellung, dass neue und innovative Wege zur internationalen Durchsetzungskoordinierung identifiziert, erforscht und nutzbar gemacht werden.

Die Entschließung erkennt an, dass das Global Privacy Enforcement Network (GPEN) bislang das einzige globale Netzwerk ist, das sich ausschließlich der Zusammenarbeit bei der Durchsetzung widmet, in dem alle Datenschutzbehörden mitwirken können, und sie möchte die Behörden ermutigen, GPEN beizutreten und zur Steigerung seiner Effektivität beizutragen.

Zum weiteren Ausbau der bisherigen Bemühungen und zur Entwicklung konkreter Mechanismen zur Gestaltung und Erleichterung der internationalen Durchsetzungskoordinierung wird der Datenschutzbeauftragte des Vereinigten Königreichs Gastgeber der dritten Jahresveranstaltung zur internationalen Durchsetzungskoordinierung in Manchester im April 2014 sein.

Angesichts des technologischer Wandels und der Leichtigkeit, mit der personenbezogene Daten über die ganze Welt mitgeteilt werden können, müssen die Datenschutzbehörden die erforderlichen Instrumente und Mechanismen zur Koordinierung miteinander entwickeln, sodass sie angemessen auf die Forderungen ihrer Bürger nach einer wirksamen Aufsicht über solche Ereignisse reagieren können.

Obwohl es bereits Zusammenarbeits- und Koordinierungsmechanismen gibt, müssen sich die Datenschutzbehörden an anderen einschlägigen internationalen Organisationen wie der APEC, den in der Artikel-29-Datenschutzgruppe vertretenen Datenschutzbehörden, dem Europarat und der OECD orientieren und sich von dort Ideen für die Entwicklung ihrer eigenen rechtlichen und technischen Rahmenbedingungen holen.

Einige bestehende Gesetze enthalten Beschränkungen für den Informationsaustausch über mögliche oder laufende Ermittlungen, weshalb einige Datenschutzbehörden bestimmte nationale Bedingungen zu erfüllen haben, bevor sie grenzüberschreitend Informationen austauschen. Das wurde oft durch Absichtserklärungen oder regionale Vereinbarungen erleichtert. Durch die Entwicklung eines solchen Ansatzes mit multilateralem Geltungsbereich können wir dazu beitragen, den Verwaltungsaufwand zu reduzieren, den Prozess zu beschleunigen und somit eine Intensivierung des Austauschs von Informationen fördern, die für die Durchsetzung wichtig sind. Behörden, die aus rechtlichen oder anderen Erwägungen die Entwicklung bilateraler und regionaler Kooperationsübereinkommen oder Absichtserklärungen bevorzugen, sollten dies auch weiterhin tun. Diese werden nicht durch die oben unter Nummer 1 vorgeschlagene Arbeit ausgeschlossen.

Die in dieser Entschließung vorgeschlagene Informations-Plattform soll die Arbeit der GPENBehörden unterstützen, und sie soll auf einem mehrschichtigen Ansatz fußen, der es den Behörden erlaubt, Entscheidungen über den Austausch von Informationen mit anderen Behörden zu treffen, und zwar im Vertrauen darauf, dass sie gegenseitige Verpflichtungen eingegangen sind und ähnliche Funktionen und Pflichten haben.

Obwohl es unwahrscheinlich ist, dass sich jeder Fall über einen universellen Ansatz regeln lässt, sollte dies nicht das Ziel der Dokumentation gemeinsamer Konzepte verhindern, die den Informationsaustausch erleichtern und zu einer verbesserten Koordinierung und Zusammenarbeit beitragen.

Erklärung von Warschau zur „Appifikation“ der Gesellschaft

Warschau, Polen – 24. September 2013

Mobile Anwendungen (Apps) sind heute allgegenwärtig. Auf unseren Smartphones und Tablets, in den Autos, im und um das Haus herum: Eine wachsende Anzahl von Geräten besitzt mit dem Internet verbundene Benutzeroberflächen. Derzeit stehen mehr als 6 Millionen Apps im öffentlichen und im privaten Be-

reich zur Verfügung. Diese Anzahl nimmt mit über 30.000 pro Tag ständig zu. Apps machen vieles in unserem täglichen Leben leichter und bringen mehr Spaß. Gleichzeitig sammeln Apps große Mengen personenbezogener Daten. Dies ermöglicht eine ständige digitale Überwachung, oftmals ohne dass sich die Nutzer bewusst sind, dass dies geschieht und für welche Zwecke ihre Daten genutzt werden.

App-Entwickler sind sich der Auswirkungen ihrer Arbeit auf die Privatsphäre häufig nicht bewusst und nicht mit Begriffen wie „Privacy by Design" und „Datenschutzfreundliche Voreinstellungen"/„Privacy by Default" vertraut. Die wichtigsten Betriebssysteme und App-Plattformen bieten einige datenschutzfreundliche Einstellungen, aber sie ermöglichen den Nutzern nicht die vollständige Kontrolle zum Schutz ihrer Daten und zur Überprüfung, welche Informationen zu welchem Zweck erhoben werden.

Während ihrer 35. Internationalen Konferenz am 23. und 24. September 2013 in Warschau diskutierten die Beauftragten für Datenschutz und Privatsphäre über die „Appifikation" der Gesellschaft, über die Herausforderungen aufgrund der verstärkten Nutzung von mobilen Anwendungen sowie über Möglichkeiten zu ihrer Bewältigung.

Verschiedene Berichte der Datenschützer über mobile Apps, die in den vergangenen Jahren veröffentlicht wurden, einschließlich – jedoch nicht allein – der Stellungnahme der Artikel 29 Datenschutzgruppe der Europäischen Union „Apps auf intelligenten Endgeräten", der *„Guidance for mobile app developers"* der Datenschutzbeauftragen von Kanada, des Beurteilungsberichts der US Federal Trade Commission *„Mobile privacy disclosures: building trust through transparency"* sowie des Sopot Memorandums der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation von 2012, geben wertvolle Hinweise zum Umgang mit der Beziehung zwischen Apps und Privatsphäre.

Die Datenschutzbeauftragten brachten ihr klares Engagement zum Ausdruck, sicherzustellen, dass den Nutzern ein besserer Schutz ihrer Privatsphäre geboten wird, und sie planen, verschiedene Akteure im öffentlichen wie im privaten Bereich im Hinblick auf ihre Aufgaben und Verantwortlichkeiten anzusprechen.

Wesentlich ist, dass die **Nutzer** für ihre eigenen Daten verantwortlich sind und bleiben. Sie sollten in der Lage sein zu entscheiden, welche Informationen sie mit wem und zu welchen Zwecken teilen. Zu diesem Zweck sollten – auch innerhalb einer App – klare und verständliche Informationen über Datensammlungen zur Verfügung stehen, die stattfinden, bevor die eigentliche Sammlung beginnt. Den Nutzern sollte die Möglichkeit eingeräumt werden, den Zugang zu speziellen Informationen wie Ortungsdaten oder Adressbucheinträgen von Fall zu Fall zu

gestatten. Vor allem aber sollten Apps auf der Grundlage der Minimierung von Überraschungen entwickelt werden: keine versteckten Funktionen, keine nicht überprüfbaren Datensammlungen im Hintergrund.

App-Entwickler treiben das Wachstum in der digitalen Wirtschaft an und bringen Erleichterungen in unser tägliches Leben. Gleichzeitig müssen sie die Einhaltung bestehender Regelungen zum Schutz der Privatsphäre und der Daten weltweit gewährleisten. Um dieses Ziel zu erreichen und gleichzeitig für eine positive Nutzererfahrung zu sorgen, ist der Datenschutz bereits am Anfang der Entwicklung einer App zu berücksichtigen. Auf diese Weise kann der Datenschutz auch ein Wettbewerbsvorteil durch die Erhöhung des Vertrauens der Nutzer sein. Entwickler müssen klar entscheiden, welche Informationen für die Leistung der App notwendig sind und sicherstellen, dass keine zusätzlichen personenbezogenen Daten ohne die informierte Einwilligung der Nutzer gesammelt werden. Dies gilt auch, wenn Codes von Drittanbietern oder Plug-Ins von App-Entwicklern verwendet werden, zum Beispiel von Ad-Netzwerken. Entwickler müssen sich jederzeit darüber bewusst sein, was sie den Nutzern anbieten und was sie von ihnen verlangen.

Die Verantwortung für den Schutz der Privatsphäre liegt nicht allein bei den App-Entwicklern. **Anbieter von Betriebssystemen** müssen die Verantwortung für ihre Plattformen tragen. Zwar übernehmen diese Akteure zunehmend Verantwortung, indem sie allgemeine datenschutzfreundliche Einstellungen auf mobilen Geräten anbieten. Allerdings sind diese nur unzureichend granular, um eine vollständige Nutzerkontrolle für alle bedeutsamen Aspekte der einzelnen Datensammlung zu ermöglichen. Da Plattform-Anbieter den Rahmen, in dem Apps verwendet werden, herstellen und pflegen, sind sie am besten zur Gewährleistung des Datenschutzes geeignet und tragen eine besondere Verantwortung gegenüber den Nutzern. In dieser Hinsicht ist die Bereitschaft der Industrie für Datenschutz-Gütesiegel oder andere durchsetzbare Zertifizierungssysteme zu fördern.

Obgleich die Hauptverantwortung für den Schutz der Privatsphäre der Nutzer bei der App-Industrie liegt, können und sollen die **Beauftragten für Datenschutz und Privatsphäre** das Bewusstsein für diese Themen bei den Akteuren der App-Industrie sowie bei den App-Nutzern, der breiten Öffentlichkeit, erhöhen. Insbesondere sollte die Zusammenarbeit mit den Anbietern von Betriebssystemen angestrebt werden, um sicherzustellen, dass die wesentlichen Elemente des Datenschutzes in ihren Plattformen eingesetzt werden. Es ist nicht unsere Aufgabe, den Spaß zu verderben, den Apps ihren Nutzern bieten können, aber der Missbrauch personenbezogener Daten ist zu verhindern. Wenn die Anregungen für eine bessere Praxis zum Schutz der Privatsphäre nicht zu zufriedenstellenden Ergebnissen führen, werden die Datenschutzbeauftragten bereit stehen, die Rechtsvorschriften zur Nutzerkontrolle in einer globalen Anstrengung einzufordern und durchzusetzen.

Die Beauftragten für Datenschutz und Privatsphäre aus aller Welt möchten das kommende Jahr für ernsthafte Schritte zur Verbesserung des Schutzes der Privatsphäre und der Daten in diesem Bereich nutzen und das Thema auf ihrer 36. Konferenz auf Mauritius wieder aufgreifen.

Wojciech Rafal Wiewiórowski
Generalny Inspektor Ochrony
Danych Osobowych

Jacob Kohnstamm
Vorsitzender des Exekutivkomitees
der Internationalen Konferenz

VI. Resolution der UN-Vollversammlung vom 18. Dezember 2013 (GA/11475, 68. Sitzung)

Das Recht auf Privatheit im digitalen Zeitalter

Die Generalversammlung,

in Bekräftigung der Ziele und Grundsätze der Charta der Vereinten Nationen,

sowie in Bekräftigung der in der Allgemeinen Erklärung der Menschenrechte und den einschlägigen internationalen Menschenrechtsverträgen, einschließlich des Internationalen Paktes über bürgerliche und politische Rechte und des Internationalen Paktes über wirtschaftliche, soziale und kulturelle Rechte, verankerten Menschenrechte und Grundfreiheiten,

ferner in Bekräftigung der Erklärung und des Aktionsprogramms von Wien,

feststellend, dass das rasche Tempo der technologischen Entwicklung Menschen in der ganzen Welt in die Lage versetzt, sich neuer Informations- und Kommunikationstechnologien zu bedienen, und gleichzeitig die Fähigkeit der Regierungen, Unternehmen und Personen zum Überwachen, Abfangen und Sammeln von Daten vergrößert, das eine Verletzung oder einen Missbrauch der Menschenrechte darstellen kann, insbesondere des in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte festgelegten Rechts auf Privatheit, weshalb diese Frage in zunehmendem Maße Anlass zur Sorge gibt,

in Bekräftigung des Menschenrechts auf Privatheit, dem zufolge niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr ausgesetzt werden darf, und des Anspruchs auf rechtlichen Schutz gegen solche Eingriffe sowie in der Erkenntnis, dass die Ausübung des Rechts auf Privatheit für die Verwirklichung des Rechts auf freie Meinungsäußerung und auf unbehinderte Meinungsfreiheit wichtig ist und eine der Grundlagen einer demokratischen Gesellschaft bildet,

unter nachdrücklichem Hinweis auf die Wichtigkeit der uneingeschränkten Achtung der Freiheit, Informationen sich zu beschaffen, zu empfangen und weiterzugeben, namentlich auch die grundlegende Wichtigkeit des Zugangs zu Informationen und der demokratischen Teilhabe,

unter Begrüßung des dem Menschenrechtsrat auf seiner dreiundzwanzigsten Tagung vorgelegten Berichts des Sonderberichterstatters über die Förderung und den Schutz der Meinungsfreiheit und des Rechts der freien Meinungsäußerung[1] zu den Auswirkungen, die das Überwachen von Kommunikation durch die Staaten auf die Ausübung der Menschenrechte auf Privatheit und auf Meinungsfreiheit und freie Meinungsäußerung hat,

betonend, dass das rechtswidrige oder willkürliche Überwachen und/oder Abfangen von Kommunikation sowie die rechtswidrige oder willkürliche Sammlung personenbezogener Daten, als weitreichende Eingriffe, die Rechte auf Privatheit und freie Meinungsäußerung verletzen und im Widerspruch zu den Prinzipien einer demokratischen Gesellschaft stehen können,

feststellend, dass Besorgnisse über die öffentliche Sicherheit das Sammeln und den Schutz bestimmter sensibler Informationen zwar rechtfertigen können, dass die Staaten jedoch die vollständige Einhaltung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen müssen,

tief besorgt über die nachteiligen Auswirkungen, die das Überwachen und/oder Abfangen von Kommunikation, einschließlich des extraterritorialen Überwachens und/oder Abfangens von Kommunikation, sowie die Sammlung personenbezogener Daten, insbesondere wenn sie in massivem Umfang durchgeführt werden, auf die Ausübung und den Genuss der Menschenrechte haben können,

bekräftigend, dass die Staaten sicherstellen müssen, dass alle zur Bekämpfung des Terrorismus ergriffenen Maßnahmen mit ihren Verpflichtungen nach dem Völkerrecht, insbesondere den internationalen Menschenrechtsnormen, dem Flüchtlingsvölkerrecht und dem humanitären Völkerrecht, im Einklang stehen,

1. *bekräftigt* das Recht auf Privatheit, dem zufolge niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr ausgesetzt werden darf, und den Anspruch auf rechtlichen Schutz gegen solche Eingriffe, wie in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte festgelegt;

2. *ist sich dessen bewusst*, dass der globale und offene Charakter des Internets und das rasche Voranschreiten der Informations- und Kommunikationstechnologien als eine treibende Kraft für die Beschleunigung des Fortschritts bei der Entwicklung in ihren verschiedenen Formen wirken;

[1] A/HRC/23/40 und Corr.1.

3. *erklärt*, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen, einschließlich des Rechts auf Privatheit;

4. *fordert* alle Staaten *auf*:

   a) das Recht auf Privatheit zu achten und zu schützen, namentlich im Kontext der digitalen Kommunikation;

   b) Maßnahmen zu ergreifen, um Verletzungen dieser Rechte ein Ende zu setzen und die Bedingungen dafür zu schaffen, derartige Verletzungen zu verhindern, namentlich indem sie sicherstellen, dass die einschlägigen innerstaatlichen Rechtsvorschriften mit ihren Verpflichtungen nach den internationalen Menschenrechtsnormen im Einklang stehen;

   c) ihre Verfahren, Praktiken und Rechtsvorschriften hinsichtlich der Überwachung von Kommunikation, deren Abfangen und der Sammlung personenbezogener Daten zu überprüfen, namentlich Überwachen, Abfangen und Sammeln in massivem Umfang, mit dem Ziel, das Recht auf Privatheit zu wahren, indem sie die vollständige und wirksame Umsetzung aller ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen;

   d) unabhängige, wirksame innerstaatliche Aufsichtsmechanismen einzurichten oder bestehende derartige Mechanismen beizubehalten, die in der Lage sind, Transparenz, soweit angebracht, und Rechenschaftspflicht der staatlichen Überwachung von Kommunikation, deren Abfangen und der Sammlung personenbezogener Daten sicherzustellen;

5. *ersucht* die Hohe Kommissarin der Vereinten Nationen für Menschenrechte, dem Menschenrechtsrat auf seiner siebenundzwanzigsten Tagung und der Generalversammlung auf ihrer neunundsechzigsten Tagung einen Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen zur Prüfung durch die Mitgliedstaaten vorzulegen;

6. *beschließt*, diese Frage auf ihrer neunundsechzigsten Tagung unter dem Unterpunkt „Menschenrechtsfragen, einschließlich anderer Ansätze zur besseren Gewährleistung der effektiven Ausübung der Menschenrechte und Grundfreiheiten“ des Punktes „Förderung und Schutz der Menschenrechte“ zu behandeln.

