Dokumente
zu Datenschutz
und Informationsfreiheit
2010

Impressum

Herausgeber:	**Berliner Beauftragter für Datenschutz und Informationsfreiheit** An der Urania 4 – 10, 10787 Berlin Telefon: 0 30/1 38 89-0 Telefax: 0 30/2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de

Druck: Offsetdruckerei Holga Wende

Stand: Januar 2011

Inhaltsverzeichnis

Seite

Vorwort 7

A. Dokumente zum Datenschutz 9

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 9

1. Entschließungen der 79. Konferenz am 17./18. März 2010 in Stuttgart 9

– Körperscanner – viele offene Fragen 9

– Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle! 10

– Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich 11

– Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung 12

– Keine Vorratsdatenspeicherung! 13

2. Entschließungen zwischen der 79. und 80. Konferenz 14

– Beschäftigtendatenschutz stärken statt abbauen (vom 22. Juni 2010) 14

– Erweiterung der Steuerdatenbank enthält große Risiken (vom 24. Juni 2010) 16

– Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz! (vom 11. Oktober 2010) 17

3. Entschließungen der 80. Konferenz am 3./4. November 2010 in Freiburg 18

– Keine Volltextsuche in Dateien der Sicherheitsbehörden 18

– Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs 19

– Förderung des Datenschutzes durch Bundesstiftung 21

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich 22

1. Beschluss der Sitzung am 28./29. April 2010 in Hannover (i. d. F. vom 23. August 2010) 22

– Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen 22

2. Beschlüsse der Sitzung am 24./25. November 2010 in Düsseldorf 23

– Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen 23

– Minderjährige in sozialen Netzwerken wirksamer schützen 24

– Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG) 25

– Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste 28

III. Europäische Konferenz der Datenschutzbeauftragten 30

Prag, 29./30. April 2010 30

– Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen 30

– Entschließung zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen 32

IV. Dokumente der Europäischen Union 34

1. Europäisches Parlament und Rat 34

– Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation in der Fassung der Richtlinie 2009/136/EG vom 25. November 2009 34

2. Europäische Kommission 70

– Beschluss 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG 70

3. Artikel 29-Datenschutzgruppe 92

– Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting (WP 171) 92

– Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (WP 176) 130

V. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation 138

47. Sitzung am 15./16. April 2010 in Granada 138

– Die „Granada Charta" des Datenschutzes in einer digitalen Welt 138

– Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft (Revision des Arbeitspapiers der 46. Sitzung vom 7./8. September 2009 in Berlin) 142

48. Sitzung am 6./7. September 2010 in Berlin 147

– Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken 147

– Arbeitspapier „Mobile Verarbeitung personenbezogener Daten und Datensicherheit“ 149

B. Dokumente zur Informationsfreiheit 155

Konferenz der Informationsfreiheitsbeauftragten in Deutschland 155

1. Entschließung der 20. Konferenz am 24. Juni 2010 in Berlin 155

– Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten 155

2. Stellungnahme der Konferenz der Informationsfreiheitsbeauftragten zur Evaluation des Verbraucherinformationsgesetzes (VIG) vom 2. September 2010 156

3. Entschließungen der 21. Konferenz am 13. Dezember 2010 in Kleinmachnow 169

– Open Data: Mehr statt weniger Transparenz! 169

– Verträge zwischen Staat und Unternehmen offen legen! 169

Vorwort

Das Spektrum der Themen, mit denen sich die Beauftragten für Datenschutz und Informationsfreiheit auseinanderzusetzen haben, wird ständig breiter. Um diesen beiden Grundrechten Geltung zu verschaffen, stimmen die Beauftragten sich auf nationaler und internationaler Ebene ab und äußern sich in Entschließungen und Stellungnahmen, die für das zurückliegende Jahr erneut in diesem Dokumentenband zusammengefasst sind.

Neben Themen, die schon lange auf der Tagesordnung stehen wie die Vorratsdatenspeicherung und der Beschäftigtendatenschutz, hat sich die deutsche Datenschutzkonferenz erstmals zu intelligenten Stromzählern und -netzen und zur geplanten Bundesstiftung Datenschutz geäußert. Die im „Düsseldorfer Kreis" zusammenarbeitenden Aufsichtsbehörden für den Datenschutz in der Wirtschaft haben ebenfalls zahlreiche Beschlüsse zu aktuellen Themen gefasst, darunter zum Safe Harbor-Abkommen mit den USA und zum wirksamen Schutz von Minderjährigen in sozialen Netzwerken.

Auch die Umsetzung der geänderten europäischen Richtlinie zum Datenschutz in der elektronischen Kommunikation hat die Aufsichtsbehörden zu einer Stellungnahme veranlasst, weil die Bundesregierung hier bisher den Änderungsbedarf im nationalen Recht unterschätzt. Diese „ePrivacy-Richtlinie" ist ohnehin angesichts der heute vorherrschenden elektronischen Informations- und Kommunikationsdienste (Telemedien) so bedeutsam für den Datenschutz, dass ihr in dieser konsolidierten Form noch nicht veröffentlichter Text ebenfalls in den vorliegenden Band aufgenommen wurde. Zu der im Internet weit verbreiteten Praxis der gezielten Werbung (Behavioral Targeting), die nach der geänderten Richtlinie den Datenschutz stärker berücksichtigen muss, hat die Gruppe nach Art. 29 der Datenschutzrichtlinie ein Arbeitspapier beschlossen, das für Aufsehen in der Werbewirtschaft gesorgt hat.

Auch die als „Berlin Group" bekannte Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat zum Datenschutz in der digitalen Welt einen Forderungskatalog formuliert. Daneben standen praktische Fragen wie die Nutzung der „Deep Packet Inspection"-Technologie für Werbezwecke auf der Tagesordnung dieser Gruppe.

Die deutschen Informationsfreiheitsbeauftragten setzten sich für die Informationsfreiheit bei den Rundfunkanstalten und für die Offenlegung von Verträgen zwischen der öffentlichen Hand und privaten Investoren nach dem Vorbild Berlins ein. Schließlich warben sie für das in den USA und Großbritannien bereits

stärker akzeptierte Open Data-Konzept, bei dem Behörden Informationen von Amts wegen und nicht erst auf Antrag öffentlich bereitstellen. Die Wikileaks-Veröffentlichungen sollten nicht als Vorwand für den Rückfall in eine ungerechtfertigte Geheimhaltung dienen.

Diese Dokumentensammlung kann auch über unsere Webseite abgerufen werden.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließungen der 79. Konferenz am 17./18. März 2010 in Stuttgart

Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

– Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.

– Es darf keine Fach- und Rechtsaufsicht geben.

– Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

– Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.

– Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.

– Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung" des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,

– die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
– die Leistung, Wirkung sowie der Erfolg und die Effizienz,
– die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Ab-

rechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

2. Entschließungen zwischen der 79. und 80. Konferenz

Beschäftigtendatenschutz stärken statt abbauen (vom 22. Juni 2010)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

– Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

– Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen –, weiterhin zu unterbleiben haben.

– Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

– Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

– Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Erweiterung der Steuerdatenbank enthält große Risiken (vom 24. Juni 2010)

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs
  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept
  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsicht-

lich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz! (vom 11. Oktober 2010)

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

3. Entschließungen der 80. Konferenz am 3./4. November in Freiburg

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

– die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,

– die größtmögliche Transparenz der Tätigkeit garantiert ist und

– die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

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

1. Beschluss der Sitzung am 28./29. April 2010 in Hannover (in der Fassung vom 23. August 2010)

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor)[1]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das im-

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

portierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

2. Beschlüsse der Sitzung am 24./25. November 2010 in Düsseldorf

Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitglie-

[2] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

dern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.
- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.
- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert,

wenn die Betreiber eine freiwillige Alterskennzeichnung von lnternetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen

diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle

   - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

   - umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,

   - Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

   - Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,

   - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),

   - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),

   - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und

   - Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt der Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer

Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.

3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.

4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.

5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

III. Europäische Konferenz der Datenschutzbeauftragten

Prag, 29./30. April 2010

Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen

Der gescheiterte Anschlag auf den Delta Flug 253 Amsterdam – Detroit am 25. Dezember 2009 entfachte eine weltweite Diskussion bei Regierungen und Sicherheitsbehörden darüber, wie die Sicherheit auf Flughäfen erhöht werden könnte und ob Körperscanner zur Erleichterung der Kontrollen der Flugpassagiere, bevor sie an Bord gehen, eingesetzt werden sollten. Der Einsatz solcher Körperscanner und das Durchleuchten des gesamten menschlichen Körpers kann eine schwere Verletzung des Rechts des Passagiers auf Schutz der Privatsphäre und auf Datenschutz darstellen. Daher sollten Datenschutzprinzipien und -sicherungsmaßnahmen ebenso berücksichtigt werden wie „Privacy by Design", wenn der Einsatz von Körperscannern in Erwägung gezogen wird.

Die Notwendigkeit der Verarbeitung ist eines der Datenschutzprinzipien, das berücksichtigt werden muss. Es ist immer noch nicht klar, ob sich mit diesen Geräten wirklich eine höhere Sicherheit an Flughäfen erreichen lässt. Vor ihrem Einsatz muss auch die Frage hinsichtlich ihrer Effektivität und ihrer Auswirkungen auf die Gesundheit der Passagiere in Betracht gezogen werden.

Vor dem Hintergrund des aktuellen Diskussionsstandes sieht die Europäische Datenschutzkonferenz mit Besorgnis, dass neue Geräte eingesetzt werden, die nicht den Datenschutzstandards entsprechen. Deshalb möchte die Konferenz die Notwendigkeit einer wissenschaftlich fundierten und koordinierten Diskussion dieses Themas betonen.[1] Alle Interessengruppen, wie Wissenschaftler, Technikexperten, Fachleute aus den Bereichen Gesundheit und Datenschutz sollten angehört werden, um zu einer angemessenen Bewertung der anstehenden Punkte zu gelangen. Insbesondere sind vor einer voreiligen Entscheidung zu dem Einsatz von Körperscannern die folgenden Aspekte anzusprechen.