VII. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 53. Sitzung am 15./16. April 2013 in Prag, Tschechische Republik

Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar

– Übersetzung –

Einleitung

1. Dieses Papier gründet auf der Achtung der Grundrechte und Grundfreiheiten der Internetnutzer. Obgleich der Fokus nicht auf besonderen technischen Maßnahmen liegt, geht das Papier gleichwohl davon aus, dass das technische Verfahren des Webtracking rechtmäßig und angemessen sein und dass es sich innerhalb eines strengen Rahmens dieser Rechte bewegen muss. Die Grundsätze von Wahlmöglichkeiten und Kontrolle – die von großen Teilen der Wirtschaft gefordert werden – bilden das Zentrum dieses Rahmens; diese Grundsätze müssen mit Genauigkeit auf den Säulen von Klarheit, Transparenz und Verantwortlichkeit umgesetzt werden. Die Rechtfertigung für die Durchführung von Webtracking ist nicht offenkundig, deshalb müssen die Wirtschaft und andere Vertreter, die Tracking durchführen, beständig nach Lösungen suchen, die diese Tätigkeit nicht nur voll und ganz in den Rahmen der Grundrechte und Privatsphäre einpassen, sondern sie auch mit dem Gebot des „Privacy by Design" *[Einbeziehung des Schutzes der Privatsphäre schon bei der Entwicklung von Technologien]* in Einklang bringen.

2. In diesem Arbeitspapier behandelt die Arbeitsgruppe das Thema Webtracking und Privatsphäre. Obgleich es keine klare Definition dafür gibt, werden wir uns auf eine Definition des Webtracking[1] beziehen, nämlich als der Erhebung, Analyse und Anwendung von Daten über Nutzeraktivitäten von einem Computer oder Gerät aus, wenn verschiedene Dienste der Informationsgesellschaft (nachfol-

[1] van Eijk (2012), The DNA of OBA: unique identifiers [Die DNA der OBA: Eindeutige Identifikatoren] [OBA = Online Behavioural Advertising = Online-Werbung mit Nutzung des Surfverhaltens der Nutzer], URL: http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking.

gend: das Internet)[2] genutzt werden, um diese Nutzungsdaten zu verschiedenen Zwecken zusammen zu führen und zu analysieren, und zwar von wohltätigen und philantropischen bis hin zu kommerziellen Zwecken. Wir sind der Meinung, dass verschiedene Formen der Marktforschung unter diese Definition des Webtracking fallen, zum Beispiel die Reichweitenmessung („outreach measurement" – der Umfang, in dem Nutzer Anzeigen überall im Internet angezeigt bekommen), das Messen des Nutzungsverhaltens („engagement measurement" – der Umfang, in dem Nutzer mit Internetdiensten in Interaktion treten) und das Messen der erreichten Nutzer („audience measurement" – der Umfang, in dem Mikroprofile der Nutzer aus ihrer Interaktion mit Angeboten im Internet abgeleitet werden können).[3]

Umfang des Arbeitspapiers

3. Dieses Papier richtet sich an alle Anbieter von Web-Sites sowie an Softwareentwickler und Service Provider *[Diensteanbieter]*, die Trackingtechnologien anbieten oder nutzen. Dieses Papier diskutiert die Entwicklung von Trackingtechnologien und ihre möglichen Auswirkungen auf die Privatsphäre der Bürgerinnen und Bürger. Es befasst sich mit digitalen Spuren, die wir hinterlassen, wenn wir die verschiedenen Dienste der Informationsgesellschaft mit einem Webbrowser nutzen, dazu gehören auch eindeutige Identifikatoren („unique identifier"), die mit Hilfe von Technologien erlangt werden, die ohne Cookies arbeiten.[4] Dazu zählen ferner auch Webbrowser auf anderen Geräten, zum Beispiel auf Smartphones und Smart-TV-Geräten.

4. Dieses Papier befasst sich nicht mit besonderen zusätzlichen Gefahren der Nutzung von Apps auf mobilen Geräten.[5] Nichtsdestotrotz sollten die Grundsätze dieses Papiers ebenso auf in anderen Diensten eingesetzte Trackingmethoden angewandt werden.

---

[2] Beachten Sie bitte, dass dadurch, dass die Technologie auf IP-Grundlage zunehmend zum Rückgrat der Informationsgesellschaft wird und viele andere früher eigenständige Technologien integriert wurden („Konvergenz"), dies auch die Nutzung von Telefon (IP-Telefonie) und Fernsehen (IPTV), das Lesen digitaler Zeitungen oder jeglicher anderer Medienkonsum mittels digitaler Technologien (einschließlich das Lesen eines E-Buches) mit umfassen kann. Zu einer detaillierten Diskussion der sich daraus ergebenden Gefahren für die Privatsphäre siehe das Working Paper „Privacy Issues in the Distribution of Digital Media Content and Digital Television *[Arbeitspapier zu Themen der Privatsphäre bei der Verbreitung digitaler Medieninhalte und des digitalen Fernsehens]* (Berlin, 4./5.09.2007) dieser Gruppe; URL: http://www.datenschutz-berlin.de/attachments/349/digit_de.pdf.

[3] JICWEBS Reporting Standards *[Grundsätze der Berichterstattung im Internet des Joint Industry Committee for Webstandards]*, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf.

[4] Zum Beispiel die passive Fingerprinting-Technik, die auf dem Hashing des HTTP Endsystemteils bzw. der IP-Adresse des Ursprungs-Browsers basiert.

[5] Siehe zum Beispiel die von der Artikel-29-Datenschutzgruppe (Art. 29 WP) herausgegebene Stellungnahme 02/2013 über Apps auf Smart-Geräten WP 202, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

5. In diesem Papier geht es nicht darum, wie Schutzmaßnahmen umgesetzt werden können (z. B. rechtliche Anforderungen an eine Einwilligung). Anzumerken ist jedoch, dass in manchen Rechtsordnungen zwar je nach Zweck des Webtracking, die ausdrückliche Einwilligung (Opt-in) erforderlich ist, in anderen Rechtsordnungen jedoch die Möglichkeit zum Widerspruch („Opt-Out") für das Webtracking als gültig betrachtet wird, um den Anforderungen des Rechtssystems zu genügen, wenn bestimmte Bedingungen erfüllt sind. Diese umfassen unter anderem die angemessene Benachrichtigung über die Verarbeitung von Daten; Transparenz in der Benachrichtigung; Benachrichtigung zum Zeitpunkt der Sammlung der Daten oder zuvor; und einfache, wirksame und dauerhafte Möglichkeiten zum Widerspruch. Eine Reihe von Beschränkungen kann ebenso vorhanden sein; z. B. in Bezug auf die Verarbeitung sensibler Informationen wie zum Beispiel Informationen über die Gesundheit, über politische oder weltanschauliche Ansichten und die Verhinderung des Tracking von Kindern.

Hintergrund

6. Die technischen Möglichkeiten für die Beobachtung der Aktivitäten der Nutzer auf Web-Sites haben sich in den letzten zehn Jahren vervielfältigt; die „Informationsgesellschaft" hat seitdem schon mehrere grundlegende Veränderungen erfahren.[6] Webtracking entwickelte sich aus sehr bescheidenen Anfängen – als einzelne Provider von Online-Diensten mit der Beobachtung ihrer Nutzer mit dem Ziel der Feststellung begannen, ob ein bestimmter Nutzer diese Web-Site schon zuvor besucht hatte und was dieser Nutzer dort getan hatte – in jüngerer Zeit zu einer schon fast bizarren Vision der Anbieter. In dieser Vision scheint der Anbieter in der Lage zu sein, jeden einzelnen Aspekt des Verhaltens eines erkennbaren Nutzers im gesamten Internet zu beobachten. Dies könnte eine vollständige Verlaufsübersicht über die umfassende Nutzung des Internets einer betroffenen Person über unbegrenzte Zeitspannen hinweg (wortwörtlich von der Wiege bis zum Grab) werden, und diese *[Verlaufsübersicht]* könnte mit Profildaten aus der „Offline-Welt" angereichert werden (einschließlich aller möglichen Aspekte aus unserem Leben, über die die Datenmakler Informationen besitzen; dazu gehören auch Informationen über Finanzen sowie Informationen über zum Beispiel Freizeitgestaltung, Gesundheit, politische bzw. religiöse Überzeugungen und Informationen über Aufenthaltsorte).[7]

7. Diese Entwicklung – die zwar von Anbietern und anderen Interessenten in der Geschäftswelt begrüßt und gefördert und von einigen Politikern auf nationaler und regionaler Ebene unterstützt wird – birgt eine beispiellose Gefahr für die Pri-

[6] Die Literaturübersicht über die Messung der Privatsphäre im Internet, welche als Ergebnis der Konferenz zur Messung der Privatsphäre im Internet (Conference on Web Privacy Measurement, WPM) zusammengestellt wurde, gibt einen ausführlicheren Überblick über die für das Tracking eingesetzten Technologien, URL: http://www.law.berkeley.edu/12633.htm.

[7] In Systemen zur Pflege der Kundenbeziehungen (Customer Ralationship Management, CRM) sind hierfür die üblichen Begriffe Customer Lifetime *[Kundenleben]* und Customer Lifetime Value *[Kundenkapitalwert]*.

vatsphäre aller Bürger in der Informationsgesellschaft. Sie könnte schlimmstenfalls die uns bekannte Welt zu einem globalen Panoptikum wandeln: Das Offline-Äquivalent wäre, wenn uns ein Unbekannter ständig über die Schulter schauen würde, ganz gleich, wo wir uns befinden (auf der Straße oder in der scheinbaren Privatsphäre zu Hause) – oder was wir gerade tun (fernsehen, online einkaufen, Zeitung lesen und sogar noch intimere Tätigkeiten) und ohne dass wir wissen, wann der Unbekannte gerade zuschaut und wann nicht.[8]

8. Die möglichen Auswirkungen einer solchen Entwicklung liegen auf der Hand und sind im Hinblick auf ihre mögliche Schwere nicht zu unterschätzen: Sie kann einige der wesentlichen Grundsätze der Privatsphäre aufheben oder anullieren, – und insbesondere *[die Grundsätze von]* Transparenz und Kontrolle durch die Bürgerinnen und Bürger.[9] Um es noch deutlicher zu sagen: Dies könnte das Ende der Welt (in Bezug auf den Schutz der Privatsphäre) sein, wie wir sie kennen.

9. Die Befürworter dieser Vision behaupten andererseits, dass diese Gefahren entweder gar nicht vorhanden sind oder dass sie versucht haben, sich mit diesen Gefahren zu befassen und sie zumindest zum Teil abzuschwächen: Es gibt einen starken Widerstand seitens mancher Interessenvertreter der Wirtschaft dagegen, anzuerkennen, dass eindeutige Identifikatoren Daten über die Internetnutzung personenbezogene Informationen sind. Eine oftmals vorgebrachte Behauptung ist, dass bei vielen der genutzten Daten die Rückverfolgung auf eine bestimmte Person nicht mehr möglich ist (d. h. die Daten anonymisiert wurden) und dass, sobald dieses erledigt ist, die Daten sich nicht mehr auf eine Person beziehen und deshalb keine Gefahr mehr für die Privatsphäre von Bürgern darstellen würden. Auch wird vorgebracht, dass alle Daten über Verhaltensweisen nur mit Maschinen verbunden sind und – dies ist die Behauptung – in sehr vielen Fällen überhaupt nicht zu einer bestimmten Person zurückverfolgt werden können.

10. Allerdings gibt es für diese Behauptungen keinerlei wissenschaftlichen Nachweis und sie lassen die Tatsache außer Acht, dass Maschinen – und insbesondere Smartphones – zunehmend zu persönlichen Geräten werden und eine Verbindung zu einem jeden individuellen Nutzer leicht ermöglichen. Spuren können auch in zunehmendem Maße über verschiedene Geräten hinweg verbunden werden. Ebenso gibt es einen wissenschaftlichen Nachweis dafür, dass viele anscheinend anonyme Daten (z. B. Informationen über den Aufenthaltsort bei Mobiltelefonen) zu dem betroffenen Nutzer zurückverfolgt werden können (d. h. ihre Anonymisierung wird aufgehoben), wenn die Datenbasis und der zeitliche Rahmen groß genug sind. Jüngere wissenschaftliche Arbeiten lassen sogar vermuten, dass es

[8] Und um die Dinge noch zu verschlimmern, würde diese modernistische Version eines Panoptikums jede einzelne Bewegung einer jeglichen Privatperson und zu einem jeden Augenblick aufzeichnen, unabhängig davon, ob der Wächter gerade hinschaut oder nicht.

[9] Tracking als Technologie ist nicht transparent: Auf technischer Ebene sind in vielen Fällen die Pixel *[Bildpunkte]* (z. B. Web-Beacons *[Code-Fragmente]*) und Mini-Web-Sites (z. B. iFrames) für das menschliche Auge unsichtbar.

grundsätzlich unmöglich ist, „anonyme“ Daten vor einer Deanonymisierung zu schützen, wenn der Zeitintervall für die Beschreibung eines beliebigen Verhaltens groß genug ist (d. h. es ist schon konzeptuell unmöglich, zu garantieren, dass „anonyme“ Daten im Laufe der Zeit nicht zu einer bestimmte Person zurückverfolgt werden können). Wenn dies richtig ist, stellt es eine bahnbrechende Entwicklung dar und würde eine Reihe von Kernannahmen darüber, wie sich die Nutzung verschiedener Arten von Daten auf die Privatsphäre von Personen auswirken kann oder nicht, sinnlos machen.[10]

11. Darüber hinaus und mit leicht anderer Ausrichtung trägt auch die praktische Erfahrung des Alltags dazu bei, die von der Industrie aufgestellten Behauptungen in Frage zu stellen: Werbeanzeigen werden zwar auf technischer Ebene an eine Maschine gerichtet, es ist aber nicht die Maschine, die letzten Endes die sprichwörtlichen „schönen roten Schuhe“ kauft – es ist der oder die Einzelperson. Deshalb kann die Behauptung, dass die Verarbeitung von Daten über Verhaltensweisen für Marketingzwecke sich „nur“ zunächst an Maschinen richtet, sehr wohl als ein Versuch betrachtet werden, unseren Blick als Gesellschaft insgesamt hinsichtlich der Ernsthaftigkeit des Problems zu trüben, da in der Realität der Mensch und nicht die Maschine die einzige Instanz ist, die alle solche Trackingoperation zu einem „Erfolg“ für die Befürworter gestalten kann (d. h., wenn die roten Schuhe schließlich gekauft werden).

Eine kurze Geschichte der Technologien für Beobachtungszwecke

12. Bei dem Versuch, die oben beschriebene Entwicklung bis zu ihren bescheidenen Anfängen hin zurück zu verfolgen, stellt die Entwicklung der „Cookie-Technologie“ vor fast 20 Jahren ein Meilenstein dar: HTTP-Cookies wurden 1994 eingeführt, und zwar in erster Linie, um das „kleine“ Problem der verlässlichen Umsetzung eines virtuellen Einkaufswagens zu lösen. Weil das Hypertext Transfer Protocol (HTTP) überwiegend zustandslos („stateless“) war, konnten Endsysteme bis zu diesem Zeitpunkt keine Zustandsinformationen speichern. Die Speicherung von Zustandsinformationen war jedoch für den virtuellen Einkaufswagen ganz wesentlich, um ausgewählte Artikel beim Shopping-Vorgang zu speichern. Transparenz war schon zu diesem Zeitpunkt ein Thema im Hinblick auf die Privatsphäre, weil die Verwendung von Cookies dem gewöhnlichen Nutzer nicht mitgeteilt wurde. Zu jener Zeit wurden Cookies standardmäßig in den Browsereinstellungen freigegeben und der Nutzer wurde über den Einsatz von Cookies nicht informiert.[11]

[10] Cf. Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization *[Gebrochene Versprechen zur Privatsphäre: Eine Antwort auf das überraschende Versagen der Anonymisierung]*, August 2009. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

[11] RFC 2109, HTTP State Management Mechanism, URL: https://tools.ietf.org/html/rfc2109. Beachten Sie, dass aktuelle Varianten der Speichertechnik für Cookies zum Beispiel auch Flash-Cookies und LSOs (Local Shared Objects) umfassen, die in HTML5 mit entsprechenden Werten verwendet werden.

13. Um Gefahren für die Privatsphäre und die Sicherheit zu entschärfen, die sich daraus ergeben, dass Cookie-Informationen ungewollt zu Betreibern anderer Web-Sites gelangen, wurde die Same-Origin-Policy *[Grundregel desselben Ursprungs, SOP]* eingeführt. Diese Maßnahme bedeutet, dass Cookies nur von derselben Domain gelesen werden konnten, die sie gesetzt hat. Allerdings muss darauf hingewiesen werden, dass das World Wide Web Consortium (W3C) *[Gremium zur Standardisierung der das Internet betreffenden Techniken]* einen neuen Standard vorgeschlagen hat, nämlich das Cross Origin Resource Sharing (CORS)[12], welches den Informationsaustausch domainübergreifend zulässt. Obgleich CORS ein freiwilliger Standard ist, steht er im Widerspruch zur Same-Origin-Policy.

14. Bereits 1998 befasste sich diese Gruppe[13] mit verschiedenen Fragestellungen zur Privatsphäre in Verbindung mit der systematischen Sammlung oder Nutzung personenbezogener Daten im Internet.[14] In dem Arbeitspapier beschäftigte sie sich mit P3P (Platform for Privacy Preferences Project) *[Plattform zum Austausch von Datenschutzinformationen]*, einem vom W3C entwickelten Protokoll, welches darauf ausgelegt war, Cookies von Dritten zu blockieren, es sei denn, dass die vom Nutzer besuchte Web-Site eine für den Nutzer akzeptable P3P-Policy *[P3P-Datenschutzrichtlinie]* anbot.[15] Allerdings hat nur ein großer Browserhersteller den Standard umgesetzt. Infolgedessen wurde P3P in keinem breiten Umfang im Internet angenommen.