[1] Die Artikel 29 Arbeitsgruppe hat am 11. Februar 2009 ein Arbeitspapier zu Körperscannern angenommen. Dieses Arbeitspapier und der Begleitbrief an die Europäische Kommission ist auf folgender Webseite zu finden: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_annex_consultation_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

1. Ist der Einsatz von Körperscannern an Flughäfen für die Flugsicherheit notwendig und wenn ja, in welchen Ausmaß? Zu dieser Frage sind detaillierte Studien unter Einbeziehung wissenschaftlicher Methoden durchzuführen. Die Nützlichkeit der Körperscanner sollte auf einer soliden empirischen Grundlage bewiesen werden. Bis heute gibt es ernsthafte Zweifel hinsichtlich der erweiterten Fähigkeiten der Körperscanner mit Blick auf die Detektierbarkeit explosiver Stoffe, wie zum Beispiel kleiner Mengen von Flüssigkeiten oder anderer Stoffen von geringer Dichte. Ist im Vergleich mit anderen Methoden zur Personenkontrolle wie dem Gang durch Metalldetektoren, Handscannern oder Leibesvisitationen ein Zugewinn an Sicherheit zu verzeichnen? Falls es weniger einschneidende Methoden zur Erreichung des gleichen zusätzlichen Sicherheitsniveaus gibt[2], dann sollten diese genutzt werden.

2. Gibt es angemessene Schutzmaßnahmen, die die Privatsphäre der durch Körperscanner durchleuchteten Personen gewährleisten? Technische Maßnahmen müssen sicherstellen, dass die personenbezogenen Daten der Reisenden weder gespeichert noch weitergeleitet werden. Sobald der Passagier für sicher erklärt wurde, sollten die Bilder sofort gelöscht werden. Schematische Darstellungen der Körper von Personen sind überaus datenschutzfreundlich. Daher könnte dieser Methode, Körper auf Bildschirmen zu zeigen, der Vorzug gegeben werden. Falls intime Details von Personen, wie z. B. medizinische Hilfsmittel oder künstliche Körperteile angezeigt werden, sollten sie nur für die diensthabende Person zu sehen sein. Die mit dem Ansehen der vom Körperscanner angezeigten Bilder befassten Personen dürfen nicht mit den Personen, die an weiteren Kontrollen beteiligt sind, identisch sein. Sie müssen ihre Aufgaben in Einrichtungen wahrnehmen, die ihnen keine Kommunikation mit den anderen Kontrolleuren erlauben, und sie dürfen nicht in der Lage sein, die Passagiere zu sehen. Außerdem sollten Körperscanner nur eingesetzt werden, nachdem eine Datenschutz-Verträglichkeitsprüfung (PIA) durchgeführt wurde, aus der hervorgehen sollte, dass die hier erwähnten Grundsätze mit einbezogen wurden.

Nur wenn ein fairer Ausgleich zwischen der Effektivität und Notwendigkeit dieser neuen technologischen Geräte einerseits und der Auswirkung auf die Privatsphäre der Flugpassagiere andererseits geschaffen wird, könnte der Einsatz von Körperscannern aus datenschutzrechtlicher Sicht als angemessen und als ein geeignetes Mittel für die Sicherheitsdurchleuchtung betrachtet werden.

Deshalb ruft die Europäische Datenschutzkonferenz alle Entscheidungsträger aus ganz Europa dazu auf, gründlich über die Auswirkungen der Körperscanner auf die Grundrechte der Reisenden nachzudenken, bevor sie ihren Einsatz am Flughafen beschließen.

[2] wie z. B. Handscanner oder Spürhunde

Es sollten nur Geräte eingesetzt werden, in die datenschutzfreundliche Technologien eingebaut wurden und die einen angemessenen Ausgleich zwischen der Notwendigkeit nach erhöhter Sicherheit und dem Recht auf Schutz der Privatsphäre und des Datenschutzes schaffen. Die Datenschutzbehörden sollten weiterhin in den Entscheidungsprozess einbezogen werden, insbesondere während der Probe- und Testphasen, vor allem durch Vorabprüfung von Körperscannersystemen (falls nach nationalem Recht anwendbar) und durch Kontrollmöglichkeiten mit Blick auf das Funktionieren der Geräte nach deren Installation.

Die Passagiere sollten vor der Kontrolle durch Körperscanner angemessen über diese Geräte und über ihre Datenschutzrechte informiert werden. Zu diesem Zweck sollten die Flughafenbehörden eng mit ihren jeweils zuständigen Datenschutzbehörden zusammenarbeiten um sicherzustellen, dass entsprechende Merkblätter den rechtlichen Anforderungen entsprechen.

Entschließung zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf der Grundlage des Abschlussberichts der sogenannten High Level Contact Group wollen Vertreter der Europäischen Union und der Vereinigten Staaten von Amerika Verhandlungen über ein Abkommen zu Datenschutzstandards für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aufnehmen.

Die Europäischen Datenschutzbeauftragten begrüßen dieses Vorhaben sehr. Sie hegen große Hoffnung, dass sich die Europäische Union und die Vereinigten Staaten von Amerika durch dieses Abkommen verpflichten werden, beim Austausch personenbezogener Daten in Strafsachen ein hohes Datenschutzniveau einzuhalten und dadurch ein Beispiel für andere internationale Abkommen zum Datenaustausch im Bereich der Strafverfolgung geben.

Die europäischen Datenschutzbeauftragten messen dem Abkommen große Bedeutung bei, denn angesichts von internationalem Terrorismus und grenzüberschreitender Kriminalität werden die Herausforderungen an die internationale Kooperation von Strafverfolgungsbehörden aller Voraussicht nach weiter anwachsen und damit auch die Bedingungen für den internationalen Datenaustausch zwischen den Sicherheitsbehörden zunehmend auf der politischen Tagesordnung stehen.

In diesem Sinne fordert die Europäische Datenschutzkonferenz die Europäische Union auf, sich für ein hohes Datenschutzniveau stark zu machen und – mittels

dieses Abkommens – unverrückbare Prinzipien – insbesondere eine enge Zweckbindung der übermittelten Daten, eine hohe Datensicherheit, unabhängige Datenschutzaufsichtsbehörden sowie das Auskunftsrecht und den gerichtlichen Rechtsschutz für alle Betroffenen, unabhängig von ihrer Nationalität oder ihres Aufenthaltslandes – auch bei einem Datenaustausch mit den USA auf effektive Weise sicherzustellen.

Nähere Einzelheiten zu den Erwartungen und Hoffnungen der Europäischen Datenschutzkonferenz finden Sie in dem gemeinsamen Beitrag der WPPJ und der Artikel 29-Arbeitsgruppe zu der öffentlichen Konsultation der Europäischen Kommission in dieser Angelegenheit.

IV. Dokumente der Europäischen Union

1. Europäisches Parlament und Rat

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der Fassung der Richtlinie 2009/136/EG vom 25. November 2009[1]

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 95,

auf Vorschlag der Kommission[2],

nach Stellungnahme des Wirtschafts- und Sozialausschusses[3],

nach Anhörung des Ausschusses der Regionen,

gemäß dem Verfahren des Artikels 251 des Vertrags[4],

in Erwägung nachstehender Gründe:

(1) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[5] schreibt vor, dass die Mitgliedstaaten die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten und insbesondere ihr Recht auf Privatsphäre sicherstellen, um in der Gemeinschaft den freien Verkehr personenbezogener Daten zu gewährleisten.

---

1 Es handelt sich um eine nicht amtliche konsolidierte Fassung der Richtlinie 2002/58/EG (ABl. L 201 vom 31.7.2002, S. 37) mit den Änderungen durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11).

2 ABl. C 365 E vom 19.12.2000, S. 223.

3 ABl. C 123 vom 25.4.2001, S. 53.

4 Stellungnahme des Europäischen Parlaments vom 13. November 2001, Gemeinsamer Standpunkt des Rates vom 28. Januar 2002 (ABl. C 113 E vom 14.5.2002, S. 39) und Beschluss des Europäischen Parlaments vom 30. Mai 2002. Beschluss des Rates vom 25. Juni 2002.

5 ABl. L 281 vom 23.11.1995, S. 31.

(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.

(3) Die Vertraulichkeit der Kommunikation wird nach den internationalen Menschenrechtsübereinkünften, insbesondere der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, und den Verfassungen der Mitgliedstaaten garantiert.

(4) Mit der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[10] wurden die Grundsätze der Richtlinie 95/46/EG in spezielle Vorschriften für den Telekommunikationssektor umgesetzt. Die Richtlinie 97/66/EG muss an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden, um den Nutzern öffentlich zugänglicher elektronischer Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie den gleichen Grad des Schutzes personenbezogener Daten und der Privatsphäre zu bieten. Jene Richtlinie ist daher aufzuheben und durch die vorliegende Richtlinie zu ersetzen.

(5) Gegenwärtig werden öffentliche Kommunikationsnetze in der Gemeinschaft mit fortschrittlichen neuen Digitaltechnologien ausgestattet, die besondere Anforderungen an den Schutz personenbezogener Daten und der Privatsphäre des Nutzers mit sich bringen. Die Entwicklung der Informationsgesellschaft ist durch die Einführung neuer elektronischer Kommunikationsdienste gekennzeichnet. Der Zugang zu digitalen Mobilfunknetzen ist für breite Kreise möglich und erschwinglich geworden. Diese digitalen Netze verfügen über große Kapazitäten und Möglichkeiten zur Datenverarbeitung. Die erfolgreiche grenzüberschreitende Entwicklung dieser Dienste hängt zum Teil davon ab, inwieweit die Nutzer darauf vertrauen, dass ihre Privatsphäre unangetastet bleibt.

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

(7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und

[6] ABl. L 24 vom 30.1.1998, S. 1.

Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

(8) Die von den Mitgliedstaaten erlassenen rechtlichen, ordnungspolitischen und technischen Bestimmungen zum Schutz personenbezogener Daten, der Privatsphäre und der berechtigten Interessen juristischer Personen im Bereich der elektronischen Kommunikation sollten harmonisiert werden, um Behinderungen des Binnenmarktes der elektronischen Kommunikation nach Artikel 14 des Vertrags zu beseitigen. Die Harmonisierung sollte sich auf die Anforderungen beschränken, die notwendig sind, um zu gewährleisten, dass die Entstehung und die Weiterentwicklung neuer elektronischer Kommunikationsdienste und -netze zwischen Mitgliedstaaten nicht behindert werden.

(9) Die Mitgliedstaaten, die betroffenen Anbieter und Nutzer sowie die zuständigen Stellen der Gemeinschaft sollten bei der Einführung und Weiterentwicklung der entsprechenden Technologien zusammenarbeiten, soweit dies zur Anwendung der in dieser Richtlinie vorgesehenen Garantien erforderlich ist; als Ziele zu berücksichtigen sind dabei insbesondere die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß und die Verwendung anonymer oder pseudonymer Daten.

(10) Im Bereich der elektronischen Kommunikation gilt die Richtlinie 95/46/EG vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen. Die Richtlinie 95/46/EG gilt für nicht öffentliche Kommunikationsdienste.

(11) Wie die Richtlinie 95/46/EG gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die

Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

(12) Bei den Teilnehmern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann es sich um natürliche oder juristische Personen handeln. Diese Richtlinie zielt durch Ergänzung der Richtlinie 95/46/EG darauf ab, die Grundrechte natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, sowie die berechtigten Interessen juristischer Personen zu schützen. Aus dieser Richtlinie ergibt sich keine Verpflichtung der Mitgliedstaaten, die Richtlinie 95/46/EG auf den Schutz der berechtigten Interessen juristischer Personen auszudehnen, der im Rahmen der geltenden gemeinschaftlichen und einzelstaatlichen Rechtsvorschriften sichergestellt ist.

(13) Das Vertragsverhältnis zwischen einem Teilnehmer und einem Diensteanbieter kann zu einer regelmäßigen oder einmaligen Zahlung für den erbrachten oder zu erbringenden Dienst führen. Auch vorbezahlte Karten gelten als eine Form des Vertrags.

(14) Standortdaten können sich beziehen auf den Standort des Endgeräts des Nutzers nach geografischer Länge, Breite und Höhe, die Übertragungsrichtung, den Grad der Genauigkeit der Standortinformationen, die Identifizierung des Netzpunktes, an dem sich das Endgerät zu einem bestimmten Zeitpunkt befindet, und den Zeitpunkt, zu dem die Standortinformationen erfasst wurden.

(15) Eine Nachricht kann alle Informationen über Namen, Nummern oder Adressen einschließen, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt. Der Begriff „Verkehrsdaten“ kann alle Formen einschließen, in die diese Informationen durch das Netz, über das die Nachricht übertragen wird, für die Zwecke der Übermittlung umgewandelt werden. Verkehrsdaten können sich unter anderem auf die Leitwege, die Dauer, den Zeitpunkt oder die Datenmenge einer Nachricht, das verwendete Protokoll, den Standort des Endgeräts des Absenders oder Empfängers, das Netz, von dem die Nachricht ausgeht bzw. an das es gesendet wird, oder den Beginn, das Ende oder die Dauer einer Verbindung beziehen. Sie können auch das Format betreffen, in dem die Nachricht über das Netz weitergeleitet wird.

(16) Eine Information, die als Teil eines Rundfunkdienstes über ein öffentliches Kommunikationsnetz weitergeleitet wird, ist für einen potenziell unbegrenzten Personenkreis bestimmt und stellt keine Nachricht im Sinne dieser Richtlinie dar.

Kann jedoch ein einzelner Teilnehmer oder Nutzer, der eine derartige Information erhält, beispielsweise durch einen Videoabruf-Dienst identifiziert werden, so ist die weitergeleitete Information als Nachricht im Sinne dieser Richtlinie zu verstehen.

(17) Für die Zwecke dieser Richtlinie sollte die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person". Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website.

(18) Dienste mit Zusatznutzen können beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen umfassen.

(19) Die Anwendung bestimmter Anforderungen für die Anzeige des rufenden und angerufenen Anschlusses sowie für die Einschränkung dieser Anzeige und für die automatische Weiterschaltung zu Teilnehmeranschlüssen, die an analoge Vermittlungen angeschlossen sind, sollte in besonderen Fällen nicht zwingend vorgeschrieben werden, wenn sich die Anwendung als technisch nicht machbar erweist oder einen unangemessen hohen wirtschaftlichen Aufwand erfordert. Für die Beteiligten ist es wichtig, in solchen Fällen in Kenntnis gesetzt zu werden, und die Mitgliedstaaten müssen sie deshalb der Kommission anzeigen.

(20) Diensteanbieter sollen geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Dienste, erforderlichenfalls zusammen mit dem Netzbetreiber, zu gewährleisten, und die Teilnehmer über alle besonderen Risiken der Verletzung der Netzsicherheit unterrichten. Solche Risiken können vor allem bei elektronischen Kommunikationsdiensten auftreten, die über ein offenes Netz wie das Internet oder den analogen Mobilfunk bereitgestellt werden. Der Diensteanbieter muss die Teilnehmer und Nutzer solcher Dienste unbedingt vollständig über die Sicherheitsrisiken aufklären, gegen die er selbst keine Abhilfe bieten kann. Diensteanbieter, die öffentlich zugängliche elektronische Kommunikationsdienste über das Internet anbieten, sollten die Nutzer und Teilnehmer über Maßnahmen zum Schutz ihrer zu übertragenden Nachrichten informieren, wie z. B. den Einsatz spezieller Software oder von Verschlüsselungstechniken. Die Anforderung, die Teilnehmer über besondere Sicherheitsrisiken aufzuklären, entbindet einen Diensteanbieter nicht von der Verpflichtung, auf eigene Kosten unverzüglich geeignete Maßnahmen zu treffen, um einem neuen, unvorhergesehenen Sicherheitsrisiko vorzubeugen und den normalen Sicherheitsstandard des Dienstes

wiederherzustellen. Abgesehen von den nominellen Kosten, die dem Teilnehmer bei Erhalt oder Abruf der Information entstehen, beispielsweise durch das Laden einer elektronischen Post, sollte die Bereitstellung der Informationen über Sicherheitsrisiken für die Teilnehmer kostenfrei sein. Die Bewertung der Sicherheit erfolgt unter Berücksichtigung des Artikels 17 der Richtlinie 95/46/EG.

(21) Es sollten Maßnahmen getroffen werden, um den unerlaubten Zugang zu Nachrichten – und zwar sowohl zu ihrem Inhalt als auch zu mit ihnen verbundenen Daten – zu verhindern und so die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen elektronischen Kommunikationsdiensten erfolgenden Nachrichtenübertragung zu schützen. Nach dem Recht einiger Mitgliedstaaten ist nur der absichtliche unberechtigte Zugriff auf die Kommunikation untersagt.

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. Wenn dies für eine effizientere Weiterleitung einer öffentlich zugänglichen Information an andere Empfänger des Dienstes auf ihr Ersuchen hin erforderlich ist, sollte diese Richtlinie dem nicht entgegenstehen, dass die Information länger gespeichert wird, sofern diese Information der Öffentlichkeit auf jeden Fall uneingeschränkt zugänglich wäre und Daten, die einzelne, die Information anfordernde Teilnehmer oder Nutzer betreffen, gelöscht würden.

(23) Die Vertraulichkeit von Nachrichten sollte auch im Rahmen einer rechtmäßigen Geschäftspraxis sichergestellt sein. Falls erforderlich und rechtlich zulässig, können Nachrichten zum Nachweis einer kommerziellen Transaktion aufgezeichnet werden. Diese Art der Verarbeitung fällt unter die Richtlinie 95/46/EG. Die von der Nachricht betroffenen Personen sollten vorab von der Absicht der Aufzeichnung, ihrem Zweck und der Dauer ihrer Speicherung in Kenntnis gesetzt werden. Die aufgezeichnete Nachricht sollte so schnell wie möglich und auf jeden Fall spätestens mit Ablauf der Frist gelöscht werden, innerhalb deren die Transaktion rechtmäßig angefochten werden kann.

(24) 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. So genannte „Spyware“, „Web-Bugs“, „Hidden Identifiers“ und ähnliche Instrumente können ohne das Wissen

des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.

(25) Solche Instrumente, z. B. so genannte „Cookies", können ein legitimes und nützliches Hilfsmittel sein, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen. Dienen solche Instrumente, z. B. „Cookies", einem rechtmäßigen Zweck, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft, so sollte deren Einsatz unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/EG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer muss wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden. Die Nutzer sollten die Gelegenheit haben, die Speicherung eines Cookies oder eines ähnlichen Instruments in ihrem Endgerät abzulehnen. Dies ist besonders bedeutsam, wenn auch andere Nutzer Zugang zu dem betreffenden Endgerät haben und damit auch zu dort gespeicherten Daten, die sensible Informationen privater Natur beinhalten. Die Auskunft und das Ablehnungsrecht können einmalig für die Nutzung verschiedener in dem Endgerät des Nutzers während derselben Verbindung zu installierender Instrumente angeboten werden und auch die künftige Verwendung derartiger Instrumente umfassen, die während nachfolgender Verbindungen vorgenommen werden können. Die Modalitäten für die Erteilung der Informationen oder für den Hinweis auf das Verweigerungsrecht und die Einholung der Zustimmung sollten so benutzerfreundlich wie möglich sein. Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt.

(26) Teilnehmerdaten, die in elektronischen Kommunikationsnetzen zum Verbindungsaufbau und zur Nachrichtenübertragung verarbeitet werden, enthalten Informationen über das Privatleben natürlicher Personen und betreffen ihr Recht auf Achtung ihrer Kommunikationsfreiheit, oder sie betreffen berechtigte Interessen juristischer Personen. Diese Daten dürfen nur für einen begrenzten Zeitraum und nur insoweit gespeichert werden, wie dies für die Erbringung des Dienstes, für die Gebührenabrechnung und für Zusammenschaltungszahlungen erforderlich ist. Jede weitere Verarbeitung solcher Daten, die der Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen vornehmen möchte, darf nur unter der Bedingung gestattet werden, dass der Teilnehmer dieser Verarbeitung auf der Grundlage ge-

nauer, vollständiger Angaben des Betreibers des öffentlich zugänglichen elektronischen Kommunikationsdienstes über die Formen der von ihm beabsichtigten weiteren Verarbeitung und über das Recht des Teilnehmers, seine Einwilligung zu dieser Verarbeitung nicht zu erteilen oder zurückzuziehen, zugestimmt hat. Verkehrsdaten, die für die Vermarktung von Kommunikationsdiensten oder für die Bereitstellung von Diensten mit Zusatznutzen verwendet wurden, sollten ferner nach der Bereitstellung des Dienstes gelöscht oder anonymisiert werden. Diensteanbieter sollen die Teilnehmer stets darüber auf dem Laufenden halten, welche Art von Daten sie verarbeiten und für welche Zwecke und wie lange das geschieht.