15. Third Party Cookies *[Cookies von Dritten]* sind zum Lebensnerv der komplexen digitalen Werbeindustrie geworden. 2008 diskutierten leitende Marketingfachleute aus Webtracking-Unternehmen die Zukunft von Webanalyse und Webstatistik. Die Zukunft in fünf Jahren stellte man sich so vor, dass die traditionelle Webstatistik über die Besuche der Web-Site (nachfolgend: First und Third Party Analytics) mit Analysedaten anderer Webanalysedienste zusammengeführt wird, zu denen auch zum Beispiel Videodienste, Widgets *[Komponenten von Benutzeroberflächen]*, soziale Netzwerke, Spiele und Suchmaschinen gehören (nachfolgend: Web Analytics).[16]

---

[12] Cross-Origin Resource Sharing, URL: http://www.w3.org/TR/cors/ (abgerufen am 30. Mai 2013).

[13] International Working Group on Data Protection in Telecommunications *[IWGDPT,Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation]*.

[14] Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb; (Hong Kong, 15.04.1998), http://www.datenschutz-berlin.de/attachments/177/priv_de.pdf

[15] Das Platform for Privacy Preferences Project (P3P) ermöglicht Web-Sites, ihre jeweiligen Methoden für den Umgang mit Privatsphäre in einem Standardformat auszudrücken, das automatisch abgefragt und von Nutzeragenten *[Anwendungssoftware, z. B. browser]* leicht interpretiert werden kann. P3P Nutzeragenten ermöglichen den Nutzern, über Methoden der Web-Site Kenntnis zu erlangen (sowohl in maschinenlesbaren, als auch für Menschen lesbaren Formaten) und Entscheidungsprozesse gegebenenfalls auf der Grundlage dieser Methoden zu automatisieren. Nutzer müssen nicht auf jeder von ihnen besuchten Web-Site die Datenschutzrichtlinien lesen. URL: http://www.w3.org/P3P/.

[16] Omma Global Measurement 3.0, http://www.webmetricsguru.com/archives/2008/09/measurement-30-on-the-next-5-years-omma-global-day-2/.

16. Heutzutage stellen Daten aus Webanalysen eine neue Form des wirtschaftlichen Wertes dar. Zwar stellt diese Gruppe nicht den Nutzen in Frage, den das Messen des Verbraucherverhaltens für das Online Behavioural Advertising (OBA) *[Online-Werbung mit Nutzung des Surfverhaltens der Nutzer]* (in Echtzeit) bringen kann, doch ist sie der festen Überzeugung, dass solche Methoden nicht auf Kosten der Rechte von Privatpersonen im Hinblick auf Privatsphäre und Datenschutz eingesetzt werden dürfen.

Webtracking

17. Das Webtracking umfasst die Erhebung und nachfolgende Speicherung, Nutzung oder den Austausch von Daten des individuellen Online-Verhaltens über eine Vielzahl von Web-Sites durch den Einsatz von Cookies, JavaScript oder jeglichen anderen Formen des Device Fingerprinting *[Ermittlung von Einzelpersonen anhand von Eigenschaften technischer Geräte, z. B. Browser-Einstellungen]*. Webtracking-Technologien ermöglichen einen konstanten Fluss von Informationen über Nutzer in Echtzeit, wie zum Beispiel Registrierungsdaten, Daten über die Online-Suche, verhaltensbezogene Daten, Statistiken über Besuche von Web-Sites und Conversion-Daten *[Daten über Umwandlung von Klicks in Handlungen, wie z. B. Einkäufe]*, die alle widerspiegeln, auf welche Art und Weise ein Nutzer auf individuelle Angebote reagiert hat. Diese Daten können genutzt werden, um auf die Interessen, politischen Überzeugungen oder Krankheiten eines Nutzers zu schließen. Sie können mit dem Ziel verarbeitet werden, den Zustand oder das Verhalten einer bestimmten Person einzuschätzen, beides auf eine bestimmte Art und Weise zu behandeln oder zu beeinflussen. Daten über individuelles Verhalten lenken geschäftliche Entscheidungen auf der Grundlage von Kundenprofilen. Eine Kaufabsicht kann aus der vermuteten digitalen Identität einer Person abgeleitet werden. Der Wert eines potenziellen Kunden wird mit der Möglichkeit in Verbindung gebracht, ihn zum Kauf einer Ware zu bringen.

18. Webtracking-Technologie ist auf mobilen Geräten vorhanden. Privatpersonen tauschen ein mobiles, „smartes“ Gerät untereinander sehr wahrscheinlich nicht aus, und daher ist die Verbindung zwischen dem Gerät und der Privatperson enger als zum Beispiel zwischen Mensch und Desktop-Computer. Mobile Geräte enthalten eindeutige Geräte-Identifikatoren, wie zum Beispiel besondere Identifikatoren für Werbung,[17] die Unique Device ID (UDID) *[eindeutige maschinenlesbare Kennung]*, die MAC-Adresse (Media Access Control) *[Hardware-Adresse z. B. jedes einzelnen Netzwerkadapters]*, die Bluetooth MAC-Adresse, die NFC MAC-Adresse (Near Field Communications) *[international genormter Standard zur Datenübertragung im Nahbereich]*, die International Mobile Subscriber Identifier (IMSI, eine eindeutige SIM-Kartennummer) und die International Mobile

[17] Um zum Beispiel Frequency Capping durchführen zu können (Kontrolle der Häufigkeit, wie oft einem Nutzer eine Anzeige von Online-Werbung eingeblendet wird), Behavioral Ads *[auf Surfverhalten beruhende Anzeigen]* einzublenden und die Reichweite und Wirksamkeit einer Werbeaktion zu messen.

Equipment Identifier (IMEI) *[eindeutige Seriennummer bei Mobilgeräten]*. Diese Identifikatoren kann der gewöhnliche Nutzer nicht ändern. Über eindeutige Identifikatoren hinaus können mobile, „smarte" Geräte eine große Menge an Daten enthalten, wie zum Beispiel Nutzernamen, Passwort, Alter, Geschlecht und das Adressbuch. Solche Geräte können genaue verhaltensbezogene Daten über den Aufenthaltsort eines Nutzers offenlegen. Präzise Geopositionsdaten stehen für Browser auf mobilen, „smarten" Geräten fertig nutzbar zur Verfügung.

19. Webtracking-Technologie wird auf verschiedene Art und Weise eingesetzt. Eine digitale Datenspur kann sich aus der unabsichtlichen oder ungewollten Offenlegung von Daten ergeben und zu einer nicht erforderlichen Offenlegung (personenbezogener) Daten führen. Es gibt sehr viele verschiedene Wege zur Erzeugung einer digitalen Datenspur. Zum Beispiel könnte der Manager einer digitalen Anzeigenaktion dem Nutzer, Browser oder Gerät einen eindeutigen Identifikator zuordnen. Ein anderer Weg ist die Personalisierung von Verweisinformationen durch Hinzufügen von Zielgruppeninformationen (Mikroprofile) beim Surfen im Internet, sodass andere Web-Sites, die sich auch an der Werbeaktion beteiligen, den Nutzer, Browser oder das Gerät ebenso nachverfolgen können. Ein drittes Beispiel ist die Korrelation eindeutiger Identifikatoren mit aus früheren Besuchen auf einer bestimmten Web-Site gesammelten Daten. Und ein viertes Beispiel ist, dass Webtracking für eine Werbeaktion durch die Kombination neuer Trackingdaten (über einen Nutzer, einen Browser oder Gerätedaten) mit zuvor auf einer bestimmten Web-Site gesammelten Daten oder mit von einem anderen oder Dritten erhaltenen Daten stattfinden kann. Ein letztes Beispiel sieht die Nutzung von Cookie Matching-Services *[Dienste zum Abgleich von Cookies auf besuchten Web-Sites mit dem auf dem Computer des Nutzers abgelegten Cookie]* vor, welche digitale Spuren desselben Nutzers, Browsers oder Gerätes mit der Nutzung verschiedener Teile des Internets verbinden.[18]

20. Webtracking besteht aus mehreren automatisierten Schritten, beginnend mit der Erhebung von Daten über die Internet-Nutzung, der Speicherung dieser Daten und der Nutzung der Daten. Durch neue Zusammenstellung der Daten, Korrelation und ihre Dekontextualisierung können Internetdaten dazu genutzt werden, sehr detailgenaue Profile und Vorhersagen individuellen Verhaltens aufzubauen. Schließlich führt das Webtracking zur tatsächlichen Anwendung des Profils einer bestimmten Person.

21. Daten können mittels verschiedener Dienste im Internet in einer Graphen-Datenbank gespeichert werden.[19] Die Struktur des Graphen ermöglicht die He-

[18] Siehe zum Beispiel URL: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is.

[19] Ein Graph basiert auf der Graphentheorie, die einen mathematischen Ansatz für die Entwicklung paarweiser Beziehungen zwischen Objekten darstellt. Eine Graphdatenbank speichert Graphen, welche im wesentlichen Strukturen mit Knoten, Ecken und Eigenschaften darstellen. Die Eigenschaften können Metainformationen über die Knoten und Ecken enthalten.

rausbildung von Verhaltensmustern, die sonst unentdeckt geblieben wären. Webtracking-Daten in einem Graphen können aus sich selbst heraus oder durch Kombination mit anderen Daten aus verschiedenen Quellen aussagekräftige Muster über das Nutzerverhalten generieren. Zum Beispiel geben einzelne eindeutige Identifikatoren, die direkt oder indirekt mit einem Nutzer oder Computer verbunden sind, zwar nur wenige Informationen über den gelegentlichen Surfer bekannt, doch die Sammlung eindeutiger Identifikatoren bietet einen tief greifenden Einblick in die Gewohnheiten und das Surfverhalten einer Person im Internet. Die Sammlung eindeutiger Identifikatoren kann zur Erstellung einer digitalen Identität benutzt werden.

Webtracking und das Recht auf Privatsphäre und Datenschutz der Privatperson

22. Ein Schlüsselgrundsatz für eine große Bandbreite internationaler Rechtsordnungen ist das Recht auf Privatsphäre, das der Internetnutzer unabhängig von der Technologie besitzt. Schlüsselelemente sind Transparenz, Kontrolle und Beachtung des Kontextes. Es ist eine Gefahr für die Privatsphäre, dass Nutzern nicht bewusst ist, dass ihre Spuren verfolgt werden. Webtracking als Prozess verwendet eine Reihe technischer Tools, die die Gelegenheit der Mitteilung an die Nutzer begrenzen. Zum Beispiel sind Pixel (z. B. Web-Beacons) und Mini-Web-Sites (z. B. iFrames) für das menschliche Auge unsichtbar und ihre Einbindung in eine Web-Site löst eine automatische HTTP-Anfrage einschließlich der Möglichkeit des Setzens von und des Zugangs zu Cookies aus, die ihrerseits eindeutige Identifikatoren enthalten.

23. Viele Webtracking-Technologien wurden entwickelt und in der Wirtschaft eingesetzt, ohne dass den Nutzern Informationen darüber bereitgestellt wurden, wessen Daten gesammelt werden und ohne ihnen eine Wahlmöglichkeit zu bieten. Meldungen des Nutzers, die als Ausdruck der Ablehnung des Tracking verstanden werden könnten, wurden nicht beachtet und technische Methoden gegen einige Trackingmethoden wurden aktiv umgangen, zum Beispiel durch erneutes Hervorbringen gelöschter Cookies, (passives) Fingerprinting und das Umgehen von Browsereinstellungen. Erst als dieses Verhalten aufgedeckt und öffentlich kritisiert wurde, haben die entsprechenden Parteien ihre Verpflichtung akzeptiert, den freien Willen des Nutzers zu achten. In solchen Fällen wurden manchmal Opt-Out-Programme hinzugefügt, was aber oft zu schwerfälligen Mechanismen mit nur begrenztem Nutzen für den Nutzer führte. Diese Fälle haben im Hinblick auf das Vertrauen der Nutzer in die Verlässlichkeit und Aufrichtigkeit aller Internetanbieter einen großen Schaden verursacht und die gesunde Entwicklung innovativer Internetdienste untergraben.

24. Webtracking bedeutet in vielen Rechtsordnungen die Verarbeitung personenbezogener Daten, und zwar aufgrund der Tatsache, dass die Technologie die

Individualisierung oder Identifizierung[20] von Nutzern bzw. das Treffen automatisierter Entscheidungen über sie ermöglicht. Ein Beispiel einer solchen Praxis könnten Maschinen für automatische Entscheidungen mit Algorithmen in Real Time Bidding Plattformen *[Verfahren für Werbungtreibende für das Bieten auf Werbeplätze in der Online-Werbung in Echtzeit]* für personalisierte Werbung auf der Grundlage von Nutzerverhalten sein.

25. Es gibt einen starken Widerstand seitens einiger beteiligter Interessengruppen gegen die Einstufung eindeutiger Identifikatoren in Webdaten als personenbezogene Informationen. Eine oftmals vorgebrachte Behauptung ist die, dass sobald Daten anonymisiert wurden,[21] diese Daten nicht mehr personenbezogen sind. Es sollte jedoch klar sein, dass auch ein „zweckgebundenes" Element dafür verantwortlich sein kann, dass Informationen „sich" auf eine bestimmte Person „beziehen" oder diese Person betreffen können.[22]

Die potenzielle Wirkung (oder mangelnde Wirkung) des „Do Not Track" (DNT) *[nicht verfolgen]* – eine Fallstudie

26. Im September 2011 gründete das W3C die Tracking Protection Working Group[23] *[Arbeitsgruppe zum Schutz vor Webtracking]*. Die Gruppe arbeitet an einem Do-Not-Track Standard (DNT). Alle großen Browserhersteller haben sich zwar dazu verpflichtet, den Standard umzusetzen (und die meisten haben bereits den HTTP-Header umgesetzt), allerdings dauert bei jenen Interessengruppen, die den DNT:1 Request[24] beachten werden, eine offene Diskussion über Teile des freiwilligen Standards an. Einige Interessengruppen haben angedeutet, das DNT-Flag aus verschiedenen Gründen nicht beachten zu wollen. Der übergreifende Erfolg von DNT ist von der tatsächlichen Beachtung des DNT-Flag durch die empfangende Organisationen und der tatsächlichen Annahme des DNT-Standards im gesamten Internet durch alle Interessengruppen abhängig.

---

[20] Erwägungsgrund Nr. 26 der allgemeinen Datenschutzrichtlinie 95/46/EG: Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html] (…), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[21] De-Identifikation von Daten einer bestimmten Person bedeutet das Entfernen, Ändern, Kumulieren, Anonymisieren oder anderweitige Manipulation von Daten.

[22] Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten (Arbeitspapier WP136), S. 10 URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf .

[23] Die Aufgabenstellung der Tracking Protection Working Group besteht darin, die Privatsphäre und Kontrolle durch die Nutzer zu verbessern, und zwar durch die Definition von Mechanismen zum Ausdruck von Festlegungen durch Nutzer rund um das Webtracking und zum Blocken oder Zulassen von Webtracking-Elementen, http://www.w3.org/2011/tracking-protection/charter .

[24] Im aktuellen Entwurf des DNT-Standards bedeutet das Aussenden von „0"-Meldungen das Einverständnis mit Tracking und „1" zeigt an, dass Tracking NICHT gewünscht wird.

27. Standardeinstellungen im DNT und die Standardaktionen der Webtracking-Organisationen bleiben wiederum äußerst wichtig. Damit DNT ein wirksames Instrument für die Umsetzung der Kontrolle durch den Benutzer ist, ist es somit äußerst wichtig, dass die Betreiber von Webtracking auch sicher sein können, dass die von ihnen empfangene DNT-Meldung eine echte Anzeige der Wünsche des Nutzers darstellt. Fehlt dem Nutzer eine solche Wahlmöglichkeit mit umfassender Informationen, muss eine Webtracking-Organisation annehmen, dass einem Nutzer das Webtracking nicht bewusst ist, und deshalb muss sie dann von der Standardeinstellung ausgehen, als ob sie nämlich eine DNT:1 Meldung erhalten hätte, welches den Wunsch des Nutzers anzeigt, dass Tracking unerwünscht ist.

28. Jede für die Zwecke des Webtracking eingesetzte Technologie muss angemessen sein. Weltweit angewandte Datenschutzgrundsätze basieren auf der Vorstellung, dass Daten für spezifizierte, explizite und rechtmäßige Zwecke gesammelt und nicht auf eine Art und Weise weiterverarbeitet werden sollten, die mit solchen Zwecken unvereinbar ist. Die Verarbeitung von Daten sollte angemessen und relevant sein und nicht exzessiv im Verhältnis zu den Zwecken stehen, für die sie gesammelt bzw. weiterverarbeitet werden.

29. Schließlich muss eine jede Technologie gerichtsfest sein, wenn sie dazu beitragen soll, dem Schutze der Privatsphäre zu dienen. DNT läuft Gefahr, ein Werkzeug zu bleiben, durch das ein Nutzer Wünsche gegenüber Serviceprovidern der Informationsgesellschaft ausdrücken kann, ohne dass dieses ein wirksames Instrument für einen konstruktiven Dialog darstellt. Dies lässt den Nutzer selbst oder eine jede öffentlich-rechtliche (oder private) Körperschaft, die mit die Durchsetzung solcher Wünsche oder Regelungen beauftragt ist (einschließlich der entsprechenden rechtlichen Verpflichtungen, die Auswahl einer Einzelperson zu beachten) im Hinblick auf solche Anbieter mit leeren Händen dastehen. Manche Interessenvertreter der Wirtschaft versuchen die Position zu verteidigen, dass das DNT keine Verpflichtung zur Beachtung eines Wunsches darstellt. Zwar ist diese Interpretation mehr als zweifelhaft, doch bleibt die Tatsache im Raume stehen, dass der Beweis schwer zu führen ist, ob ein solcher Wunsch beachtet oder missachtet wurde.[25] Mit anderen Worten, das DNT könnte aus der Perspektive der Umsetzung ein Placebo anstatt eines wirksamen Heilmittels bleiben, und als solches würde es auch nutzlos bleiben.