(27) Der genaue Zeitpunkt des Abschlusses der Übermittlung einer Nachricht, nach dem die Verkehrsdaten außer zu Fakturierungszwecken gelöscht werden sollten, kann von der Art des bereitgestellten elektronischen Kommunikationsdienstes abhängen. Bei einem Sprach-Telefonanruf beispielsweise ist die Übermittlung abgeschlossen, sobald einer der Teilnehmer die Verbindung beendet. Bei der elektronischen Post ist die Übermittlung dann abgeschlossen, wenn der Adressat die Nachricht – üblicherweise vom Server seines Diensteanbieters – abruft.

(28) Die Verpflichtung, Verkehrsdaten zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, steht nicht im Widerspruch zu im Internet angewandten Verfahren wie dem Caching von IP-Adressen im Domain-Namen-System oder dem Caching einer IP-Adresse, die einer physischen Adresse zugeordnet ist, oder der Verwendung von Informationen über den Nutzer zum Zwecke der Kontrolle des Rechts auf Zugang zu Netzen oder Diensten.

(29) Der Diensteanbieter kann Verkehrsdaten in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeiten, um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln. Für Fakturierungszwecke notwendige Verkehrsdaten dürfen ebenfalls vom Diensteanbieter verarbeitet werden, um Fälle von Betrug, die darin bestehen, die elektronischen Kommunikationsdienste ohne entsprechende Bezahlung nutzen, ermitteln und abstellen zu können.

(30) Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste sollten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. Jedwede Tätigkeit im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste, die über die Übermittlung einer Nachricht und die Fakturierung dieses Vorgangs hinausgeht, sollte auf aggregierten Verkehrsdaten basieren, die nicht mit Teilnehmern oder Nutzern in Verbindung gebracht werden können. Können diese Tätigkeiten nicht auf aggregierte Daten gestützt werden, so sollten sie als Dienste mit Zusatznutzen angesehen werden, für die die Einwilligung des Teilnehmers erforderlich ist.

(31) Ob die Einwilligung in die Verarbeitung personenbezogener Daten im Hinblick auf die Erbringung eines speziellen Dienstes mit Zusatznutzen beim Nutzer oder beim Teilnehmer eingeholt werden muss, hängt von den zu verarbeitenden Daten, von der Art des zu erbringenden Dienstes und von der Frage ab, ob es technisch, verfahrenstechnisch und vertraglich möglich ist, zwischen der einen elektronischen Kommunikationsdienst in Anspruch nehmenden Einzelperson und der an diesem Dienst teilnehmenden juristischen oder natürlichen Person zu unterscheiden.

(32) Vergibt der Betreiber eines elektronischen Kommunikationsdienstes oder eines Dienstes mit Zusatznutzen die für die Bereitstellung dieser Dienste erforderliche Verarbeitung personenbezogener Daten an eine andere Stelle weiter, so sollten diese Weitervergabe und die anschließende Datenverarbeitung in vollem Umfang den Anforderungen in Bezug auf die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter im Sinne der Richtlinie 95/46/EG entsprechen. Erfordert die Bereitstellung eines Dienstes mit Zusatznutzen die Weitergabe von Verkehrsdaten oder Standortdaten von dem Betreiber eines elektronischen Kommunikationsdienstes an einen Betreiber eines Dienstes mit Zusatznutzen, so sollten die Teilnehmer oder Nutzer, auf die sich die Daten beziehen, ebenfalls in vollem Umfang über diese Weitergabe unterrichtet werden, bevor sie in die Verarbeitung der Daten einwilligen.

(33) Durch die Einführung des Einzelgebührennachweises hat der Teilnehmer mehr Möglichkeiten erhalten, die Richtigkeit der vom Diensteanbieter erhobenen Entgelte zu überprüfen, gleichzeitig kann dadurch aber eine Gefahr für die Privatsphäre der Nutzer öffentlich zugänglicher elektronischer Kommunikationsdienste entstehen. Um die Privatsphäre des Nutzers zu schützen, müssen die Mitgliedstaaten daher darauf hinwirken, dass bei den elektronischen Kommunikationsdiensten beispielsweise alternative Funktionen entwickelt werden, die den anonymen oder rein privaten Zugang zu öffentlich zugänglichen elektronischen Kommunikationsdiensten ermöglichen, beispielsweise Telefonkarten und Möglichkeiten der Zahlung per Kreditkarte. Zu dem gleichen Zweck können die Mitgliedstaaten die Anbieter auffordern, ihren Teilnehmern eine andere Art von ausführlicher Rechnung anzubieten, in der eine bestimmte Anzahl von Ziffern der Rufnummer unkenntlich gemacht ist.

(34) Im Hinblick auf die Rufnummernanzeige ist es erforderlich, das Recht des Anrufers zu wahren, die Anzeige der Rufnummer des Anschlusses, von dem aus der Anruf erfolgt, zu unterdrücken, ebenso wie das Recht des Angerufenen, Anrufe von nicht identifizierten Anschlüssen abzuweisen. Es ist gerechtfertigt, in Sonderfällen die Unterdrückung der Rufnummernanzeige aufzuheben. Bestimmte Teilnehmer, insbesondere telefonische Beratungsdienste und ähnliche Einrichtungen, haben ein Interesse daran, die Anonymität ihrer Anrufer zu gewährleisten. Im Hinblick auf die Anzeige der Rufnummer des Angerufenen ist es

erforderlich, das Recht und das berechtigte Interesse des Angerufenen zu wahren, die Anzeige der Rufnummer des Anschlusses, mit dem der Anrufer tatsächlich verbunden ist, zu unterdrücken; dies gilt besonders für den Fall weitergeschalteter Anrufe. Die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste sollten ihre Teilnehmer über die Möglichkeit der Anzeige der Rufnummer des Anrufenden und des Angerufenen, über alle Dienste, die auf der Grundlage der Anzeige der Rufnummer des Anrufenden und des Angerufenen angeboten werden, sowie über die verfügbaren Funktionen zur Wahrung der Vertraulichkeit unterrichten. Die Teilnehmer können dann sachkundig die Funktionen auswählen, die sie zur Wahrung der Vertraulichkeit nutzen möchten. Die Funktionen zur Wahrung der Vertraulichkeit, die anschlussbezogen angeboten werden, müssen nicht unbedingt als automatischer Netzdienst zur Verfügung stehen, sondern können von dem Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes auf einfachen Antrag bereitgestellt werden.

(35) In digitalen Mobilfunknetzen werden Standortdaten verarbeitet, die Aufschluss über den geografischen Standort des Endgeräts des mobilen Nutzers geben, um die Nachrichtenübertragung zu ermöglichen. Solche Daten sind Verkehrsdaten, die unter Artikel 6 dieser Richtlinie fallen. Doch können digitale Mobilfunknetze zusätzlich auch in der Lage sein, Standortdaten zu verarbeiten, die genauer sind als es für die Nachrichtenübertragung erforderlich wäre und die für die Bereitstellung von Diensten mit Zusatznutzen verwendet werden, wie z. B. persönliche Verkehrsinformationen und Hilfen für den Fahrzeugführer. Die Verarbeitung solcher Daten für die Bereitstellung von Diensten mit Zusatznutzen soll nur dann gestattet werden, wenn die Teilnehmer darin eingewilligt haben. Selbst dann sollten sie die Möglichkeit haben, die Verarbeitung von Standortdaten auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(36) Die Mitgliedstaaten können die Rechte der Nutzer und Teilnehmer auf Privatsphäre in Bezug auf die Rufnummernanzeige einschränken, wenn dies erforderlich ist, um belästigende Anrufe zurückzuverfolgen; in Bezug auf Rufnummernanzeige und Standortdaten kann dies geschehen, wenn es erforderlich ist, Notfalldiensten zu ermöglichen, ihre Aufgaben so effektiv wie möglich zu erfüllen. Hierzu können die Mitgliedstaaten besondere Vorschriften erlassen, um die Anbieter von elektronischen Kommunikationsdiensten zu ermächtigen, einen Zugang zur Rufnummernanzeige und zu Standortdaten ohne vorherige Einwilligung der betreffenden Nutzer oder Teilnehmer zu verschaffen.

(37) Es sollten Vorkehrungen getroffen werden, um die Teilnehmer vor eventueller Belästigung durch die automatische Weiterschaltung von Anrufen durch andere zu schützen. In derartigen Fällen muss der Teilnehmer durch einfachen Antrag beim Betreiber des öffentlich zugänglichen elektronischen Kommunikationsdienstes die Weiterschaltung von Anrufen auf sein Endgerät unterbinden können.

(38) Die Verzeichnisse der Teilnehmer elektronischer Kommunikationsdienste sind weit verbreitet und öffentlich. Das Recht auf Privatsphäre natürlicher Personen und das berechtigte Interesse juristischer Personen erfordern daher, dass die Teilnehmer bestimmen können, ob ihre persönlichen Daten – und gegebenenfalls welche – in einem Teilnehmerverzeichnis veröffentlicht werden. Die Anbieter öffentlicher Verzeichnisse sollten die darin aufzunehmenden Teilnehmer über die Zwecke des Verzeichnisses und eine eventuelle besondere Nutzung elektronischer Fassungen solcher Verzeichnisse informieren; dabei ist insbesondere an in die Software eingebettete Suchfunktionen gedacht, etwa die umgekehrte Suche, mit deren Hilfe Nutzer des Verzeichnisses den Namen und die Anschrift eines Teilnehmers allein aufgrund dessen Telefonnummer herausfinden können.

(39) Die Verpflichtung zur Unterrichtung der Teilnehmer über den Zweck bzw. die Zwecke öffentlicher Verzeichnisse, in die ihre personenbezogenen Daten aufzunehmen sind, sollte demjenigen auferlegt werden, der die Daten für die Aufnahme erhebt. Können die Daten an einen oder mehrere Dritte weitergegeben werden, so sollte der Teilnehmer über diese Möglichkeit und über den Empfänger oder die Kategorien möglicher Empfänger unterrichtet werden. Voraussetzung für die Weitergabe sollte sein, dass die Daten nicht für andere Zwecke als diejenigen verwendet werden, für die sie erhoben wurden. Wünscht derjenige, der die Daten beim Teilnehmer erhebt, oder ein Dritter, an den die Daten weitergegeben wurden, diese Daten zu einem weiteren Zweck zu verwenden, so muss entweder der ursprüngliche Datenerheber oder der Dritte, an den die Daten weitergegeben wurden, die erneute Einwilligung des Teilnehmers einholen.

(40) Es sollten Vorkehrungen getroffen werden, um die Teilnehmer gegen die Verletzung ihrer Privatsphäre durch unerbetene Nachrichten für Zwecke der Direktwerbung, insbesondere durch automatische Anrufsysteme, Faxgeräte und elektronische Post, einschließlich SMS, zu schützen. Diese Formen von unerbetenen Werbenachrichten können zum einen relativ leicht und preiswert zu versenden sein und zum anderen eine Belastung und/oder einen Kostenaufwand für den Empfänger bedeuten. Darüber hinaus kann in einigen Fällen ihr Umfang auch Schwierigkeiten für die elektronischen Kommunikationsnetze und die Endgeräte verursachen. Bei solchen Formen unerbetener Nachrichten zum Zweck der Direktwerbung ist es gerechtfertigt, zu verlangen, die Einwilligung der Empfänger einzuholen, bevor ihnen solche Nachrichten gesandt werden. Der Binnenmarkt verlangt einen harmonisierten Ansatz, damit für die Unternehmen und die Nutzer einfache, gemeinschaftsweite Regeln gelten.

(41) Im Rahmen einer bestehenden Kundenbeziehung ist es vertretbar, die Nutzung elektronischer Kontaktinformationen zuzulassen, damit ähnliche Produkte oder Dienstleistungen angeboten werden; dies gilt jedoch nur für dasselbe Unternehmen, das auch die Kontaktinformationen gemäß der Richtlinie 95/46/EG erhalten hat. Bei der Erlangung der Kontaktinformationen sollte der Kunde über

deren weitere Nutzung zum Zweck der Direktwerbung klar und eindeutig unterrichtet werden und die Möglichkeit erhalten, diese Verwendung abzulehnen. Diese Möglichkeit sollte ferner mit jeder weiteren als Direktwerbung gesendeten Nachricht gebührenfrei angeboten werden, wobei Kosten für die Übermittlung der Ablehnung nicht unter die Gebührenfreiheit fallen.

(42) Sonstige Formen der Direktwerbung, die für den Absender kostspieliger sind und für die Teilnehmer und Nutzer keine finanziellen Kosten mit sich bringen, wie Sprach-Telefonanrufe zwischen Einzelpersonen, können die Beibehaltung eines Systems rechtfertigen, bei dem die Teilnehmer oder Nutzer die Möglichkeit erhalten, zu erklären, dass sie solche Anrufe nicht erhalten möchten. Damit das bestehende Niveau des Schutzes der Privatsphäre nicht gesenkt wird, sollten die Mitgliedstaaten jedoch einzelstaatliche Systeme beibehalten können, bei denen solche an Teilnehmer und Nutzer gerichtete Anrufe nur gestattet werden, wenn diese vorher ihre Einwilligung gegeben haben.

(43) Zur Erleichterung der wirksamen Durchsetzung der Gemeinschaftsvorschriften für unerbetene Nachrichten zum Zweck der Direktwerbung ist es notwendig, die Verwendung falscher Identitäten oder falscher Absenderadressen oder Anrufernummern beim Versand unerbetener Nachrichten zum Zweck der Direktwerbung zu untersagen.

(44) Bei einigen elektronischen Postsystemen können die Teilnehmer Absender und Betreffzeile einer elektronischen Post sehen und darüber hinaus diese Post löschen, ohne die gesamte Post oder deren Anlagen herunterladen zu müssen; dadurch lassen sich die Kosten senken, die möglicherweise mit dem Herunterladen unerwünschter elektronischer Post oder deren Anlagen verbunden sind. Diese Verfahren können in bestimmten Fällen zusätzlich zu den in dieser Richtlinie festgelegten allgemeinen Verpflichtungen von Nutzen bleiben.

(45) Diese Richtlinie berührt nicht die Vorkehrungen der Mitgliedstaaten, mit denen die legitimen Interessen juristischer Personen gegen unerbetene Direktwerbungsnachrichten geschützt werden sollen. Errichten die Mitgliedstaaten ein Register der juristischen Personen – großenteils gewerbetreibende Nutzer –, die derartige Nachrichten nicht erhalten möchten („opt-out Register"), so gilt Artikel 7 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr")[7] in vollem Umfang.

(46) Die Funktion für die Bereitstellung elektronischer Kommunikationsdienste kann in das Netz oder in irgendeinen Teil des Endgeräts des Nutzers, auch in die

[7] ABl. L 178 vom 17.7.2000, S. 1.

Software, eingebaut sein. Der Schutz personenbezogener Daten und der Privatsphäre des Nutzers öffentlich zugänglicher elektronischer Kommunikationsdienste sollte nicht von der Konfiguration der für die Bereitstellung des Dienstes notwendigen Komponenten oder von der Verteilung der erforderlichen Funktionen auf diese Komponenten abhängen. Die Richtlinie 95/46/EG gilt unabhängig von der verwendeten Technologie für alle Formen der Verarbeitung personenbezogener Daten. Bestehen neben allgemeinen Vorschriften für die Komponenten, die für die Bereitstellung elektronischer Kommunikationsdienste notwendig sind, auch noch spezielle Vorschriften für solche Dienste, dann erleichtert dies nicht unbedingt den technologieunabhängigen Schutz personenbezogener Daten und der Privatsphäre. Daher könnten sich Maßnahmen als notwendig erweisen, mit denen die Hersteller bestimmter Arten von Geräten, die für elektronische Kommunikationsdienste benutzt werden, verpflichtet werden, in ihren Produkten von vornherein Sicherheitsfunktionen vorzusehen, die den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und Teilnehmers gewährleisten. Der Erlass solcher Maßnahmen in Einklang mit der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität[8] gewährleistet, dass die aus Gründen des Datenschutzes erforderliche Einführung von technischen Merkmalen elektronischer Kommunikationsgeräte einschließlich der Software harmonisiert wird, damit sie der Verwirklichung des Binnenmarktes nicht entgegensteht.

(47) Das innerstaatliche Recht sollte Rechtsbehelfe für den Fall vorsehen, dass die Rechte der Benutzer und Teilnehmer nicht respektiert werden. Gegen jede – privatem oder öffentlichem Recht unterliegende – Person, die den nach dieser Richtlinie getroffenen einzelstaatlichen Maßnahmen zuwiderhandelt, sollten Sanktionen verhängt werden.

(48) Bei der Anwendung dieser Richtlinie ist es sinnvoll, auf die Erfahrung der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe aus Vertretern der für den Schutz personenbezogener Daten zuständigen Kontrollstellen der Mitgliedstaaten zurückzugreifen.

(49) Zur leichteren Einhaltung der Vorschriften dieser Richtlinie bedarf es einer Sonderregelung für die Datenverarbeitungen, die zum Zeitpunkt des Inkrafttretens der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits durchgeführt werden.

[Ergänzt um die Erwägungsgründe 51–76 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009]

[8] ABl. L 91 vom 7.4.1999, S. 10.

(51) Die Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich ist, um einen gleichwertigen Schutz der Grundrechte und -freiheiten, insbesondere des Rechts auf Privatsphäre und des Rechts auf Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und elektronischer Kommunikationsgeräte und -dienste in der Gemeinschaft zu gewährleisten. Werden gemäß der Richtlinie 1999/5/EG oder dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation[9] Maßnahmen getroffen um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die den Schutz personenbezogener Daten und der Privatsphäre gewährleistet, so sollten solche Maßnahmen den Grundsatz der Technologieneutralität wahren.

(52) Die Entwicklungen bei der Nutzung von IP-Adressen sollten genau verfolgt werden, wobei die Arbeit, die u. a. bereits von der gemäß Artikel 29 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[10] eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten geleistet wurde, und gegebenenfalls entsprechende Vorschläge zu berücksichtigen sind.

(53) Die Verarbeitung von Verkehrsdaten in dem für die Sicherstellung der Netz- und Informationssicherheit strikt notwendigen Ausmaß, d. h. der Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder unrechtmäßige böswillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten oder übermittelten Daten und die Sicherheit damit zusammenhängender Dienste, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind, beeinträchtigen, durch Anbieter von Sicherheitstechnologien und -diensten bei Ausübung ihrer Tätigkeit als Verantwortliche für die Verarbeitung der Daten unterliegt Artikel 7 Buchstabe f der Richtlinie 95/46/EG. Dazu könnten beispielsweise die Verhinderung des unberechtigten Zugangs und der Verbreitung schädlicher Programmcodes oder die Abwehr von Angriffen, die Dienstleistungsverhinderungen bewirken, und von Schädigungen von Computersystemen und Systemen der elektronischen Kommunikation gehören.

(54) Die Marktliberalisierung im Bereich der elektronischen Kommunikationsnetze und -dienste sowie die rasante technische Entwicklung treiben gemeinsam den Wettbewerb und das Wirtschaftswachstum voran, die ihrerseits eine große

[9] ABl. L 36 vom 7.2.1987, S. 31.

[10] ABl. L 281 vom 23.11.1995, S. 31.

Vielfalt von Diensten für die Endnutzer hervorbringen, die über öffentliche elektronische Kommunikationsnetze zugänglich sind. Es ist erforderlich sicherzustellen, dass den Verbrauchern und Nutzern unabhängig von der zur Erbringung eines bestimmten Dienstes verwendeten Technik der gleiche Schutz ihrer Privatsphäre und personenbezogenen Daten gewährt wird.