Empfehlungen

30. Ungeprüftes Webtracking kann das Gleichgewicht zwischen Dienstanbietern und Privatpersonen auch im Hinblick auf den Schutz der Privatsphäre verändern. Die Arbeitsgruppe unterstreicht, dass Kontext, Transparenz und Kontrolle äußerst wichtige Elemente auch im Kontext des Webtracking bleiben.

[25] Ein externes Audit könnte bei der Lösung von zumindest Teilen der oben beschriebenen Probleme eine wichtige Rolle spielen, würde aber andererseits das Ökosystem noch komplexer gestalten.

31. Um zur Lösung der Gefahren für die Privatsphäre der Privatperson beizutragen, gibt die Arbeitsgruppe die folgenden Empfehlungen an die verschiedenen Interessenvertreter, die im Ökosystem des Webtracking eine Rolle spielen.

Wiedereinführung der Beachtung von Kontext und Zweckbegrenzung als Kerngrundsätze für jede Nutzung personenbezogener Daten:

- Umsetzung von Vorsichtsmaßnahmen für jede (automatisierte) Erhebung, Verarbeitung und die Praxis des Austausches von Daten, sodass in einem bestimmten Kontext gesammelte Daten nicht in einem anderen Kontext angewandt werden können;

- Information über den Zweck der Erhebung von Daten gleich zu Beginn und im Vorhinein und keine Änderung des Zweckes ohne erneute Information und Wahlmöglichkeit.

Wiederherstellung der Transparenz:

- Keine Verwendung unsichtbarer Trackingelemente;

- Mindestens eine verständlich formulierte Mitteilung an den Nutzer, wenn das Anwendungsprogramm im Begriff ist, eine Webtracking-Kennzeichnung an den Empfangsserver zu senden oder eine solche Kennzeichnung vom Ursprungsserver zu empfangen;

- Einblenden einer für den Nutzer ausreichend erkennbaren Anzeige[26] immer dann, wenn Webtracking gerade stattfindet;

- Anzeige eines Hinweises, dass Webtracking gerade stattfindet, der auch für besondere Nutzergruppen, einschließlich der Sehbehinderten, zur Verfügung steht.

Rückverlagerung der Kontrollmöglichkeit zum Nutzer:

- Einrichtung von Mechanismen, die den Nutzern die Ausübung ihres Rechtes auf Privatsphäre und Datenschutz im Internet ermöglichen und kein Einsatz (neuer) Trackingmethoden, welche keine Kontrolle durch den Nutzer ermöglichen; Angebot der Möglichkeit zur expliziten Auswahl bezüglich des Tracking an Nutzer – wenn Browsersoftware installiert, aktiviert oder aktualisiert wird, muss der Nutzer eine Wahlmöglichkeit besitzen;

[26] Ein besonderes Augenmerk muss darauf gerichtet werden, sicherzustellen, dass keine Nutzergruppe des Internets benachteiligt oder anderweitig diskriminiert wird, zum Beispiel aufgrund einer Behinderung.

- Besitzt der Browser keine Anwenderschnittstelle (user interface), sollte die Standardeinstellung so sein, dass das Tracking des Nutzers nicht stattfindet;

- Einräumen der Möglichkeit für Nutzer zur Änderung der Auswahl- und der Änderungseinstellungen nach der ursprünglichen Entscheidung und zu jeder Zeit; Schaffung einer einfachen Prüfmöglichkeit für den Nutzer für die (automatisierten) Wahlmöglichkeiten, die für das Webtracking getroffen wurden; Erinnerung des Nutzers daran, dass Wahlmöglichkeiten bezüglich der (automatisierten) Einstellungen für das Webtracking jederzeit widerrufen werden können und Sicherstellung, dass eine Änderung der Auswahl technisch auf einfache Art und Weise möglich ist, welche der Einzelperson keine ungebührliche Last auferlegt.

- Beachten von Mitteilungen, wenn das Anwendungprogramm meldet, dass Tracking abgelehnt wird;

- Unterlassung des (passiven) Fingerprinting, zum Beispiel durch Mining *[Durchsuchen]* der vom Nutzer generierten Daten (wie zum Beispiel Service Configurations oder User Agent Strings *[Zeichenkette, mit der sich der Browser identifiziert]*), um daraus eine eindeutige Benutzerkennung abzuleiten (Device Fingerprinting), wenn ein Nutzer mitgeteilt hat, dass er Tracking ablehnt.

- Sicherstellen, dass der Einsatz einer jeden Technologie mit dem Ziel, dem Nutzer Wahlmöglichkeiten zu geben, prüffähig ist und von den zuständigen, mit der Umsetzung von Bestimmungen beauftragten privaten oder öffentlich-rechtlichen Körperschaften auch überprüft werden kann, und insbesondere die Umsetzung der in den verschiedenen vorhandenen Rechtssystemen niedergelegten Bestimmungen, welche ihrerseits die Grundlage für den Schutz der Privatsphäre der Privatperson in vielen Rechtsordnungen weltweit bilden.

Arbeitspapier und Empfehlungen zu der Veröffentlichung personenbezogener Daten im Web, der Indexierung des Inhalts von Websites und dem Schutz der Privatsphäre

– Übersetzung –

1. Hintergrund

Einer der wesentlichen Stützpfeiler des Datenschutzes war schon immer das Recht des Betroffenen, über seine Daten zu bestimmen. Ein wesentliches Element dieser Kontrolle ist das Recht, die eigenen Daten gelöscht zu bekommen, wenn sie rechtswidrig verarbeitet werden oder wenn der Betroffene ihrer Verarbeitung nicht länger zustimmt. Der kürzliche Vorschlag der Europäischen Kommission für einen neuen Regulierungsrahmen versucht, dieses Recht zu stärken, indem er ein „Recht auf Vergessen" durch andere und im Web vorsieht. Dies gilt unbeschadet von solchen Fällen, in denen es ein legitimes und rechtlich gerechtfertigtes Interesse gibt, Daten veröffentlicht und sichtbar zu halten, wie etwa in Medienarchiven oder zum Zwecke historischer Aufzeichnungen, und es ist klar, dass das Recht auf Vergessen nicht a priori Vorrang vor dem Recht auf freie Meinungsäußerung oder der Medienfreiheit haben kann[1].

Angesichts der Struktur des Webs sind viele Einzelfragen im Hinblick darauf, wie ein solches „Recht auf Vergessen" implementiert werden könnte, sowohl auf der technischen als auch auf der juristischen Seite immer noch ungelöst. Personenbezogene Daten (und jegliche andere Informationen), werden sehr wahrscheinlich öffentlich zugänglich bleiben, wenn sie einmal online veröffentlicht sind. Sogar wenn sie auf der ursprünglichen Webseite gelöscht werden, können sie vor der Löschung auf anderen Seiten verlinkt oder gespiegelt werden. Das Web weiß nicht zu „vergessen" und gegenwärtig ist kein einfaches technisches Werkzeug verfügbar, das die systematische Löschung von Daten im Web sicherstellen könnte (d. h., dem Web das Vergessen beibringen könnte). Kurz gesagt, es gibt keinen „Löschknopf" und es ist zweifelhaft, ob es ihn jemals geben wird.

Dennoch gibt es bereits heute Wege, das Recht des Einzelnen auf Vergessen in einem gewissen Ausmaß zu schützen, indem man sich Werkzeuge zu Nutze macht, die Administratoren von Webseiten zur Verfügung stehen[2], um die freie Verfüg-

[1] The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Viviane Reding SPEECH/12/26, Innovation Conference Digital, Life, Design, München, 22. Januar 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26; für eine Kritik dieses Ansatzes s. Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88

[2] Eine solche Sammlung von Werkzeugen sind die Google Webmaster Tools, die es Webmastern ermöglichen, zu sehen, wie Google ihre Site durchsucht und indexiert, und es Webmastern ermöglicht, zu beeinflussen, wie die indexierten URLs angezeigt werden. Ein Link zu den Werkzeugen ist unter http://www.google.ca/webmasters/ verfügbar.

barkeit personenbezogener Daten zu begrenzen, wie auch durch Nutzbarmachung der Möglichkeiten von Suchmaschinen. Im gegenwärtigen Web könnte das Recht auf Vergessen[3] besser als ein „Recht, nicht gefunden zu werden" interpretiert und umgesetzt werden.

2. Die Aussichten der Nutzer, die Kontrolle über ihre personenbezogenen Daten im Web zurückzugewinnen

Die zunehmende Veröffentlichung personenbezogener Daten im Web in den letzten Jahren hat zu neue Herausforderungen und Risiken des Schutzes der Privatsphäre der Bürger Anlass hervorgerufen und gleichzeitig zur Verschärfung existierender Risiken geführt. Das Aufkommen sozialer Netzwerke hat in diesem Zusammenhang eine besonders wichtige Rolle gespielt[4].

Während in diesem Zusammenhang Technologien zur Förderung der Veröffentlichung und verfügbar machen von Daten – einschließlich personenbezogener Daten – im Web dramatische Fortschritte gemacht haben, scheint die Entwicklung von Technologien zur Kontrolle der Verfügbarkeit solcher Daten im Web immer noch in den Kinderschuhen zu stecken. Während Arbeiten für ein „policy-aware Web"[5] in der vergangenen Dekade stattgefunden haben, scheinen wir immer noch weit von jeglichen effektiven, einfach zu nutzenden und breit verfügbaren Werkzeugen entfernt zu sein, die es Bürgern ermöglichen würden, die Kontrolle über ihre eigenen Daten auch nur in einem begrenzten Maß (zurück-) zu gewinnen, wenn diese einmal im Web veröffentlicht worden sind.

Ein mögliches Entwicklungsziel für solche Technologien könnte die Förderung der Löschung aller Kopien von Daten auf jeglichen Geräten oder in jeglichen Speichern sein, in denen sie aufbewahrt werden. Gegenwärtig könnte dies wohl Probleme hinsichtlich der Skalierbarkeit aufwerfen (sogar wenn ein automatisierter Ansatz gewählt wird), besonders, wenn Daten im Laufe der Zeit von der Gemeinschaft der Nutzer im Web verbreitet, weiter verfeinert oder re-kontextualisiert worden sind. Es gibt gegenwärtig keine technische Möglichkeit, alle Kopien eines Objekts und Kopien von Informationen, die mit diesem Objekt im Web zusammenhängen, zu identifizieren und zu lokalisieren. Allerdings könnte dies in einem zukünftigen „policy-aware Web" möglich sein.

---

[3] Man beachte, dass der Ausdruck „Recht auf Vergessen" in diesem Papier in einem weiteren Sinne genutzt wird als in dem Entwurf der Datenschutzgrundverordnung der Europäischen Union, und dass dieses Papier keine Aussage enthält, ob ein „Recht auf Vergessen" in dieser Verordnung umgesetzt werden soll oder nicht.

[4] Vgl. Bericht und Empfehlung dieser Gruppe zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum" (Rom (Italien), 3. – 4. März 2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf

[5] Für einige existierende Vorschläge zur Schaffung eines „policy-aware Web" vgl. Fußnote 27 auf Seite 10 des „Rome Memorandum" (Fußnote 4 oben). Das Konzept des policy-aware web kombiniert verschiedene existierende Technologien, namentlich strukturierte Daten, Identitätsmanagement, Zugriffskontrolle und „sticky policies" (d. h. Nutzungsregeln, die zusammen mit den Daten selbst verbreitet werden).

Für neu erzeugte Daten könnte die Verfügbarkeit im Web durch das Setzen von zeitlichen Begrenzungen (Verfallsdaten) im Bezug auf das jeweilige Objekt begrenzt werden. Dies kann auf vielen Wegen erreicht werden. Beispielsweise könnte man Daten mit „aktiver" (ausführbarer) Software verbinden, die interveniert, wenn das Verfallsdatum erreicht ist, um die Anzeige der Daten auf einem Bildschirm zu deaktivieren oder die Möglichkeit, Screenshots von einem Bild zu erstellen, zu blockieren oder den ursprünglichen Inhalt zu löschen oder zu verschlüsseln. Alternativ können Daten auch mit einem Verfallsdatum „markiert" werden, sodass alle Server, die mit dem Objekt umgehen, dieses Datum berücksichtigen und die Daten nach dem Verfallsdatum entfernen können.

Weitere interessante Beispiele, wie die Lebenszeit neu generierter Daten im Web angepasst werden kann, werden von einigen anderen neu entstehenden Anwendungen gegeben. Zum Beispiel können Nutzer ein sicheres Overlay-Netz benutzen, das die Sichtbarkeit von Inhalten, wie z. B. einer Nachricht oder eines Bildes durch Nutzung von Ende-zu-Ende-Sicherheit und Zugriffskontrollregeln auf eine Gruppe beschränkt, die zu dem selben Overlay-Netzwerk gehört. In wiederum anderen Anwendungen bleibt eine Textnachricht im Mobilfunk bis zu einem bestimmbaren Verfallsdatum zu einem Nutzer verfügbar. Schließlich können „Nutzer-zentrierte" Lösungen genannt werden, bei denen der legitime Eigentümer eines Datums selektiv Zugriff darauf gewähren kann, indem er Links zu dem Ort veröffentlicht, wo die Daten in Wirklichkeit nur in einem spezifiziertem Zeitraum gespeichert sind.

Diese Beispiele können als Bausteine für ein zukünftiges „policy-aware Web" dienen. Allerdings ist eine Menge gründlicher Forschung und Entwicklung nötig, um diese Elemente zu effektiven Werkzeugen für den besseren Schutz der Privatsphäre der Bürger weiterzuentwickeln. Die Arbeitsgruppe ruft die relevanten Akteure in diesem Feld (Industrie, Wissenschaft und Regierungen) dazu auf, ihre Anstrengungen weiter zu verstärken, um hier Fortschritte zu machen.

3. Beschränkung der Verfügbarkeit personenbezogener Daten im Web durch Kontrolle ihrer Indexierbarkeit durch Suchmaschinen

Ein weiter Baustein zur Beschränkung der Verfügbarkeit und ein Beitrag zur Löschbarkeit von Daten im gegenwärtigen Web besteht in der Beschränkung ihrer Verfügbarkeit in den Ergebnissen von Anfragen bei Suchmaschinen[6]. Dies ist bereits jetzt technisch möglich und steht Website-Administratoren als Option zur Verfügung. Sie beruht im Wesentlichen auf zwei Alternativen: Dem „robots.

[6] S. auch Recommendation CM/Rec(2012)3 des Europarats zum Schutz der Menschenrechte in Bezug auf Suchmaschinen.

txt-Protokoll“[7] und der Nutzung von an ein Objekt gebundenen Markierungen („tags“), um zu signalisieren, dass ein bestimmter Inhalt oder eine bestimmte Seite nicht von einer Suchmaschine indexiert werden soll.

Das „robots.txt-Protokoll“ arbeitet mit einem kleinen Satz von Instruktionen, die in einer Text-Datei codiert sind (der „robots.txt“-Datei), die im Wurzelverzeichnis einer Domain enthalten ist (z. B. http://example.com/robots.txt). Die Datei wird, falls sie vorhanden ist, von einem Crawler (einem Programm, das von Suchmaschinen genutzt wird, um eine Momentaufnahme einer Website zu erstellen) vor der Indexierung der jeweiligen Website gelesen. Die betreffenden Instruktionen erlauben es, bestimmte Crawler dazu aufzufordern, bestimmte Dateien und/oder Verzeichnisse auf der Website zu ignorieren. Die Instruktionen werden von Crawlern durch Textvergleich alphanumerischer Zeichenketten in der Reihenfolge ausgeführt, in der sie in der robots.txt-Datei enthalten sind. Zu den Anwendungsgrenzen des Protokolls zählen das Fehlen einer ausreichenden Skalierbarkeit, dass es mit ftp-Servern nicht funktioniert und dass die Information verloren geht, wenn Inhalte von einer Website kopiert werden[8].

Alternativ können verschiedene Kategorien von Markierungen („tags“) als Attribute einer spezifischen Web-Seite genutzt werden (aber auch in Verbindung mit individuellen Elementen einer spezifischen Seite, wie einem Bild oder einer Datei darin), um zu signalisieren, dass das Objekt/die Seite nicht in die Ergebnisse einer Suchanfrage aufgenommen werden sollte.

Es sollte betont werden, dass diese Ansätze beide vollständig auf Netz-Etikette (d. h. auf die Kooperation der betroffenen Parteien) basieren. Als solche sind sie nur sehr schwer durchzusetzen. Ihre Implementierung durch Websites und Einhaltung durch Suchmaschinen ist völlig freiwillig. Während sie die Risiken der Indexierung, die durch Verlinkung von Webseiten Dritter verursacht werden, abschwächen können, können sie nicht per se sicherstellen, dass ein bestimmtes Informationsobjekt niemals durch eine Suchmaschine indexiert werden wird, besonders, wenn dieses Objekt öffentlich zugänglich ist und von anderen Webseiten mit anderen Zugangsregeln für Crawler verarbeitet werden kann[9].

---

[7] Das „robots.txt-Protokoll“ wird auch als „Robots Exclusion Protocol“ und als „Robots Exclusion Standard“ bezeichnet. Das Protokoll ist in einem abgelaufenen „Internet Draft“ der IETF definiert, online verfügbar unter http://www.robotstxt.org/norobots-rfc.txt.

[8] Manchmal können außerdem Veränderungen bei Web-Inhalten und/oder Präferenzen bei der Indexierung nicht in Suchergebnissen widergespiegelt werden. Es hat sich als bedeutsames Problem erwiesen, Suchmaschinen dazu zu bringen, ihre Indizes zu aktualisieren.