(55) Im Einklang mit den Zielen des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste sowie den Grundsätzen der Verhältnismäßigkeit und Subsidiarität und im Bemühen um Rechtssicherheit und Effizienz für die europäischen Unternehmen wie auch für die nationalen Regulierungsbehörden stellt die Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) auf öffentliche elektronische Kommunikationsnetze und -dienste ab und findet keine Anwendung auf geschlossene Benutzergruppen oder Unternehmensnetze.

(56) Der technische Fortschritt erlaubt die Entwicklung neuer Anwendungen auf der Grundlage von Datenerfassungs- und Identifizierungsgeräten, bei denen es sich auch um kontaktlos mit Funkfrequenzen arbeitende Geräte handeln könnte. So werden beispielsweise in RFID-Funkfrequenzerkennungsgeräten (Radio Frequency Identification Devices) Funkfrequenzen genutzt, um von eindeutig gekennzeichneten Etiketten Daten abzulesen, die dann über bestehende Kommunikationsnetze weitergeleitet werden können. Die breite Nutzung solcher Technologien kann erhebliche wirtschaftliche und soziale Vorteile bringen und damit einen großen Beitrag zum Binnenmarkt leisten, wenn ihr Einsatz von den Bürgern akzeptiert wird. Um dieses Ziel zu erreichen, muss gewährleistet werden, dass sämtliche Grundrechte des Einzelnen, einschließlich des Rechts auf Privatsphäre und Datenschutz, gewahrt bleiben. Werden solche Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), einschließlich der Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit, zur Anwendung kommen.

(57) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes sollte geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten. Unbeschadet der Richtlinie 95/46/EG sollten derartige Maßnahmen sicherstellen, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten und dass die gespeicherten oder übermittelten personenbezogenen Daten sowie das Netz und die Dienste geschützt sind. Außerdem sollte ein Sicherheitskonzept für die Verarbeitung personenbezogener Daten eingeführt werden, um Systemschwachstellen zu ermitteln, es sollte eine Überwachung erfolgen und es sollten regelmäßig vorbeugende, korrektive und schadensbegrenzende Maßnahmen getroffen werden.

(58) Die zuständigen nationalen Behörden sollten unter anderem durch einen Beitrag zur Sicherstellung eines hohen Niveaus des Schutzes personenbezogener Daten und der Privatsphäre die Interessen der Bürger fördern. Hierzu sollten die zuständigen nationalen Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Mittel verfügen, wie z. B. den Zugang zu vollständigen und verlässlichen Daten über Sicherheitsverletzungen, in deren Folge die personenbezogenen Daten natürlicher Personen preisgegeben wurden. Sie sollten die getroffenen Maßnahmen überwachen und optimale Verfahren unter den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste verbreiten. Die Anbieter sollten daher ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten führen, um eine weitere Analyse und Prüfung durch die zuständigen nationalen Behörden zu ermöglichen.

(59) Das Gemeinschaftsrecht erlegt den für die die Verarbeitung der Daten Verantwortlichen Pflichten im Hinblick auf die Datenverarbeitung auf, die die Umsetzung geeigneter technischer und organisatorischer Schutzmaßnahmen, z. B. gegen Datenverlust, umfassen. Die Pflichten zur Anzeige von Verstößen gemäß der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) enthalten eine Struktur zur Benachrichtigung der zuständigen Behörden und Personen für den Fall, dass personenbezogene Daten trotzdem missbraucht werden. Diese Anzeigepflicht ist auf Sicherheitsverletzungen im Bereich der elektronischen Kommunikation beschränkt. Die Anzeige von Sicherheitsverletzungen spiegelt jedoch ein allgemeines Interesse der Bürger an der Benachrichtigung über Sicherheitsverletzungen wider, die zum Verlust oder zur Preisgabe personenbezogener Daten der Nutzer führen, und über vorhandene oder empfohlene Vorkehrungen, die sie treffen könnten, um mögliche wirtschaftliche Schäden oder soziale Nachteile, die sich aus solchen Sicherheitsverletzungen ergeben, so gering wie möglich zu halten. Das Interesse der Nutzer an der Benachrichtigung ist ersichtlich nicht auf den Bereich der elektronischen Kommunikation beschränkt, so dass ausdrückliche Anzeigepflichten vorrangig in allen Wirtschaftsbereichen auf Gemeinschaftsebene eingeführt werden sollten. Bis zu einer Überprüfung aller einschlägigen gemeinschaftlichen Rechtsvorschriften auf diesem Gebiet durch die Kommission sollte die Kommission in Abstimmung mit dem Europäischen Datenschutzbeauftragten unverzüglich geeignete Maßnahmen ergreifen, um die gemeinschaftsweite Anwendung der in der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) enthaltenen Leitlinien für die Anzeigepflicht bei Verstößen gegen die Datensicherheit, ungeachtet des Sektors oder der Art der betreffenden Daten, zu fördern.

(60) Die zuständigen nationalen Behörden sollten die getroffenen Maßnahmen überwachen und optimale Verfahren unter den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste verbreiten.

(61) Eine Verletzung des Schutzes personenbezogener Daten kann erhebliche wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs für den Teilnehmer oder die betroffene Person nach sich ziehen, wenn nicht rechtzeitig und angemessen darauf reagiert wird. Deshalb sollte der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste unmittelbar nach Bekanntwerden der Verletzung die zuständige nationale Behörde von der Verletzung benachrichtigen. Teilnehmer oder natürliche Personen, für die eine solche Verletzung des Datenschutzes und der Privatsphäre nachteilige Auswirkungen haben kann, sollten unverzüglich benachrichtigt werden, damit sie die erforderlichen Schutzvorkehrungen treffen können. Die Auswirkungen einer Verletzung werden für den Datenschutz oder die Privatsphäre des Teilnehmers oder der natürlichen Person als nachteilig erachtet, wenn sie z. B. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschaden in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in der Gemeinschaft zur Folge haben. Die Benachrichtigung sollte Informationen über die vom Betreiber nach der Verletzung ergriffenen Maßnahmen sowie Empfehlungen für die betroffenen Nutzer oder Personen enthalten.

(62) Bei der Durchführung von Maßnahmen zur Umsetzung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) sollten die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit der genannten Richtlinie auslegen, sondern auch gewährleisten, dass sie sich nicht auf eine Auslegung der Richtlinie stützen, die im Widerspruch zu anderen Grundrechten oder allgemeinen Grundsätzen des Gemeinschaftsrechts wie dem Grundsatz der Verhältnismäßigkeit stehen würde.

(63) Der Erlass technischer Durchführungsmaßnahmen zu den Voraussetzungen, zum Format und zu den Verfahren für die Informations- und Anzeigepflichten sollte vorgesehen werden, um ein angemessenes Niveau des Schutzes der Privatsphäre und der Sicherheit der übermittelten und verarbeiteten personenbezogenen Daten im Zusammenhang mit der Nutzung elektronischer Kommunikationsnetze innerhalb des Binnenmarktes zu gewährleisten.

(64) Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, z. B. ob personenbezogene Daten durch geeignete technische Schutzmaßnahmen geschützt waren, die die Wahrscheinlichkeit des Identitätsbetrugs oder anderer Formen des Missbrauchs effektiv verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände der Verletzung durch ein frühzeitiges Bekanntwerden in unnötiger Weise behindert würde.

(65) Computerprogramme, die heimlich zugunsten Dritter das Verhalten des Nutzers überwachen oder die Funktionsweise seines Endgerätes beeinträchtigen („Spähsoftware“) sind genauso wie Viren eine ernste Bedrohung für die Privatsphäre des Nutzers. Ein hoher und einheitlicher Schutz der Privatsphäre der Nutzer muss unabhängig davon gewährleistet werden, ob unerwünschte Spähprogramme oder Viren versehentlich über elektronische Kommunikationsnetze heruntergeladen werden oder aber versteckt in anderer Software, die auf externen Speichermedien wie CD, CD-ROM oder USB-Speicherstift verbreitet wird, ausgeliefert und installiert werden. Die Mitgliedstaaten sollten zur Bereitstellung von Information an Endnutzer über mögliche Schutzvorkehrungen auffordern und die Endnutzer auffordern, die notwendigen Maßnahmen zu ergreifen, um ihre Endgeräte vor Viren und Spähsoftware zu schützen.

(66) Es ist denkbar, dass Dritte aus einer Reihe von Gründen Informationen auf der Endeinrichtung eines Nutzers speichern oder auf bereits gespeicherte Informationen zugreifen wollen, die von legitimen Gründen (wie manchen Arten von Cookies) bis hin zum unberechtigten Eindringen in die Privatsphäre (z. B. über Spähsoftware oder Viren) reichen. Daher ist es von größter Wichtigkeit, dass den Nutzern eine klare und verständliche Information bereitgestellt wird, wenn sie irgendeine Tätigkeit ausführen, die zu einer solchen Speicherung oder einem solchen Zugriff führen könnte. Die Methoden der Information und die Einräumung des Rechts, diese abzulehnen, sollten so benutzerfreundlich wie möglich gestaltet werden. Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen. Wenn es technisch durchführbar und wirksam ist, kann die Einwilligung des Nutzers zur Verarbeitung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden. Die Umsetzung dieser Voraussetzungen sollte durch die Stärkung der Befugnisse der zuständigen nationalen Behörden wirksamer gestaltet werden.

(67) Vorkehrungen, die getroffen werden, um die Teilnehmer gegen ein Eindringen in ihre Privatsphäre durch unerbetene Direktwerbenachrichten per elektronischer Post zu schützen, sollten auch für SMS- und MMS-Nachrichten sowie für ähnliche Anwendungen gelten.

(68) Die Anbieter elektronischer Kommunikationsdienste tätigen zur Bekämpfung unerbetener Werbung („Spam“) erhebliche Investitionen. Außerdem sind sie aufgrund der erforderlichen Sachkenntnis und Ressourcen besser als die Endnutzer in der Lage, Spam-Versender festzustellen und zu identifizieren. Die Betreiber von E-Mail-Diensten und andere Diensteanbieter sollten daher die Möglichkeit haben, rechtlich gegen Spam-Versender vorzugehen, um auf diese Weise die

Interessen ihrer Kunden als Teil ihrer eigenen rechtmäßigen Geschäftsinteressen zu schützen.

(69) Angesichts der Notwendigkeit, in der Gemeinschaft einen angemessenen Schutz der Privatsphäre und personenbezogener Daten bei deren Übermittlung und Verarbeitung im Zusammenhang mit der Nutzung elektronischer Kommunikationsnetze zu gewährleisten, müssen als hinreichender Anreiz für die Einhaltung der Schutzbestimmungen wirksame Um- und Durchsetzungsbefugnisse geschaffen werden. Die zuständigen nationalen Behörden und gegebenenfalls andere relevante nationale Stellen sollten mit ausreichenden Befugnissen und Ressourcen ausgestattet werden, um Verstöße effektiv untersuchen zu können, einschließlich der Befugnis, alle benötigten Informationen einzuholen, damit sie Beschwerden nachgehen und bei Verstößen Sanktionen verhängen können.

(70) Die Um- und Durchsetzung dieser Richtlinie erfordert häufig eine Zusammenarbeit zwischen den nationalen Regulierungsbehörden zweier oder mehrerer Mitgliedstaaten, wie etwa bei der Bekämpfung von grenzüberschreitender unerbetener Werbung („Spam“) und Spähsoftware. Damit in solchen Fällen eine reibungslose und schnelle Zusammenarbeit gewährleistet ist, sollten durch die zuständigen nationalen Behörden Verfahren festgelegt werden und der Prüfung durch die Kommission unterliegen, die beispielsweise die Menge und das Format der zwischen Behörden ausgetauschten Informationen oder die einzuhaltenden Fristen betreffen. Diese Verfahren werden auch die Harmonisierung der daraus resultierenden Pflichten der Marktteilnehmer ermöglichen und damit zur Schaffung gleicher Wettbewerbsbedingungen in der Gemeinschaft beitragen.

(71) Die grenzübergreifende Zusammenarbeit und Rechtsdurchsetzung sollte im Rahmen der bestehenden Verfahren, die beispielsweise in der Verordnung (EG) Nr. 2006/2004 (Verordnung über die Zusammenarbeit im Verbraucherschutz)[11] festgelegt sind, durch eine Änderung der genannten Verordnung verstärkt werden.

(72) Die zur Durchführung der Richtlinien 2002/22/EG (Universaldienstrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) erforderlichen Maßnahmen sollten gemäß dem Beschluss 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse[12] erlassen werden.

(73) Insbesondere sollte die Kommission die Befugnis erhalten, Durchführungsmaßnahmen in Bezug auf die effektive Einführung der „112“-Dienste zu treffen

[11] ABl. L 364 vom 9.12.2004, S. 1.

[12] ABl. L 184 vom 17.7.1999, S. 23.

sowie die Anhänge an den technischen Fortschritt oder an die Veränderungen der Marktnachfrage anzupassen. Sie sollte auch die Befugnis erhalten, Durchführungsmaßnahmen in Bezug auf Informations- und Anzeigepflichten und die Sicherheit der Verarbeitung zu erlassen. Da es sich hierbei um Maßnahmen von allgemeiner Tragweite handelt, die eine Änderung nicht wesentlicher Bestimmungen der Richtlinien 2002/22/EG (Universaldienstrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) durch Ergänzung um neue nicht wesentliche Bestimmungen bewirken, sind diese Maßnahmen nach dem Regelungsverfahren mit Kontrolle des Artikels 5a des Beschlusses 1999/468/EG zu erlassen. Da die Durchführung des Regelungsverfahrens mit Kontrolle innerhalb der normalen Fristen in bestimmten Ausnahmesituationen einem rechtzeitigen Erlass von Durchführungsmaßnahmen entgegenstehen könnte, sollten das Europäische Parlament, der Rat und die Kommission rasch handeln, um sicherzustellen, dass diese Maßnahmen rechtzeitig erlassen werden.

(74) Bei der Annahme von Durchführungsmaßnahmen im Zusammenhang mit der Sicherheit der Verarbeitung sollte die Kommission alle zuständigen europäischen Behörden und Organisationen (die Europäische Agentur für Netz- und Informationssicherheit (ENISA), den Europäischen Datenschutzbeauftragten und die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten) sowie alle anderen relevanten Interessengruppen mit einbeziehen, um sich insbesondere über die besten verfügbaren technischen und wirtschaftlichen Methoden für eine Verbesserung der Durchführung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) zu informieren.

(75) Die Richtlinien 2002/22/EG (Universaldienstrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) sollten daher entsprechend geändert werden.

(76) Nach Nummer 34 der Interinstitutionellen Vereinbarung über bessere Rechtsetzung[13] sind die Mitgliedstaaten aufgefordert, für ihre eigenen Zwecke und im Interesse der Gemeinschaft eigene Tabellen aufzustellen, aus denen im Rahmen des Möglichen die Entsprechungen zwischen den Richtlinien 2002/22/EG (Universaldienstrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und den Umsetzungsmaßnahmen zu entnehmen sind, und diese zu veröffentlichen –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

[13] ABl. C 321 vom 31.12.2003, S. 1.

Artikel 1

Geltungsbereich und Zielsetzung

(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Artikel 2

Begriffsbestimmungen

Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie 95/46/EG und der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie“)[14] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) „Nutzer“ eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

[14] ABl. L 108 vom 24.4.2002, S. 33.

b) „Verkehrsdaten“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

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

d) „Nachricht“ jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

e) „Einwilligung“ eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG;

f) „Dienst mit Zusatznutzen“ jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

g) „elektronische Post“ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

h) „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden.

Artikel 3

Betroffene Dienste

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunika-

tionsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.

Artikel 4

Sicherheit der Verarbeitung

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(1a) Unbeschadet der Richtlinie 95/46/EG ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen:

– Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten,

– Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe und

– Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Die zuständigen nationalen Behörden haben die Möglichkeit, die von den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste getroffenen Maßnahmen zu prüfen und Empfehlungen zu bewährten Verfahren im Zusammenhang mit dem mit Hilfe dieser Maßnahmen zu erreichenden Sicherheitsniveau zu abzugeben.

(2) Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.

(3) Im Fall einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste unverzüglich die zuständige nationale Behörde von der Verletzung.

Ist anzunehmen, dass durch die Verletzung personenbezogener Daten die personenbezogenen Daten, oder Teilnehmer oder Personen in ihrer Privatsphäre, beeinträchtigt werden, so benachrichtigt der Betreiber auch den Teilnehmer bzw. die Person unverzüglich von der Verletzung.

Der Anbieter braucht die betroffenen Teilnehmer oder Personen nicht von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn er zur Zufriedenheit der zuständigen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Diese technischen Schutzmaßnahmen verschlüsseln die Daten für alle Personen, die nicht befugt sind, Zugang zu den Daten zu haben.

Unbeschadet der Pflicht des Betreibers, den betroffenen Teilnehmer und die Person zu benachrichtigen, kann die zuständige nationale Behörde, wenn der Betreiber den Teilnehmer bzw. die Person noch nicht über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, diesen nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung zur Benachrichtigung auffordern.

In der Benachrichtigung des Teilnehmers bzw. der Person werden mindestens die Art der Verletzung des Schutzes personenbezogener Daten und die Kontaktstellen, bei denen weitere Informationen erhältlich sind, genannt und Maßnahmen zur Begrenzung der möglichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten empfohlen. In der Benachrichtigung der zuständigen nationalen Behörde werden zusätzlich die Folgen der Verletzung des Schutzes personenbezogener Daten und die vom Betreiber nach der Verletzung vorgeschlagenen oder ergriffenen Maßnahmen dargelegt.

(4) Vorbehaltlich technischer Durchführungsmaßnahmen nach Absatz 5 können die zuständigen nationalen Behörden Leitlinien annehmen und gegebenenfalls Anweisungen erteilen bezüglich der Umstände, unter denen die Benachrichtigung seitens der Betreiber über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist, sowie bezüglich des Formates und der Verfahrensweise für die Benachrichtigung. Sie müssen auch in der Lage sein zu überwachen, ob die Betreiber ihre Pflichten zur Benachrichtigung nach diesem Absatz erfüllt haben, und verhängen, falls dies nicht der Fall ist, geeignete Sanktionen.

Die Betreiber führen ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten, das Angaben zu den Umständen der Verletzungen, zu deren Aus-

wirkungen und zu den ergriffenen Abhilfemaßnahmen enthält, wobei diese Angaben ausreichend sein müssen, um den zuständigen nationalen Behörden die Prüfung der Einhaltung der Bestimmungen des Absatzes 3 zu ermöglichen. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen.

(5) Zur Gewährleistung einer einheitlichen Anwendung der in den Absätzen 2, 3 und 4 vorgesehenen Maßnahmen kann die Kommission nach Anhörung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten und des Europäischen Datenschutzbeauftragten technische Durchführungsmaßnahmen in Bezug auf Umstände, Form und Verfahren der in diesem Artikel vorgeschriebenen Informationen und Benachrichtigungen erlassen. Beim Erlass dieser Maßnahmen bezieht die Kommission alle relevanten Interessengruppen mit ein, um sich insbesondere über die besten verfügbaren technischen und wirtschaftlichen Mittel zur Durchführung dieses Artikels zu informieren.

Diese Maßnahmen zur Änderung nicht wesentlicher Bestimmungen dieser Richtlinie durch Ergänzung werden nach dem in Artikel 14a Absatz 2 genannten Regelungsverfahren mit Kontrolle erlassen.

Artikel 5

Vertraulichkeit der Kommunikation

(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Nachrichten und der damit verbundenen Verkehrsdaten, wenn dies im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht geschieht.

(3) Die Mitgliedstaaten stellen sicher, 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. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Artikel 6

Verkehrsdaten

(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

(4) Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht; bei einer Verarbeitung für die in Absatz 3 genannten Zwecke muss diese Mitteilung erfolgen, bevor um Einwilligung ersucht wird.