[9] S. in dieser Hinsicht auch die Empfehlungen, die im „gemeinsamen Standpunkt zu Datenschutz bei Suchmaschinen im Internet“, wie 1998 verabschiedet und 2006 überarbeitet, enthalten sind; http://www.datenschutz-berlin.de/attachments/237/WP_Suchmaschinen_de.pdf

4. Empfehlungen für Website-Administratoren

Website-Administratoren spielen eine entscheidende Rolle in den beiden oben beschriebenen Kategorien der Löschung, und zwar durch ihre Möglichkeit, die Verfügbarkeit von Daten und die Indexierbarkeit von Objekten zu begrenzen. Um zu den o. g. Zielen beizutragen, gibt die Arbeitsgruppe die folgenden Empfehlungen:

- Betreiber von Websites sollten ihre Nutzer darüber informieren, welche personenbezogenen Daten sie aufbewahren und für welche Zwecke. Sie sollten ihren Nutzern einen einfachen Mechanismus für die Auskunft über ihre personenbezogenen Daten zur Verfügung stellen, und ihnen erlauben, diese zu berichtigen und/oder dauerhaft zu löschen, wie es in der existierenden Datenschutzgesetzgebung vorgesehen ist. Solche Auskunftsmechanismen sollten nutzerfreundlich sein und sollten nicht zu zusätzlichen Kosten für Nutzer führen oder ihnen ungerechtfertigte Verzögerungen oder praktische Belastungen aufbürden.

- Auf spezifische Anforderung eines Betroffenen, und wenn keine anderen legitimen Interessen oder gesetzlich bindende Beschränkungen existieren, sollten Webmaster die relevante Information umgehend von ihrer Website entfernen. Zusätzlich sollten sie Anbietern von Suchmaschinen signalisieren, den betreffenden Teil der Website zu re-indexieren, um die Daten auch aus dem Suchindex und existierende Kopien im Cache von Suchmaschinen löschen zu lassen.

- Webmaster sollten ihren Nutzern spezifische Werkzeuge zur Verfügung stellen, die es ihnen erlauben, ihre Indexierungs-Präferenzen für die Suche individuell anzupassen[10]. Alternativ könnte auch die Nutzung des „noindex"-meta-tag erwogen werden, dass in dem HTML-Code der betreffenden Seite oder in dem HTTP-Header eingebunden wird oder der sitemap.xml-Datei, um die relevanten Suchpräferenzen im Zusammenhang mit bestimmten Objekten zu signalisieren[11].

- Besondere Sorgfalt sollte beim Schreiben der robots.txt-Datei im Bezug auf die lexikalische und semantische Korrektheit der Anweisungen wie auch ihrer inhärenten logischen Konsistenz gewidmet werden (um gegensätzliche und/oder überlappende Anweisungen zu vermeiden). Es sollte betont werden,

[10] Vgl. den von der „blogger.com"-Plattform zur Verfügung gestellten Mechanismus, der es Nutzern ermöglicht, ihre Indexierungs-Präferenzen in einem besonderen Formular anzulegen, das bei der Einrichtung des blog-services auszufüllen ist und den Webmaster anweist, wie er seine eigene robots.txt-Datei konfigurieren soll (http://buzz.blogger.com/2012/03/customize-your-search-preferences.html).

[11] Diese Empfehlung ist besonders relevant in dynamischen Umgebungen oder auf komplexen Webseiten, wo die robots.txt-Lösung nicht ausreichend mit der Größe der Webseite skalieren könnte. Ein Beispiel der Nutzung der robots.txt-Kommandos, um einer Suchmaschine das Verfallsdatum einer Seite zu signalisieren, ist verfügbar unter http://googleblog.blogspot.fr/2007/07/robots-exclusion-protocol-now-with-even.html. In gleicher Weise signalisiert die sitemap.xml-Datei, wie oft sich eine Webseite verändern kann, und die Priorität, die ein Webmaster einer URL beimisst, was der Suchmaschine erlaubt, die angemessene Auffrischungsgeschwindigkeit zu wählen. Vgl. auch http://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0224.html

dass ein Crawler in Ermangelung *spezifischer Ausschluss-Anweisungen* in der robots.txt-Datei annehmen wird, dass der Administrator die Indexierung der Website oder die Indexierung bestimmter Unterverzeichnisse gestattet (d. h. ein Crawler wird annehmen, dass der Inhalt der Website für Suchmaschinen verfügbar gemacht werden soll).

- Es sollte beachtet werden, dass das robots.txt-Protokoll nicht für die Regelung des Zugriffs auf besonders „riskante" Inhalte wie Verkehrsdaten elektronischer Kommunikationsdienste, Inhalte von SMS-Nachrichten, Speicher von Anrufbeantwortern, Aufenthaltsdaten, Finanzdaten etc. geeignet, noch dass es zur Verhinderung des Zugangs zu spezifischen administrativen Bereichen einer Website gedacht ist. Das robots.txt-Protokoll ist kein Ersatz für Verschlüsselung oder Zugriffskontrollmechanismen.

- Wenn ein Webmaster zu signalisieren beabsichtigt, dass bestimmte Seiten und/oder Dateien nicht von Suchmaschinen indexiert werden sollen, sollte besondere Sorgfalt auf die Auswahl der URLs verwendet werden. Tatsächlich könnte, da die robots.txt-Datei öffentlich sichtbar ist, das Vertrauen auf „selbsterklärende" URLs letztlich die Verfügbarkeit der betreffenden Inhalte erhöhen und damit die Vorteile des Protokolls zunichtemachen. Der Inhalt der robots.txt-Datei ist für Hacker besonders wertvoll, wie auch für jede andere Instanz, die versucht, personenbezogene Daten zu verbreiten oder zu beschaffen.

5. Empfehlungen für Suchmaschinen

Als eine ihrer Kernaktivitäten arbeiten Anbieter von Suchmaschinen überwiegend als Informationsvermittler/Intermediäre[12]. Allerdings gibt es auch bestimmte Arten der Verarbeitung, für die sie als eigenständige verantwortliche Stellen agieren.

Insbesondere führen einige Suchmaschinen viele verschiedene Aktivitäten durch, die von der Indexierung von Webseiten bis zur zeitweisen Speicherung des diesbezüglichen Inhalts reichen, um Nutzern das Auffinden der Informationen in Fällen zu ermöglichen, in denen ein Server und/oder Link abgeschaltet/nicht verfügbar ist. Dieses „Caching" stellt eine Wiederveröffentlichung dar, für die der Anbieter der Suchmaschine als verantwortliche Stelle betrachtet wird[13].

[12] Vgl. die Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148) der Artikel-29-Datenschutzgruppe der Europäischen Datenschutzbeauftragten (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf). Man beachte, dass diese Angelegenheit gegenwärtig vor dem Europäischen Gerichtshof verhandelt wird.

[13] Wie in der Stellungnahme zu Suchmaschinen von der Artikel-29-Datenschutzgruppe der europäischen Datenschutzbeauftragten (WP 148) betont wird, ist „… jegliche Zwischenspeicherung von auf indexierten Webseiten enthaltenen, personenbezogenen Daten über diesen aus Gründen der technischen Verfügbarkeit notwendigen Zeitraum hinaus (…) als eine unabhängige Neuveröffentlichung anzusehen. Nach Auffassung der [Artikel-29-] Arbeitsgruppe liegt die Verantwortung für die Einhaltung der Datenschutzgesetze hier beim Anbieter derartiger Caching-Funktionalitäten in seiner Rolle als Verantwortlicher für die Verarbeitung der personenbezogenen Daten, die in den zwischengespeicherten Veröffentlichungen enthalten sind."

Dementsprechend werden die folgenden Empfehlungen für Anbieter von Suchmaschinen unterschieden im Hinblick auf die unterschiedlichen Rollen, die sie spielen.

Bloße Indexierung

- Suchmaschinen sollten die von den Websites in Bezug auf die Inhalte, die sie enthalten ausgedrückten Präferenzen immer respektieren, sei es durch die robots.txt-Datei oder durch andere „noindex"-Markierungsmechanismen, einschließlich Anweisungen zu Verfallsdaten. Solche Indexierungs-Präferenzen können vor der ersten Durchsuchung der Website ausgedrückt werden, oder nachdem sie schon durchsucht worden ist. Im letzteren Fall sollten Aktualisierungen der von einer Suchmaschine durchgeführten Indexierung so schnell wie möglich durchgeführt werden.

- Suchmaschinen sollten die Effizienz ihrer Kommunikationskanäle mit Webmastern erweitern, um schnell über jegliche Veränderung der Indexierungs-Präferenzen in Kenntnis gesetzt zu werden, die von Webmastern durch die geeigneten Anweisungen des robots.txt-Protokolls ausgedrückt werden, oder von jeder Veränderung von Objekten innerhalb einer Website. Die Aktualisierungs/Berichtigungs-Prozeduren sollten so datenschutzfreundlich wie möglich sein – insbesondere sollten keine zusätzlichen personenbezogenen Daten von Nutzern verlangt werden, die verlangen, dass bestimmte personenbezogene Daten aktualisiert/berichtigt werden.

- Suchmaschinen sollten ihre Crawling-Häufigkeit den Suchpräferenzen der Webmaster anpassen. Sie sollten auch jegliche Anforderungen von Webmastern zur Re-Indexierung ihrer Webseiten oder von Teilen davon infolge der Löschung oder Berichtigung von personenbezogenen Daten unverzüglich ausführen.

- Da es bisher keine konsistente Interpretation der in einer robots.txt-Datei oder anderen Signalisierungsmechanismen für Indexierungspräferenzen (z. B. Metatags, sitemap.xml.-Dateien) enthaltenen Anweisungen durch Suchmaschinen gibt, ist schwer vorherzusagen, welchen Einfluss solche Mechanismen auf die Indexierung einer Website durch die verschiedenen Crawler haben wird. Es ist wünschenswert, dass sich Suchmaschinen in dieser Hinsicht auf einen „modus operandi" einigen. Die für die einzelnen Befehle anwendbaren Mechanismen sollten in klarer Weise auf einer Seite beschrieben werden, auf die von Nutzern leicht zugegriffen werden kann (z. B. von den Hauptseiten des Suchmaschinenportals).

- Suchmaschinen sollten in einem größeren Maße in die Unterstützung von Website-Administratoren eingebunden sein, indem sie Anleitungen und/oder

Werkzeuge für die automatisierte Analyse von Indexierungs-Präferenzen zur Verfügung stellen. Dies wird Administratoren ermöglichen, zu überprüfen, welche Effekte die von Ihnen gegebenen Befehle in Bezug auf die Indexierung haben werden.

- Suchmaschinen sollten die Terminierung und Kriterien des „crawling", das sie auf einer bestimmten Website durchführen, klarer spezifizieren, so dass Administratoren und Nutzer in vernünftiger Weise abschätzen können, wie lange eine bestimmte Information als Suchergebnis verfügbar bleibt.

Zeitweise Speicherung von durchsuchten Informationen

- Suchmaschinen sollten spezifische Crawler implementieren, wenn sie beabsichtigen, Daten nach verschiedenen Kategorien und für verschiedene Zwecke (z. B. generelle Indexierung, Nachrichten, Bilder, etc.) zu gruppieren, um Administratoren von Webseiten zu ermöglichen, den Kontext, in dem Informationen veröffentlicht werden, besser zu kontrollieren.

- Bei der Indexierung einer Website sollten Suchmaschinen komplexere und granularere Instruktionen für ihre Crawler zulassen, wie beispielsweise die folgenden:

  – Die Erlaubnis zur Indexierung von Informationen für bestimmte Zwecke (z. B. Allzweck-Suchmaschinen vs. Nachrichten-Suchmaschinen, etc.)[14];

  – die Erlaubnis, Informationen zeitweise für bestimmte Zwecke zu speichern, einschließlich diesbezüglicher Zeitbegrenzungen (z. B. caching, snippets);

  – die Erlaubnis, Informationen für bestimmte Zwecke an Dritte weiterzugeben;

  – die Erlaubnis, die abgefragten Informationen für bestimmte Anwendungsfälle[15] basierend auf dem Vorkommen von Eigenschaften, wie geografischer Lage oder IP-Adressräumen zu verarbeiten.

- Wo die Durchsuchung eine zeitweisen Speicherung von Inhalten einer Website für andere Zwecke zur Folge hat, als es Nutzern zu ermöglichen, auf diese

[14] Vgl. z. B. die von der italienischen Kartellbehörde verlauteten Feststellungen infolge einer Beschwerde der italienischen Vereinigung der Zeitungsverleger gegen Google. Danach verpflichtete sich Google öffentlich auf eine Reihe von Maßnahmen, um Verlage mit Werkzeugen auszustatten, die ihnen dabei helfen sollen, zwischen der Indexierung von Inhalten auf der allgemeinen Suchmaschine und der Indexierung auf der Nachrichten-Suchmaschine zu unterscheiden.

[15] Wegen der zunehmend komplexen Anwendungsfälle, die auf die von Suchmaschinen durchsuchten Informationen anwendbar sind, könnte es angemessen sein, das gegenwärtige Muster umzudrehen, nachdem Crawler eine Information lesen dürfen, wenn eine Anweisung formal inkorrekt ist oder von dem Crawler nicht interpretiert werden kann. Wenn es sich als unmöglich erweist, eine komplexe Menge von Anweisungen zu interpretieren, sollte dies automatisch als ein Verbot der Indexierung/Speicherung durch den Crawler interpretiert werden.

Inhalte im Falle zuzugreifen, dass der betreffende Server/das betreffende Netzwerk abgeschaltet/nicht verfügbar ist, sollten Suchmaschinen die Administratoren von Websites mit eindeutigen, spezifischen Informationen über den Zeitablauf versorgen und über technische Mechanismen, die für diese Speicherung gelten.

- Suchmaschinen sollten aufgrund spezifischer Anforderungen von Webmastern durch deren Such-Präferenzen jegliche Cache-Kopie der von Webseiten abgerufenen Daten unverzüglich löschen, und sollten von der weiteren Verarbeitung dieser Daten absehen, um das Risiko der Verbreitung der Daten und deren übermäßiger Exponierung zu begrenzen.

6. Ein abschließender Vorbehalt

In diesem Papier hat die Arbeitsgruppe Werkzeuge für die Kontrolle der Verfügbarkeit (personenbezogener) Daten im Web untersucht, die heute für Nutzer, Webmaster und Suchmaschinen verfügbar sind, zumeist gegründet auf die Begrenzung der Verfügbarkeit von Inhalten auf einer Website entweder durch Anwendung von (automatisierten) Löschmechanismen[16] oder durch die Implementierung von Protokollen zur Signalisierung von Suchpräferenzen. Es sollte daran erinnert werden, dass letztere immer noch auf einfachen ein/aus- (binären) Regeln für Crawler beruhen, die vor über 15 Jahren entworfen wurden. Im Gegenzug sind Suchmaschinen über die Jahre immer komplexer geworden und der ehe simple Inklusions-/Exklusionsmechanismus, der dem betreffenden Protokoll zugrunde liegt, ist nicht länger vollständig fähig, das fortwährend wachsenden Ausmaß der Gewinnung und Speicherung von Daten zu bewältigen. Es sollte z. B. herausgestellt werden, dass die Verfügbarkeit von Daten (einschließlich Daten, die Nutzer über sich selbst preisgeben), in Kombination mit Gesichtserkennungstechniken und Aufenthaltsinformationen, letztendlich eher die Indexierung von Individuen als nur von Inhalten oder Informationen ermöglichen kann. Ein vordringliches Augenmerk auf diese Aspekte ist deswegen notwendig.

Ein anderer, zukünftiger technologischer Durchbruch für den besseren Schutz personenbezogener Daten im Web könnte die Entwicklung des „policy-aware, semantic Web" sein, in dem Daten untrennbar mit Attributen (z. B. einer „Bedeutung") und Zugriffsregeln verknüpft werden könnten. Dies würde auf der einen Seite die Schaffung von neuen Beziehungen zwischen Daten ermöglichen und das Konzept einer vernetzten Welt erweitern, und auf der anderen Seite effektivere Mechanismen zur Erkennung und Auffindung von Inhalten ermöglichen, und potenziell auch von Kopien von Informationen, die mit diesem Objekt in

[16] Es ist hervorzuheben, dass aufgrund der öffentlichen Natur des Web andere Zugriffskontrollmechanismen wie die Authentifizierung von Nutzern und/oder Verschlüsselung von Daten implementiert werden sollten, wenn der Administrator einer Website Inhalte aus der „Öffentlichkeit" entfernen möchte.

Beziehung stehen, gestützt auf den Abgleich von Attributen (anstatt auf einfache Textvergleiche, wie dies heute stattfindet). Dies macht es vorstellbar, Informationen von einer Vielzahl von Websites zu entfernen und Suchergebnisse von Websites zu entkoppeln, und damit jegliche unbeabsichtigte Verbreitung von Daten zu vermeiden[17].

Natürlich sollte die Benutzbarkeit des Web nicht unterminiert werden und es muss eine Balance zwischen Innovation und den Grundrechten des Individuums auf Datenschutz und Schutz der Privatsphäre gefunden werden. Die Möglichkeit der Einführung granularerer Mechanismen, die nicht auf der einfachen Exklusions-/Inklusionsregel basieren, sollte weiter bedacht werden, aber eher darauf gerichtet sein, Betroffene in die Lage zu versetzen, ihre eigenen Suchpräferenzen besser auszudrücken und die Information mit dem angemessenen Kontext zu verbinden (z. B., indem es Betroffenen ermöglicht wird, zu signalisieren, ob eine bestimmte Information noch aktuell oder relevant ist, oder das Vorkommen jeglicher Ereignisse, die Auswirkungen auf diese Informationen gehabt haben könnten). Dies würde den Betroffenen mehr Möglichkeiten eröffnen als die einfache Wahl zwischen pauschaler, überschießender Verfügbarkeit im Web oder einem kompletten Verzicht auf neue Technologien.

Es gibt bedeutende und wachsende ökonomische Interessen sowohl bei Suchmaschinen als auch bei Administratoren von Websites, die auf die größtmögliche Verfügbarkeit von Daten durch die Implementierung der Indexierung von Daten und Informationen dringen. Diese Indexierung von Websites dient den ökonomischen Interessen bestimmter Marktteilnehmer und die Entfernung öffentlich zugänglicher Webinhalte oder die Signalisierung, dass solche Inhalte nicht durch eine Suchmaschine indexiert und abgerufen werden sollten, wird zwangsläufig Auswirkungen auf Geschäftsmodelle und die Marktdynamik haben. Eine Zusammenarbeit der verschiedenen Interessenvertreter ist notwendig, um die diesbezüglichen Interessen mit der Notwendigkeit des Schutzes der Privatsphäre angemessen in Einklang zu bringen.

[17] Google hat kürzlich eine Aktualisierung seines Suchalgorithmus angekündigt, die die Platzierung von Sites mit einer großen Anzahl von Mitteilungen über Löschungen herunterstufen wird und die nur in Fällen der Verletzung von Urheberrechten angewandt werden soll (http://insidesearch.blogspot.fr/2012/08/an-update-to-our-search-algorithms.html oder http://www.google.com/insidesearch/howsearchworks/).

2. 54. Sitzung am 2./3. September 2013 in Berlin

Arbeitspapier zum Recht auf vertrauliche Telekommunikation

– Übersetzung –

Angesichts der jüngsten Berichte über die Aktivitäten von Nachrichtendiensten erinnert die Arbeitsgruppe daran, dass sie bei verschiedenen Gelegenheiten die Bedeutung des Telekommunikationsgeheimnisses als Menschenrecht hervorgehoben hat[1]. Telekommunikation findet heutzutage meist grenzüberschreitend statt, so dass die Unterscheidung zwischen nationaler und internationaler Telekommunikation überholt ist. Telekommunikation und insbesondere das Internet sind lebensnotwendige Technologien für Einzelne und Gesellschaften im 21. Jahrhundert. Beide hängen von der berechtigten Erwartung der Nutzer ab, dass die Kommunikation *im Grundsatz* frei von Überwachungs- und Abhörmaßnahmen bleibt. Dies betrifft sowohl Inhalts- als auch Verbindungs- oder Nutzungsdaten und andere digitale Spuren. Wenn diese Vertraulichkeit als Grundregel bedroht ist, dann ist die Grundstruktur freier Gesellschaften in Gefahr. Die Kommunikationsüberwachung durch staatliche Behörden im Allgemeinen[2] und Nachrichtendienste im Besonderen, kann für legitime Zwecke notwendig sein, sie muss aber die *Ausnahme* bleiben und darf nicht zur Regel werden. Um den Grundsätzen der Offenheit, Transparenz und Rechenschaftspflicht zu genügen, sollten Vorkehrungen getroffen werden, um der Öffentlichkeit die Sicherheit zurückzugeben, dass Abhörbefugnisse rechtsmäßig, angemessen und verhältnismäßig genutzt werden.

Die Arbeitsgruppe fordert die Regierungen deshalb dazu auf:

1. das Telekommunikationsgeheimnis als wesentlichen Teil des weltweit garantierten Menschenrechts auf Schutz der Privatsphäre anzuerkennen[3];

---

[1] Gemeinsame Erklärung zur Kryptografie (12.9.1979) – http://www.datenschutz-berlin.de/attachements/172/crypt_de.pdf; gemeinsamer Standpunkt im Hinblick auf das Abhören privater Kommunikation, 23. Sitzung, 15.4.1998, Hongkong – http://www.datenschutz-berlin.de/attachements/904/inter_de.pdf; gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilateraler Abkommen zum Datenschutz („10 Gebote zum Schutz der Privatheit im Internet"), 28. Sitzung, 14.9.2000 Berlin – http://www.datenschutz-berlin.de/attachements/216/tc_de.pdf; Arbeitspapier zur Überwachung der Telekommunikation, 21. Sitzung, 27.3.2002 Auckland – http://www.datenschutz-berlin.de/attachements/912/wptel_de.pdf; die Charta von Granada zum Datenschutz in einer digitalen Welt, 27. Sitzung, 15.–16.4.2010, Granada – http://www.datenschutz-berlin.de/attachements/793/kopie_von675.41.21.pdf?1307526860. Der Europäische Gerichtshof für Menschenrechte hat in seiner Rechtsprechung Art. 8 der Europäischen Menschenrechtskonvention entsprechend interpretiert, vgl. Fall Weber und Seravia ./. Deutschland, Entscheidung vom 29. Juni 2006, mit weiteren Nachweisen.

[2] Zur unterschiedlichen Rechtslage weltweit vgl. International Data and Privacy Law, Vol. 2 No. 4 (2012), Special Issue on Systematic Government Access to Private Sector Data.

[3] Das Recht auf Vertraulichkeit der privaten Korrespondenz ist besonders erwähnt in Art. 12 der UN-Menschenrechtserklärung, Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte und Art. 8 der Europäischen Menschenrechtskonventionen.

2. das Telekommunikationsgeheimnis als Menschenrecht in einem völkerrechtlichen Vertrag zu stärken. Einschränkungen sollten auf das begrenzt werden, was in einer demokratischen Gesellschaft unbedingt notwendig ist;

3. sich auf internationale Regeln zu verständigen, mit denen der Zugriff staatlicher Stellen auf Daten bei Internetanbietern und der Einsatz von nachrichtendienstlichen Mitteln im Internet begrenzt wird;

4. für größere Transparenz und öffentliche Rechenschaftspflicht von Regierungsstellen bezüglich der Ergebnisse rechtmäßiger Überwachungsmaßnahmen zu sorgen[4]; dies schließt transparente Regeln zur Klassifizierung und Deklassifizierung ein[5];

5. sicherzustellen, dass jeder betroffene Mensch unabhängig von seiner Nationalität das Recht auf nachträgliche Benachrichtigung, auf Löschung oder Korrektur seiner Daten und auf Zugang zu den Gerichten hat;

6. den Bürgerinnen und Bürgern zu gestatten, dass sie frei Werkzeuge zur sicheren Kommunikation erforschen, schaffen, verteilen und nutzen, und sie dazu zu ermutigen; kein Bürger und keine Bürgerin sollte allein deshalb überwacht werden, weil er oder sie solche Werkzeuge nutzt;

7. eine effektive und unabhängige Kontrolle von Überwachungstätigkeiten sicherzustellen, die von der Polizei, Nachrichtendiensten oder in ihrem Auftrag von privaten Datenverarbeitern[6] durchgeführt werden.

---

[4] Der Europäische Gerichtshof für Menschenrechte hat im Fall Youth Initiative for Human Rights ./. Serbien, Urteil vom 25. Juni 2013, klargestellt, dass Nachrichtdienste der Informationsfreiheitsgesetzgebung unterliegen.

[5] Vgl. die Grundsätze 11–17 der weltweiten Prinzipien zur nationalen Sicherheit und zum Informationsrecht von Tshwane vom 12. Juni 2013.

[6] Vgl. Grundsatz 6 der weltweiten Prinzipien von Tshwane.

Arbeitspapier zum Datenschutz bei Überwachung aus der Luft

– Übersetzung –

Hintergrund

Überwachung ist das Beobachten von Verhalten, Aktivitäten oder anderen sich verändernden Informationen, um etwas oder jemanden zu beeinflussen, zu verwalten, zu steuern oder zu schützen. Sie beinhaltet häufig die Beobachtung von Individuen oder Gruppen durch Regierungsstellen, obwohl es einige Ausnahmen gibt, wie z. B. die Überwachung der Verbreitung von Krankheiten, bei der die Verbreitung einer Erkrankung in einer Gemeinschaft beobachtet wird, ohne Individuen direkt zu beobachten oder zu kontrollieren.

Überwachung aus der Luft ist das Erheben von Informationen, normalerweise von Bildern oder Videoaufnahmen, von einem Luftfahrzeug aus. Seit die Internationale Konferenz der Datenschutzbeauftragten zum ersten Mal über Luftüberwachung durch Satelliten diskutierte[1], hat es weitreichende technologische Entwicklungen gegeben. Während Satelliten-basierte Dienste wie Google Earth gegenwärtig keine besonderen Risiken für die Privatsphäre des Einzelnen bilden, solange nur Einzelbilder mit begrenzter Auflösung gesammelt werden, verhält es sich mit tief fliegenden Überwachungsplattformen wie Drohen anders. Während die Nutzung von Drohnen für militärische (Gefechts-) Zwecke Gegenstand einer – aufgrund von Geheimhaltung – begrenzten öffentlichen Debatte ist, wurde eine vergleichbare Diskussion über die zivile Nutzung dieser Technologie zum Zwecke der Sammlung von Informationen und deren Konsequenzen bisher vernachlässigt. Die Geschichte der Satellitentechnologie seit 1989 zeigt jedoch, dass Aufklärungstechnologien, die früher auf eine militärische Nutzung beschränkt waren, auch für die zivile Nutzung verfügbar werden können.

Überwachungsplattformen können für eine Vielzahl von Zwecken genutzt werden, einschließlich:

a) Fernerkundung: Die Nutzung verschiedener Sensoren (visueller, Infrarot- oder Nahinfrarot-Spektrum, Gamma-Strahlen, biologischer und chemischer), um die Gegenwart von Chemikalien, Mikroorganismen und anderen biologischen Faktoren, radioaktive Materialien, Waffen usw. zu erkennen;

[1] S. Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 29. Oktober 1992, Sydney, in: Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983 – 2006, S. 42; http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

b) Kommerzielle Luftüberwachung: Viehbeobachtungen, Flächenbrandkontrolle, Pipeline-Sicherheit, Gebäudesicherheit, Präzisionsackerbau, Verkehrswacht und Anti-Piraterie[2];

c) Erkundungen von Bodenschätzen: Durchführung geophysikalischer Untersuchungen zur Vorhersage der Lage von Öl-, Gas- und Mineralvorkommen, Überwachung von Öl- und Gaspipelines und vergleichbarer Infrastruktur, Vergleich der tatsächlichen Größe von Ackergrundstücken, für die Subventionen gezahlt wurden, mit Angaben in den dazugehörigen Antragsformularen[3];

d) Wissenschaftliche Forschung: Wetterbeobachtung einschließlich der Nahbeobachtung gefährlicher Wettersysteme wie Wirbelstürmen oder Nutzung in schwierigen Klimabedingungen wie in der Antarktis;

e) Suche und Rettung: Suche nach vermissten Personen, Schadensabschätzung nach Natur- (oder durch Menschen verursachte) Katastrophen; und

f) Naturschutz: Beobachtung der Bewegung von Tieren, Erkennung und Überwachung der Verbreitung von Unfällen mit Gefahrenstoffen, Waldbranderkennung, Fischereischutz, etc.

Überwachungsplattformen

Eine Vielzahl von Plattformen[4] oder Fahrzeugen wird zur Luftüberwachung verwendet oder kann dazu verwendet werden, einschließlich:

a) Starrflügler: ein Starrflügelflugzeug ist ein Flugzeug, das mithilfe von Flügeln fliegt, die Auftrieb erzeugen, der durch die Vorwärtsbewegung des Fahrzeugs und die Form der Flügel ermöglicht wird. Die Flügel eines Starrflügelflugzeugs sind nicht notwendigerweise steif; Drachen, Hängegleiter und Flugzeuge, die „wing-warping" oder variable Geometrie benutzen, werden alle als Starrflügelflugzeuge angesehen;
b) Drehflügler: Der Begriff Drehflügel beschreibt eine Tragfläche, die um eine annähernd vertikale Achse rotiert, wie die eines Helikopters oder Tragschraubers beim Fliegen;

[2] Die US-Unternehmen Skybox Imaging und Planet Labs planen die Nutzung von Flotten leichter Mikrosatelliten zur Erdüberwachung in Echtzeit. Sie ermöglichen privaten Investoren den Kauf und das Herunterladen von Bildmaterial, vgl. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyes-they-have.html?_r=0 (abgerufen am 20. Oktober 2013).

[3] Vgl. das europäische „Integrated Administration and Control System (IACS) http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm , das auf die Verhinderung von Betrug bei Landwirtschaftssubventionen gerichtet ist. IACS beinhaltet Satellitenüberwachung.

[4] Eine andere Kategorisierung findet sich auf Seite 2 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report datiert Dezember 2011 (online verfügbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

c) Unbemannte Flugsysteme (Unmanned Aircraft Systems – UAS). Ein unbemanntes Fluggerät (Unmanned Aircraft – UA), landläufig als Drohne bezeichnet, ist ein Fluggerät ohne einen menschlichen Piloten an Bord. Sein Flug wird entweder autonom von Computern innerhalb des Fahrzeugs kontrolliert oder über Fernbedienung durch einen Piloten am Boden oder in einem anderen Fahrzeug. UAS können Starr- oder Drehflügler sein und einzeln oder in Schwärmen (die untereinander und mit der zentralen Kontrollinstanz am Boden kommunizieren) betrieben werden, oder

d) Sonstige: Ein Aerostat ist ein Fahrzeug, das primär durch die Nutzung von dem Auftrieb von Gasen in der Luft bleibt, die leichter sind als Luft, und die einem Fahrzeug mit fast derselben Dichte wie Luft Auftrieb gewähren. Aerostaten beinhalten Frei- und/oder Fessel-Ballons, Zeppeline oder andere steuerbare Luftschiffe, die angetrieben oder antriebslos sein können.

Jede dieser Plattformen hat verschiedene Betriebseigenschaften wie Betriebshöhe, Geschwindigkeit, Reichweite, Höchstflugdauer (d. h. wie lange kann die Plattform in der Luft bleiben), die Fähigkeit zu schweben, und Nutzlast-Kapazität.

Überwachungstechnologien

Verschiedene Überwachungstechnologien können von den o. g. Plattformen getragen werden; die genaue Traglast hängt von einer Reihe von Faktoren wie Aufgabe, Wetterbedingungen, Nutzlast-Kapazität, die Reichweite des Sensors, sein Sichtfeld und seine Auflösung, usw. Sensoren umfassen (sind aber nicht notwendigerweise beschränkt auf):

a) Sichtbares Spektrum: Diese Sensoren haben typischerweise die Form von Kameras, einschließlich hochauflösenden und full-motion-Videosystemen[5]; sie erlauben fortlaufende Überwachung in Echtzeit und die Speicherung des gesamten Videomaterials;

b) Infrarot (IR): Diese Art von Sensoren erkennt Energie, die vom Ziel ausgesendet oder reflektiert wird. Die meisten IR-Sensoren sind passiv, obwohl sie in Verbindung mit einer IR-Beleuchtungsquelle benutzt werden können. Sie können durch Rauch, Nebel, Dunst und andere atmosphärische Verschleierungen besser „sehen“ als Kameras für sichtbares Licht;

[5] Die U.S. Army erwarb kürzlich eine 1.8 Gigapixel-Kamera zur Nutzung in ihren Drohnen. Diese Kamera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System – ARGUS IS) bietet 900 mal so viele Pixel wie eine 2-Megapixel-Kamera eines Mobiltelefons; sie wurde zu niedrigen Kosten unter Nutzung von 368 Kamera-Mikrochips aus Mobiltelefonen gebaut. Sie kann Objekte am Boden in 65 Meilen Entfernung aus einer Höhe von 20.000 Fuß verfolgen. Vgl. *US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (29. Dezember 2011), http://www.bbc.com/news/technology-16358851. Ein aufschlussreiches Video ist verfügbar unter: http://www.youtube.com/watch?v=QGxNyaXfJsA, abgerufen am 2. April 2013.

c) Nachtsicht: Die Fähigkeit bei schlechten Lichtbedingungen zu sehen, gestützt auf eine Kombination von ausreichendem Spektralbereich (d. h. wieviel vom elektromagnetischen (EM) Spektrum das Gerät erkennen kann) und ausreichendem Helligkeitsbereich (d. h. wieviel Licht ist notwendig, um ein brauchbares Bild zu erzeugen). Nachtsichttechnologien können grob in drei Hauptkategorien eingeteilt werden:

   1. Bildverstärkung: Diese Technologien arbeiten nach dem Prinzip der Vergrößerung der Menge empfangener Photonen aus verschiedenen natürlichen Quellen sowie Sternenlicht oder Mondlicht. Beispiele für solche Technologien umfassen Nachtgläser und Restlicht-Kameras;

   2. Aktive Ausleuchtung: Diese Technologien funktionieren nach dem Prinzip der Kopplung von Bildverstärkungstechnologien mit einer aktiven Lichtquelle im Nahinfrarot (NIR) oder Kurzwellen-Infrarot (shortwave infrared – SWIR)-Band. Ein Beispiel solcher Technologien sind Restlicht-Kameras; und

   3. Wärmebild-Aufklärung: Diese Technologien funktionieren durch Erkennung der Temperatur-Differenz zwischen den Hintergrund- und den Vordergrund-Objekten.

d) Radar: Radar nutzt Funkwellen des Hochfrequenz-Spektrums, um die Entfernung, Höhe, Richtung oder Geschwindigkeit eines Objekts zu bestimmen. Radar kann auch dazu genutzt werden, Objekte am Boden wie z. B. Fahrzeuge zu identifizieren und zu verfolgen (beispielsweise unter Nutzung von luftgestütztem Schrägsichtradar (Side Looking Airborne Radar – SLAR)); und

e) Spezialsensoren: Eine Reihe von Spezialsensoren (z. B. zur Erkennung von Spuren chemischer, biologischer, nuklearer, radiologischer und explosiver Materialien; Nummernschild-Scanner; akustische Sensoren, etc.) können ebenfalls von luftgestützten Überwachungsplattformen getragen werden.

Kombinationen dieser Sensortypen können Organisationen die Möglichkeit zur Durchführung von Luftüberwachung unter beinahe jeglichen Bedingungen bieten.

Auswirkungen auf die Privatsphäre

Es gibt eine Reihe von Aspekten der Überwachung, die Datenschutzbedenken hervorruft, einschließlich der Tatsache, dass Überwachung unsichtbar, intrusiv, willkürlich und kontinuierlich ist.[6] Obwohl diese Aspekte im Zusammenhang

[6] Freiwald, Susan: „A First Principles Approach to Communications Privacy“, veröffentlicht in Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), datiert 2007. Abrufbar unter http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf .

mit elektronischer Kommunikation beschrieben wurden, sind sie auch auf die Luftüberwachung anwendbar:

a) Unsichtbar: Abhängig von der Größe, der Einsatzhöhe, der Fähigkeiten der Sensoren usw., kann es unmöglich sein, Luftüberwachung (entweder die Plattform selbst oder die genutzten Sensoren) zu entdecken. Die von der Überwachung Betroffenen müssten auf deren Aufdeckung durch die Organisation selbst bauen, die die Überwachung durchführt oder auf die Aufdeckung durch einen Dritten. Die von unsichtbarer Überwachung Betroffenen haben weniger Möglichkeiten, die Organisation zur Verantwortung zu ziehen, die die Überwachung durchführt;

b) Intrusiv: Der Bandbreite möglicher Operationsbedingungen für Plattformen zur Luftüberwachung und die Fähigkeiten ihrer Sensoren verstärken die Intrusivität von Luftüberwachung (sie können fast alles und jedes „sehen“);

c) Willkürlich: Luftüberwachung deckt im allgemeinen ein Gebiet ab, das Individuen und Aktivitäten einschließt, die eine Überwachung nicht erfordern, was in der überschießenden Sammlung von Informationen resultiert; und

d) Kontinuierlich: Aufkommende Plattformen zur Luftüberwachung kombinieren zunehmende Betriebsdauer und die Fähigkeit, auf ein Gebiet zu „starren“, um eine wirksame, fortdauernde Überwachung eines beliebigen Gebiets zu erzeugen[7].

Diese Charakteristiken geben Anlass zu einigen spezifische Befürchtungen hinsichtlich des Schutzes der Privatsphäre[8]:

a) Schleichende Ausweitung des Einsatzes („Mission Creep“): Obwohl die meisten Menschen die Nutzung von Luftüberwachung (z. B. für die Entdeckung und Überwachung von Naturkatastrophen) oder zur Nutzung unter spezifischen, begrenzten Umständen bei der Strafverfolgung wahrscheinlich unterstützen würden, scheint es unvermeidlich, dass zukünftig weitere Privatsphäre-invasive Nutzungen für solche Technologien gefunden werden;

[7] Die U.S. Air Force hat die Gorgonenblick- („Gorgon Stare“) Technologie entwickelt, eine kugelförmige Anordnung von neun Kameras, die in eine Drohne eingebaut und fähig ist, Bewegtbilder ganzer Städte aufzunehmen („With Air Force's Gorgon Drone 'we can see everything'“, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html)

[8] Eine Erörterung der verschiedenen potentiellen Datenschutzbedenken findet sich auf Seite 11 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft“, ACLU Report datiert Dezember 2011 (abrufbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

b) Verfolgung: Die Fähigkeit, die Überwachung einer erweiterten Fläche über erweiterte Zeiträume aufrechtzuerhalten, birgt die Möglichkeit, dass Individuen und Fahrzeuge fortlaufend verfolgt werden können;

c) Proliferation, weil die Kosten für UAS-Technologien rapide fallen. UAS können von Privatpersonen zur Nutzung als „persönliche" oder „Do it yourself"-UAS gekauft oder gebaut werden.

Intrusiver für die Privatsphäre als Videoüberwachung

Die Auswirkungen von Videoüberwachung auf die Privatsphäre sind seit Jahren Gegenstand von Debatten gewesen, und viele Datenschutzbehörden haben Richtlinien zu den notwendigen Sicherungsmaßnahmen bei deren Nutzung herausgegeben. Wie oben erläutert verfügen Luftüberwachungssysteme aus verschiedenen Gründen über ein größeres Potenzial zur Verletzung der Privatsphäre als Videoüberwachungssysteme, einschließlich:

- Luftüberwachungssysteme können viel mehr verschiedene Sensoren nutzen als Videoüberwachungssysteme.
- Die Installation von Videoüberwachung erfordert normalerweise den Zugang zu und die Kontrolle über die entsprechenden Grundstücke; diese ist für Luftüberwachungssysteme nicht erforderlich, insbesondere für Orte im Freien.
- Abhängig von der Flughöhe und anderen Faktoren (z. B. Miniaturisierung) können Luftüberwachungssysteme von den überwachten Personen schwieriger – wenn nicht unmöglich – zu entdecken sein als die meisten Videoüberwachungssysteme.
- Luftüberwachungssysteme können ohne jegliche Verzögerung angewandt werden; sie benötigen keine Installation oder Konfigurationen vor Ort.

Dies deutet in klarer Weise darauf hin, dass die Sicherungsmaßnahmen für Videoüberwachungseinrichtungen, obwohl sie einen Minimalstandard anzeigen, im Zusammenhang mit Luftüberwachungssystemen nicht als ausreichend angesehen werden können und durch spezifische, den verschiedenen Luftüberwachungssystemen und Nutzungsszenarien angemessene Maßnahmen angepasst und ergänzt werden müssen.

Daher sollten bestimmte neue, essentielle Sicherungsmaßnahmen auf nationaler Ebene von den Gesetzgebern unter Berücksichtigung möglicher Unterschiede zwischen dem öffentlichen und dem privaten Sektor verabschiedet werden. Darüber hinaus werden internationale Vereinbarungen notwendig sein, um die Herausbildung eines „globalen Panoptikums" zu verhindern, da Luftüberwachung nicht an Landesgrenzen Halt macht.

Empfehlungen

Die zunehmende Nutzung von Luftüberwachung wird wahrscheinlich Bedenken darüber verstärken, wie die individuelle und kollektive Privatsphäre im täglichen Leben geschützt werden kann, egal ob sie von Strafverfolgungsbehörden oder anderen Einrichtungen der öffentlichen Verwaltung, oder von Privatunternehmen, oder von Bürgern zu Freizeitzwecken betrieben wird. Wenn Luftüberwachung ein zunehmend normaler Bestandteil der heutigen Gesellschaft wird, und die Gesellschaft deren Gegenwart als normal akzeptiert, ist es vorstellbar, dass die Erwartungen der Gesellschaft an den Schutz der Privatsphäre in der Öffentlichkeit ernstlich untergraben werden könnten. Es ist wichtig, eine angemessene Balance zwischen den Bedürfnissen der Strafverfolgung, der öffentlichen Sicherheit etc. auf der einen Seite und den legitimen Interessen der Individuen am Schutz der Privatsphäre auf der anderen Seite sicherzustellen. In diesem Sinne gibt die Arbeitsgruppe die folgenden Empfehlungen:

a) Die Nutzung von Luftüberwachung sollte auf spezifische Zwecke[9] beschränkt werden (z. B. die Suche nach vermissten Personen, die Überwachung von Grenzen, legitime private Zwecke, wie den Zugang zu Informationen durch Journalisten);

b) Die Nutzung personenbezogener Daten, wie beispielsweise Bildern, die durch Behörden aus der Luft gesammelt werden, sollten unter Richtervorbehalt stehen;

c) Die Öffentlichkeit sollte über die Nutzung von Luftüberwachung im größtmöglichen Ausmaß unterrichtet werden; dies erfordert z. B., dass jedes UAS mit der Fähigkeit, Informationen über eine Datenverbindung zu übertragen, seine GPS-Positionsdaten, Fähigkeiten und Angaben zum Eigentümer (z. B. die Behörde, das Unternehmen oder die Privatperson, die für die jeweilige Plattform oder das jeweilige Fahrzeug verantwortlich ist), in Echtzeit an eine geeignete Behörde übermittelt wird und dass diese Behörde die Aufenthaltsinformationen als „Open Data“ in Echtzeit verfügbar macht;

[9] Die American Civil Liberties Union (ACLU) beschreibt die folgenden Auflagen für die Nutzung von Drohnen:
a) **Nutzungsbeschränkungen:** Drohnen sollten von Strafverfolgungsbehörden nur unter Richtervorbehalt oder in Notfällen angewendet werden, oder wenn es spezifische und benennbare Gründe zu der Annahme gibt, dass die Drohne Beweismittel in Bezug auf eine bestimmte Straftat sammeln wird;
b) **Datenspeicherung:** Bilder sollten nur aufbewahrt werden, wenn der berechtigte Verdacht besteht, dass sie Beweismittel für ein Verbrechen enthalten oder für eine laufende Untersuchung oder ein laufendes Gerichtsverfahren relevant sind;
c) **Richtlinien:** Nutzungsrichtlinien für innerstaatliche Drohnen sollten durch die Repräsentanten der Öffentlichkeit festgelegt werden und nicht durch Polizeibehörden; die Richtlinien sollten klar, schriftlich und der Öffentlichkeit zugänglich sein; und
d) **Missbrauchsverhinderung & Verantwortlichkeit:** Die Nutzung innerstaatlicher Drohnen sollte Gegenstand offener Überprüfungen und angemessener Aufsicht zur Verhinderung von Missbrauch sein.
Siehe http://www.aclu.org/blog/tag/domestic-drones; siehe auch die bei EPIC aufgeführten Quellen unter http://www.epic.org/privacy/drones , in der verschiedene Gesetzentwürfe erwähnt werden, die diese Themen betreffen und gegenwärtig im U.S.-Kongress behandelt werden.

d) Die Überwachung sollte auf eine Fläche beschränkt werden, die so klein wie möglich ist (durch Begrenzung der Sichtfelder des Sensors), um die Wahrscheinlichkeit für eine „überschießende Erhebung“ zu minimieren;

e) Es sollten stringente Kontrollen darüber eingeführt werden, wie Luftüberwachungsinformationen genutzt werden können und wer auf diese Informationen Zugriff hat. Für Notfälle (z. B. die Suche nach vermissten Personen) können Ausnahmen gemacht werden; und

f) Es sollte immer eine menschliche Kontrollinstanz eingebunden sein, so dass, falls es Probleme oder ungewöhnliche Umstände gibt (z. B., dass das UAS in ein Wohngebiet abdriftet), diese so schnell wie möglich angegangen werden können.

Die Arbeitsgruppe wird die Entwicklungen in diesem Bereich im Lichte der sich rasant entwickelnden Technologie weiterhin genau beobachten.

B. Dokumente zur Informationsfreiheit

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließungen der 26. Konferenz am 27. Juni 2013 in Erfurt

Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!

Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen weit über das bisherige Recht der Bürgerinnen und Bürger, einen Antrag auf Informationszugang zu stellen, hinaus. Open Data – also die aktive Bereitstellung öffentlicher Informationen im Internet – wird auf den ersten Portalen bereits praktiziert. Zahlreiche Projekte befinden sich im Aufbau. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt diese Entwicklungen ausdrücklich und formuliert in einem Positionspapier wesentliche Anforderungen an eine moderne Transparenzgesetzgebung.

Die Konferenz hält Regelungen in den Informationsfreiheits- und Transparenzgesetzen für erforderlich. Diese müssen um geeignete Instrumente zur Veröffentlichung von Informationen ergänzt werden. Datenbestände öffentlicher Stellen dürfen grundsätzlich nicht durch Urheberrecht oder Nutzungsbeschränkungen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

Open Data muss als wesentlicher Bestandteil der Informationsfreiheit verstanden werden. Allerdings wird der Anspruch auf Informationszugang im herkömmlichen Antragsverfahren auch in Zukunft unverzichtbar sein. Eine Weiterentwicklung der bestehenden Informationsfreiheitsrechte um möglichst umfassende Veröffentlichungspflichten halten die Informationsfreiheitsbeauftragten für unerlässlich. Mit dem Positionspapier unterstützen sie die begonnenen Open-Data-Projekte und empfehlen den Gesetzgebern eine enge Verzahnung von Informationsfreiheit und Open Data.

Positionspapier

der 26. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 27. Juni 2013 in Erfurt:

Informationsfreiheit und Open Data

Informationsfreiheit und Open Data sind wesentliche Voraussetzungen für Transparenz und Kontrollierbarkeit der Verwaltung und fördern die demokratische Partizipation.

Die Informationsfreiheits- und Transparenzgesetze der Länder sowie des Bundes (im Folgenden: Informationsfreiheitsgesetze) erfahren große Akzeptanz und werden intensiv genutzt. Ihnen ist zumeist eines gemeinsam: Wer Informationen von öffentlichen Stellen begehrt, muss einen Antrag stellen, ein Verwaltungsverfahren durchlaufen und dafür unter Umständen auch Gebühren entrichten. Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen jedoch darüber hinaus. Dem in seiner Durchsetzung oft aufwändigen Antragsrecht der Bürgerinnen und Bürger sollte deshalb die Pflicht öffentlicher Stellen stärker als bisher zur Seite gestellt werden, Informationen von sich aus zu veröffentlichen. Open Data – also die aktive Bereitstellung öffentlicher Informationen im Internet – wird auf den ersten Portalen im Internet bereits praktiziert. Zahlreiche Projekte befinden sich im Aufbau.

Open Data beinhaltet begrifflich bereits die Forderung nach Offenheit. Daten des öffentlichen Sektors sind in diesem Sinne offen, wenn sie maschinenlesbar sind (maschinell interpretiert werden können), das Format der Datensätze offen und frei nutzbar ist (offene Standards), sie grundsätzlich keiner beschränkenden Lizenz unterliegen und ohne Kosten zugänglich sind sowie beliebig genutzt und weiterverwendet werden können. Damit dies zum Standard für den Umgang mit Informationen öffentlicher Stellen in Deutschland werden kann, müssen neben informationstechnischen auch rechtliche Voraussetzungen geschaffen werden. Die Informationsfreiheitsbeauftragten halten zur Umsetzung von Open Data klare gesetzliche Grundlagen für erforderlich und empfehlen die Berücksichtigung der folgenden Eckpunkte:

1. Open Data braucht starke Informationsfreiheitsgesetze

a) Open Data muss als wesentlicher Bestandteil der Informationsfreiheit verstanden werden. Der Anspruch auf Informationszugang im herkömmlichen Antragsverfahren wird auch in Zukunft unverzichtbar sein.

b) Länder, in denen noch keine entsprechenden gesetzlichen Regelungen existieren, sollten unverzüglich Informationsfreiheitsgesetze mit einem starken

Anspruch auf Informationszugang und effektiver Verpflichtung zur proaktiven Veröffentlichung von Daten öffentlicher Stellen sowie zur Einrichtung von Informationsregistern bzw. Open-Data-Portalen beschließen.

c) Die Informationsfreiheitsgesetze sind, soweit erforderlich, so anzupassen, dass Informationen, die auf ihrer Grundlage herausgegeben werden, in der Regel auch veröffentlicht werden können. Die Pflichten zur Veröffentlichung sind in den Informationsfreiheitsgesetzen zu regeln und müssen für alle öffentlichen Stellen gelten, die bereits einem Zugangsanspruch nach den jeweiligen Informationsfreiheitsgesetzen unterliegen. Wenn Informationen auf dem Antragswege herauszugeben sind, sollte auch deren Veröffentlichung so wenig wie möglich beschränkt werden. Hierfür kann die Anonymisierung von Daten förderlich sein.

d) Die Gefahr der weiteren Rechtszersplitterung durch neue Open-Data-Regelungen außerhalb der Informationsfreiheitsgesetze bestätigt die Forderung der Informationsfreiheitsbeauftragten nach einer möglichst einheitlichen Rechtsgrundlage für den Informationszugang.

2. Klarere Regelungen zur Veröffentlichung als Voraussetzung für Open Data

a) Open Data ist weit mehr als Öffentlichkeitsarbeit: Bestehende Ansätze von Veröffentlichungspflichten in den Informationsfreiheitsgesetzen sind auszubauen und um effektive Instrumente zu ergänzen, die eine Veröffentlichung gewährleisten.

b) Kategorien von Dokumenten, die zu veröffentlichen sind, sollten in den Informationsfreiheitsgesetzen umfassend und konkret beschrieben werden. Die Informationsfreiheitsbeauftragten beraten bei der Konzeption und Umsetzung.

c) In den Informationsfreiheitsgesetzen sollte für alle Informationen, auf deren Zugang ein voraussetzungsloser Anspruch besteht, auf Verwendungsbeschränkungen verzichtet werden.

d) Der Ort der Veröffentlichung ist ausdrücklich zu regeln. Denkbar ist die Veröffentlichung in einem Informationsregister bzw. Open-Data-Portal. Auch kann die Einrichtung entsprechender Seiten auf den Homepages der informationspflichtigen Stellen sinnvoll sein.

e) Ein Informationsregister bzw. eine Open-Data-Plattform sollte ausschließlich in öffentlicher Regie errichtet werden. Durch die Verantwortlichkeit öffentlicher Betreiberinnen und Betreiber können nicht zuletzt die Richtigkeit und Aktualität der angebotenen Informationen am ehesten gewährleistet werden.

f) Die Ausgestaltung einer Open-Data-Plattform sollte sich bereits von der technischen Konstruktion bis hin zu den Voreinstellungen auf Funktionen beschränken, die für die Bereitstellung der Informationen für die Bürgerinnen und Bürger von Bedeutung sind, ihnen die Preisgabe nicht erforderlicher personenbezogener Daten aber nicht abverlangen (privacy by design).

3. Es bedarf eines subjektiven, durchsetzbaren Anspruchs auf Veröffentlichung

a) Ein wichtiges Instrument zur Durchsetzung von Open Data ist die Gewährleistung eines subjektiven Rechtsanspruches auf die aktive Veröffentlichung von Informationen in den Informationsfreiheitsgesetzen von Bund und Ländern. Zwar ist die Verwaltung an Recht und Gesetz gebunden, jedoch hätten Bürgerinnen und Bürger ohne einen derartigen Anspruch keine Möglichkeit, eine öffentliche Stelle, die vorhandene Daten entgegen der Veröffentlichungspflicht rechtswidrig zurückhält, zur Veröffentlichung zu verpflichten.

b) Dieser Anspruch sollte dem bisherigen Informationszugangsanspruch im Hinblick auf Einklagbarkeit und Unterstützung durch die Informationsfreiheitsbeauftragten gleichgestellt werden.

4. Keine Verwendungseinschränkung für öffentlich bereitgestellte Daten

a) Datenbestände öffentlicher Stellen dürfen nicht durch Urheber- oder Nutzungsbeschränkungen der öffentlichen Stellen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

b) Sowohl bei der Veröffentlichung als auch bei der Verwendung darf es nicht darauf ankommen, welche Absichten die Nutzerinnen und Nutzer verfolgen.

5. Open Data ist eine Investition in die Zukunft

a) Sowohl die Schaffung der Infrastruktur als auch die erstmalige Aufarbeitung und Bereitstellung der Daten können kostenintensiv sein. Auch die regelmäßige Veröffentlichung aktueller Informationen kann zusätzliche Sach- und Personalkosten binden. Es bedarf sowohl einer technischen Aufbereitung der Daten selbst (Maschinenlesbarkeit) als auch der Strukturierung einer nutzbaren, übersichtlichen Plattform.

b) Aus Praktikabilitätsgründen wird eine Beschränkung des Umfangs der tatsächlich zu veröffentlichenden Daten zunächst unumgänglich sein. Auch ein zeitlich gestaffeltes In-Kraft-Treten von Veröffentlichungspflichten kann dem Praktikabilitätsgedanken Rechnung tragen.

c) Angemessene Übergangsfristen sind auch für die Schaffung der technischen Voraussetzungen sowie für die etwaige Aufbereitung von Informationen, die vor dem In-Kraft-Treten einer entsprechenden Regelung angefallen sind, vertretbar.

d) Um die Bereitstellung von Informationen zu erleichtern, sollten Regelungen getroffen werden, damit neue Daten bereits von vornherein in den entsprechend verwertbaren Formaten geführt werden oder zumindest problemlos aufbereitet werden können.

e) Die Kosten der Verwaltung können durch Open Data langfristig reduziert werden. Insbesondere erspart die proaktive Bereitstellung von Informationen den öffentlichen Stellen die Bearbeitung individueller Informationszugangsanträge.

f) Durch innovative Geschäftsmodelle zur kommerziellen Weiterverwendung öffentlicher Daten kann Open Data zu positiven gesamtwirtschaftlichen Effekten beitragen.

g) Die Kostenerhebung für den antragsgebundenen Informationszugang steht in einem Spannungsverhältnis zur Kostenfreiheit im Rahmen von Open Data. Ein stimmiges Gesamtkonzept sollte durch einen grundsätzlichen Verzicht auf die Erhebung von Gebühren erreicht werden.

h) Open Data bedeutet einen Aufgabenzuwachs bei den Informationsfreiheitsbeauftragten. Auch nach der Begleitung im Anfangsstadium (Gesetzgebung, Projekte für Plattformen etc.) bedürfen die öffentlichen Stellen einer permanenten Beratung zur Umsetzung der Veröffentlichungspflichten. Außerdem müssen die Kapazitäten der Informationsfreiheitsbeauftragten erweitert werden.

Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!

Mit der Reform des Verbraucherinformationsrechts zum 1. September 2012 hat der Gesetzgeber als Reaktion auf die Lebensmittelskandale der letzten Jahre mit § 40 Abs. 1 a Lebensmittel- und Futtermittelgesetzbuch (LFGB) eine Rechts-

grundlage für die Veröffentlichung von Hygieneverstößen durch die zuständigen Behörden geschaffen. Schon im damaligen Gesetzgebungsverfahren hatte die Konferenz der Informationsfreiheitsbeauftragten darauf hingewiesen, dass die Vorschrift zu undifferenziert sei.

Nachdem zahlreiche Bundesländer begonnen hatten, Verbraucherinnen und Verbraucher auf eigens dafür geschaffenen Internetplattformen über entsprechende Hygieneverstöße zu informieren, sind die Veröffentlichungen durch eine Reihe von verwaltungsgerichtlichen Entscheidungen in Baden-Württemberg, Bayern, Berlin, Nordrhein-Westfalen und Rheinland-Pfalz gestoppt worden. Nach Auffassung der Gerichte greift § 40 Abs. 1 a LFGB unter anderem deshalb unverhältnismäßig in die Rechte der betroffenen Unternehmen ein, weil die Vorschrift schon bei geringen Verstößen eine Veröffentlichung zulasse und keine Grenzen für die Dauer der Veröffentlichung vorsehe.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, dringend die lebensmittelrechtlichen Vorschriften über die Information der Öffentlichkeit zu überarbeiten und wie vom Bundesrat angeregt im Fachdialog mit den Ländern ein Transparenzsystem zu schaffen, das in eine rechtskonforme und effektive Gesamtkonzeption eingebunden wird. Nach der Rechtsprechung sind als Kriterien für eine Neuregelung der Veröffentlichungspflicht im Sinne des § 40 Abs. 1a LFGB insbesondere die Schwere des Rechtsverstoßes, eine behördliche Hinweispflicht auf die Tatsache und den Zeitpunkt der Mängelbeseitigung, Löschungspflichten sowie Ermessens- und Härtefallregelungen in Erwägung zu ziehen.

Umfassende Transparenz bei der Lebensmittelsicherheit darf nicht als Belastung für die Betriebe verstanden werden. Vielmehr ist dies der einzige Weg, das Vertrauen von Verbraucherinnen und Verbrauchern in die Qualität der Lebensmittel langfristig herzustellen und zu wahren.

Transparenz bei Sicherheitsbehörden

Im Zusammenhang mit den Enthüllungen der umfassenden und anlasslosen Überwachungsmaßnahmen des US-amerikanischen und des britischen Geheimdienstes wurde bekannt, dass auch ein großer Teil des Kommunikationsverhaltens der Bürgerinnen und Bürger in Deutschland ohne ihr Wissen von diesen Geheimdiensten überwacht worden ist.

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Verantwortlichen in Deutschland und Europa auf, für Transparenz auf nationaler und internationaler Ebene zu sorgen. Das Vertrauen der Bevölkerung kann nur zurückgewonnen

werden, wenn die Aufgaben und Befugnisse der Sicherheitsbehörden völkerrechtlich festgelegt und deren tatsächliche Arbeitsweisen nachvollziehbar sind.

Zweifellos verfügen die Nachrichtendienste über Informationen, die nicht offengelegt werden dürfen. Gleichwohl hält die Konferenz die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheits- und Transparenzgesetze für nicht hinnehmbar und erwartet von den Gesetzgebern entsprechende Verbesserungen.

Darüber hinaus bedürfen die weit gefassten Ausnahmeregelungen für Sicherheitsbelange in den Informationsfreiheits- und Transparenzgesetzen einer Überprüfung und Einschränkung.

Die Informationsfreiheitsbeauftragten unterstützen die Verbesserung der Transparenz der nachrichtendienstlichen Aktivitäten gegenüber den Parlamenten und schließlich die Stärkung der parlamentarischen Kontrollgremien.

Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden – auch des Bundes

Das Bundesverwaltungsgericht hat mit Urteil vom 20. Februar 2013 entschieden, dass die Pressegesetze der Länder keine Verpflichtung von Bundesbehörden zur Auskunftserteilung an Journalistinnen und Journalisten begründen. Die Gesetzgebungskompetenz für den presserechtlichen Auskunftsanspruch gegenüber Bundesbehörden liege danach beim Bund. Eine entsprechende Auskunftsverpflichtung existiert bislang nicht. Das Bundesverwaltungsgericht sieht einen unmittelbar aus der Garantie der Pressefreiheit abgeleiteten „Minimalstandard von Auskunftspflichten“ und einen einklagbaren, ebenfalls unmittelbar aus Art. 5 Abs. 1 Satz 2 GG abgeleiteten Rechtsanspruch auf Auskunft, soweit dem nicht berechtigte schutzwürdige Vertraulichkeitsinteressen von Privatpersonen oder öffentlichen Stellen entgegenstehen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt die Entscheidung des Bundesverwaltungsgerichtes insofern, als damit der Auskunftsanspruch von Journalistinnen und Journalisten grundrechtlich abgeleitet und abgesichert wird.

Aus Sicht der Konferenz gilt es – unabhängig von der kontrovers diskutierten Regelungszuständigkeit – die notwendigen gesetzlichen Grundlagen für eine effektive journalistische Recherche herzustellen, die eine zeitnahe, aktuelle und profunde Berichterstattung ohne abschreckende Kostenhürden möglich machen. Das Urteil, das einen unscharfen, beliebig interpretierbaren Minimalstandard mit unklaren Grenzen und Beschränkungsmöglichkeiten zugesteht, darf hier jedenfalls nicht das letzte Wort sein! Bundesbehörden müssen denselben Auskunftspflichten unterliegen wie Landesbehörden.

2. Entschließung der 27. Konferenz am 28. November 2013 in Erfurt

Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!

Der freie Zugang der Bürgerinnen und Bürger der Bundesrepublik Deutschland zu den Informationen der öffentlichen Stellen muss auch in Deutschland ein fester Bestandteil der verfassungsrechtlich garantierten Rechte werden. Transparenz ist eine wesentliche Grundlage fur eine funktionierende freiheitlich demokratische Gesellschaft. Sie ist der Nährboden fur gegenseitiges Vertrauen zwischen staatlichen Stellen und den Bürgerinnen und Bürgern.

Es reicht nicht aus, dass Informationen nur auf konkreten Antrag hin herauszugeben sind. In Zukunft sollten öffentliche und private Stellen, die öffentliche Aufgaben wahrnehmen, verpflichtet sein, Informationen von sich aus zur Verfugung zu stellen. Auf diese Weise wird der Zugang zu Informationen für alle erleichtert und der Aufwand der Informationserteilung reduziert.

Die Bundesrepublik Deutschland muss jetzt die nötigen gesetzlichen Regelungen für ein modernes Transparenzrecht schaffen, um mit den internationalen Entwicklungen Schritt zu halten und die Chancen der Transparenz wahrzunehmen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder fordert daher alle Beteiligten in Bund und in den Landern auf, sich fur die Stärkung der Transparenz auf nationaler, europäischer und internationaler Ebene einzusetzen.

Sie fordert insbesondere:

- den Anspruch auf freien Zugang zu amtlichen Informationen endlich in alle Verfassungen aufzunehmen,

- einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im oöffentlichen und nicht-öffentlichen Bereich berichten,

- ein einheitliches Informationsrecht zu schaffen, das die Regelungen des Informationsfreiheitsgesetzes, des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes in einem Gesetz zusammenfasst,

- dass das Informationsfreiheitsrecht im Sinne eines Transparenzgesetzes mit umfassenden Veröffentlichungspflichten nach den Open-Data-Grundsätzen weiterentwickelt wird,

- aus der vom Bundestag in Auftrag gegebenen Evaluation des Bundesinformationsfreiheitsgesetzes die notwendigen Konsequenzen zu ziehen und die Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß zu beschränken,

- die Bereichsausnahme fur die Nachrichtendienste abzuschaffen, die entsprechende Ausnahmeregelung auf konkrete Sicherheitsbelange zu beschränken und den Umgang mit Verschluss-Sachen gesetzlich in der Weise zu regeln, dass die Klassifizierung von Unterlagen als geheimhaltungsbedürftig regelmäßig von einer unabhängigen Instanz überprüft, beschränkt und aufgehoben werden kann,

- Transparenz der Kooperationen auch zwischen privaten und wissenschaftlichen Einrichtungen sicherzustellen, die im Rahmen der Wahrnehmung öffentlicher Aufgaben fur staatliche Stellen tätig sind. Dies gilt auch und insbesondere fur Sicherheitsbehörden.

- die Berliner Erklärung der 8. Internationalen Konferenz der Informationsfreiheitsbeauftragten zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013, insbesondere die Anerkennung eines Menschenrechts auf Informationszugang im Rahmen der Vereinten Nationen, den Beitritt der Bundesrepublik zur Open Government Partnership und zur Tromsö-Konvention des Europarats (Konvention des Europarates über den Zugang zu amtlichen Dokumenten) umzusetzen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder bietet ihre Unterstützung an.

II. Internationale Konferenz der Informationsfreiheitsbeauftragten

8. Konferenz vom 18. – 20. September 2013 in Berlin

Berliner Erklärung zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013: „Transparenz – der Treibstoff der Demokratie“

In dem Bewusstsein, dass

- die Bereitschaft der Bürgerinnen und Bürger, ihre Grundrechte wahrzunehmen und sich aktiv in den politischen Prozess einzubringen, von entscheidender Bedeutung für die Demokratie ist,

- Information eine unverzichtbare Voraussetzung politischer Meinungsbildung, Teilhabe und Partizipation bildet,

- die Beachtung rechtsstaatlicher Vorgaben (Rule of law), die Transparenz staatlichen Handelns und eine starke richterliche Kontrolle staatliches Handeln legitimieren,

- Rechtsstaatlichkeit und Transparenz das Vertrauen in die Rechtstreue und Lernfähigkeit staatlicher, regionaler und kommunaler Funktionsträger und Organe stärken,

erklären die in Berlin zu ihrer 8. Internationalen Konferenz versammelten Informationsfreiheitsbeauftragten:

Transparenz ist ohne rechtlich verbürgten Informationszugang nicht möglich. Deshalb bedarf es verbindlicher rechtlicher Ansprüche auf Informationszugang auf der staatlichen und überstaatlichen Ebene.

Völkerrechtlich garantierte Informationsrechte begründen individuelle Ansprüche auf Informationszugang gegen supranationale Stellen und verpflichten die Staaten, ihr Wissen mit den Bürgerinnen und Bürgern zu teilen. Das Handeln der Staaten und der Staatengemeinschaften muss sich stärker als bisher auf Diskurs und Beteiligung gründen. Sie müssen sich mehr als bisher um das Vertrauen der Menschen bemühen, wollen sie ihre Ziele erreichen.

Demokratie, Rechtsstaatlichkeit und der Kampf gegen das Übel der Korruption können sich nur dort entwickeln, wo nationale Behörden und internationale Organisationen bereit sind, über ihr Handeln Rechenschaft abzulegen und ihre Informationen mit den Bürgerinnen und Bürgern zu teilen. Transparenz ist eine wichtige Waffe im Kampf gegen die weltweite Korruption. Diese kann nur in einem Klima der Heimlichkeit und der Abschottung von Entscheidungsprozessen gegenüber den Bürgerinnen und Bürgern gedeihen.

In vielen Staaten und internationalen Einrichtungen werden bereits heute eine Reihe von Informationen aus der Umwelt, der Tätigkeit von Parlamenten und aus vielen anderen Bereichen bekannt gemacht. Diese Form der Transparenz stärkt das Vertrauen der Bürger in deren Arbeit. Es gibt aber nach wie vor große Lücken, die endlich geschlossen werden müssen.

Dem Anspruch auf Transparenz können sich auch Geheimdienste nicht prinzipiell verweigern. Gerade weil ihre Tätigkeit tief in Grundrechtspositionen der Bürgerinnen und Bürger eingreift, ist auch hier eine öffentlich nachvollziehbare rechtsstaatliche Kontrolle erforderlich. Damit ist es nicht zu vereinbaren, diesen Bereich gänzlich vom Recht auf Zugang auf Informationen auszunehmen. Die Konferenz verweist insofern auf die Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 25. Juni 2013 (Youth Initiative for Human Rights v. Serbia), mit dem die Geltung der in der Europäischen Menschenrechtskonvention garantierten Informationsfreiheit auch für Geheimdienste prinzipiell anerkannt wird.

Transparenz ist auch dort geboten, wo Wirtschaftsunternehmen staatenübergreifend Einfluss auf politische und administrative Entscheidungen nehmen. Gerade hier sind völkerrechtlich verbindliche Garantien der Transparenz und eine verstärkte internationale öffentliche Kontrolle unverzichtbare Voraussetzungen, um wirtschaftliche Macht besser als bisher im Zaum zu halten. Transparenz ist zugleichauch ein wichtiges Instrument gegen die Korruption innerhalb von und durch Unternehmen.

Die Internationale Konferenz der Informationsfreiheitsbeauftragten

- spricht sich dafür aus, auf nationaler und supranationaler Ebene umfassende und wirksame rechtliche Verpflichtungen für den Informationszugang auf Antrag und für eine effektive aktive Bereitstellung von Informationen zu schaffen, die alle Möglichkeiten der Kommunikation, insbesondere diejenigen der Informationstechnologie, nutzt;

- unterstützt die Anerkennung eines internationalen Grundrechts auf freien Informationszugang und weist auf Artikel 19 des Internationalen Pakts über bürgerliche und politische Rechte (Zivilpakt, ICCPR) vom 16. Dezember 1966

hin, der als internationale Vereinbarung festlegt, dass alle Menschen ungehinderte Meinungsfreiheit genießen sollen, einschließlich der Freiheit, sich über Staatsgrenzen hinweg Informationen zu beschaffen, zu empfangen und weiterzugeben;

- bekräftigt ihre in Ottawa 2011 beschlossene Forderung, dass alle in Betracht kommenden Staaten der Open Government Partnership beitreten und sie aktiv unterstützen sollten;

- stellt fest, dass die Konvention des Europarats über den Zugang zu amtlichen Dokumenten vom 18. Juni 2009 (Tromsö-Konvention), welche das erste internationale Rechtsinstrument ist, in dem Regelungen für das Recht auf Informationszugang bei staatlichen Stellen völkerrechtlich detailliert getroffen werden, allen Staaten der Erde zum Beitritt offen steht, und empfiehlt, dass alle Staaten in Erwägung ziehen sollten, die Konvention zu ratifizieren.