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommu-

nikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

(6) Die Absätze 1, 2, 3 und 5 gelten unbeschadet der Möglichkeit der zuständigen Gremien, in Einklang mit den geltenden Rechtsvorschriften für die Beilegung von Streitigkeiten, insbesondere Zusammenschaltungs- oder Abrechnungsstreitigkeiten, von Verkehrsdaten Kenntnis zu erhalten.

Artikel 7

Einzelgebührennachweis

(1) Die Teilnehmer haben das Recht, Rechnungen ohne Einzelgebührennachweis zu erhalten.

(2) Die Mitgliedstaaten wenden innerstaatliche Vorschriften an, um das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Nutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen, indem sie beispielsweise sicherstellen, dass diesen Nutzern und Teilnehmern genügend andere, den Schutz der Privatsphäre fördernde Methoden für die Kommunikation oder Zahlungen zur Verfügung stehen.

Artikel 8

Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

(1) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem anrufenden Nutzer die Möglichkeit geben, die Rufnummernanzeige für jeden Anruf einzeln auf einfache Weise und gebührenfrei zu verhindern. Dem anrufenden Teilnehmer muss diese Möglichkeit anschlussbezogen zur Verfügung stehen.

(2) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige der Rufnummer eingehender Anrufe auf einfache Weise und für jede vertretbare Nutzung dieser Funktion gebührenfrei zu verhindern.

(3) Wird die Anzeige der Rufnummer des Anrufers angeboten und wird die Rufnummer vor der Herstellung der Verbindung angezeigt, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, eingehende Anrufe,

bei denen die Rufnummernanzeige durch den anrufenden Nutzer oder Teilnehmer verhindert wurde, auf einfache Weise und gebührenfrei abzuweisen.

(4) Wird die Anzeige der Rufnummer des Angerufenen angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige seiner Rufnummer beim anrufenden Nutzer auf einfache Weise und gebührenfrei zu verhindern.

(5) Absatz 1 gilt auch für aus der Gemeinschaft kommende Anrufe in Drittländern. Die Absätze 2, 3 und 4 gelten auch für aus Drittländern kommende Anrufe.

(6) Wird die Anzeige der Rufnummer des Anrufers und/oder des Angerufenen angeboten, so stellen die Mitgliedstaaten sicher, dass die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste die Öffentlichkeit hierüber und über die in den Absätzen 1, 2, 3 und 4 beschriebenen Möglichkeiten unterrichten.

Artikel 9

Andere Standortdaten als Verkehrsdaten

(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, dann müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen er-

forderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

Artikel 10

Ausnahmen

Die Mitgliedstaaten stellen sicher, dass es transparente Verfahren gibt, nach denen der Betreiber eines öffentlichen Kommunikationsnetzes und/oder eines öffentlich zugänglichen elektronischen Kommunikationsdienstes

a) die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufheben kann, wenn ein Teilnehmer beantragt hat, dass böswillige oder belästigende Anrufe zurückverfolgt werden; in diesem Fall werden nach innerstaatlichem Recht die Daten mit der Rufnummer des anrufenden Teilnehmers vom Betreiber des öffentlichen Kommunikationsnetzes und/oder des öffentlich zugänglichen elektronischen Kommunikationsdienstes gespeichert und zur Verfügung gestellt;

b) die Unterdrückung der Anzeige der Rufnummer des Anrufers aufheben und Standortdaten trotz der vorübergehenden Untersagung oder fehlenden Einwilligung durch den Teilnehmer oder Nutzer verarbeiten kann, und zwar anschlussbezogen für Einrichtungen, die Notrufe bearbeiten und dafür von einem Mitgliedstaat anerkannt sind, einschließlich Strafverfolgungsbehörden, Ambulanzdiensten und Feuerwehren, zum Zwecke der Beantwortung dieser Anrufe.

Artikel 11

Automatische Anrufweiterschaltung

Die Mitgliedstaaten stellen sicher, dass jeder Teilnehmer die Möglichkeit hat, auf einfache Weise und gebührenfrei die von einer dritten Partei veranlasste automatische Anrufweiterschaltung zum Endgerät des Teilnehmers abzustellen.

Artikel 12

Teilnehmerverzeichnisse

(1) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer gebührenfrei und vor Aufnahme in das Teilnehmerverzeichnis über den Zweck bzw. die Zwecke von gedruckten oder elektronischen, der Öffentlichkeit unmittelbar oder über Aus-

kunftsdienste zugänglichen Teilnehmerverzeichnissen, in die ihre personenbezogenen Daten aufgenommen werden können, sowie über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen informiert werden.

(2) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer Gelegenheit erhalten festzulegen, ob ihre personenbezogenen Daten – und ggf. welche – in ein öffentliches Verzeichnis aufgenommen werden, sofern diese Daten für den vom Anbieter des Verzeichnisses angegebenen Zweck relevant sind, und diese Daten prüfen, korrigieren oder löschen dürfen. Für die Nicht-Aufnahme in ein der Öffentlichkeit zugängliches Teilnehmerverzeichnis oder die Prüfung, Berichtigung oder Streichung personenbezogener Daten aus einem solchen Verzeichnis werden keine Gebühren erhoben.

(3) Die Mitgliedstaaten können verlangen, dass eine zusätzliche Einwilligung der Teilnehmer eingeholt wird, wenn ein öffentliches Verzeichnis anderen Zwecken als der Suche nach Einzelheiten betreffend die Kommunikation mit Personen anhand ihres Namens und gegebenenfalls eines Mindestbestands an anderen Kennzeichen dient.

(4) Die Absätze 1 und 2 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten tragen im Rahmen des Gemeinschaftsrechts und der geltenden einzelstaatlichen Rechtsvorschriften außerdem dafür Sorge, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf ihre Aufnahme in öffentliche Verzeichnisse ausreichend geschützt werden.

Artikel 13

Unerbetene Nachrichten

(1) Die Verwendung von automatischen Anruf- und Kommunikationssystemen ohne menschlichen Eingriff (automatische Anrufmaschinen), Faxgeräten oder elektronischer Post für die Zwecke der Direktwerbung darf nur bei vorheriger Einwilligung der Teilnehmer oder Nutzer gestattet werden.

(2) Ungeachtet des Absatzes 1 kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen zum Zeitpunkt ihrer Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat.

(3) Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um sicherzustellen, dass außer in den in den Absätzen 1 und 2 genannten Fällen unerbetene Nachrichten zum Zwecke der Direktwerbung, die entweder ohne die Einwilligung der betreffenden Teilnehmer oder Nutzer erfolgen oder an Teilnehmer oder Nutzer gerichtet sind, die keine solchen Nachrichten erhalten möchten, nicht gestattet sind; welche dieser Optionen gewählt wird, wird im innerstaatlichen Recht geregelt, wobei berücksichtigt wird, dass beide Optionen für den Teilnehmer oder Nutzer gebührenfrei sein müssen.

(4) Auf jeden Fall verboten ist die Praxis des Versendens elektronischer Nachrichten zu Zwecken der Direktwerbung, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, bei der gegen Artikel 6 der Richtlinie 2000/31/EG verstoßen wird oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, oder in denen der Empfänger aufgefordert wird, Websites zu besuchen, die gegen den genannten Artikel verstoßen.

(5) Die Absätze 1 und 3 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten stellen im Rahmen des Gemeinschaftsrechts und der geltenden nationalen Rechtsvorschriften außerdem sicher, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf unerbetene Nachrichten ausreichend geschützt werden.

(6) Unbeschadet etwaiger Verwaltungsvorschriften, die unter anderem gemäß Artikel 15a Absatz 2 erlassen werden können, stellen die Mitgliedstaaten sicher, dass natürliche oder juristische Personen, die durch Verstöße gegen die aufgrund dieses Artikels erlassenen nationalen Vorschriften beeinträchtigt werden und ein berechtigtes Interesse an der Einstellung oder dem Verbot solcher Verstöße haben, einschließlich der Anbieter elektronischer Kommunikationsdienste, die ihre berechtigten Geschäftsinteressen schützen wollen, gegen solche Verstöße gerichtlich vorgehen können. Die Mitgliedstaaten können auch spezifische Vorschriften über Sanktionen festlegen, die gegen Betreiber elektronischer Kommunikationsdienste zu verhängen sind, die durch Fahrlässigkeit zu Verstößen gegen die aufgrund dieses Artikels erlassenen nationalen Vorschriften beitragen.

Artikel 14

Technische Merkmale und Normung

(1) Bei der Durchführung der Bestimmungen dieser Richtlinie stellen die Mitgliedstaaten vorbehaltlich der Absätze 2 und 3 sicher, dass keine zwingenden Anforderungen in Bezug auf spezifische technische Merkmale für Endgeräte oder

sonstige elektronische Kommunikationsgeräte gestellt werden, die deren Inverkehrbringen und freien Vertrieb in und zwischen den Mitgliedstaaten behindern können.

(2) Soweit die Bestimmungen dieser Richtlinie nur mit Hilfe spezifischer technischer Merkmale elektronischer Kommunikationsnetze durchgeführt werden können, unterrichten die Mitgliedstaaten die Kommission darüber gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft[15].

(3) Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation[16] Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist.

Artikel 14a

Ausschussverfahren

(1) Die Kommission wird von dem durch Artikel 22 der Richtlinie 2002/21/EG (Rahmenrichtlinie) eingesetzten Kommunikationsausschuss unterstützt.

(2) Wird auf diesen Absatz Bezug genommen, so gelten Artikel 5a Absätze 1 bis 4 und Artikel 7 des Beschlusses 1999/468/EG unter Beachtung von dessen Artikel 8.

(3) Wird auf diesen Absatz Bezug genommen, so gelten Artikel 5a Absätze 1, 2, 4 und 6 und Artikel 7 des Beschlusses 1999/468/EG unter Beachtung von dessen Artikel 8.

Artikel 15

Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Arti-

[15] ABl. L 204 vom 21.7.1998, S. 37. Richtlinie geändert durch die Richtlinie 98/48/EG (ABl. L 217 vom 5.8.1998, S. 18).

[16] ABl. L 36 vom 7.2.1987. Beschluss zuletzt geändert durch die Beitrittsakte von 1994.

kel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(1b) Die Anbieter richten nach den gemäß Absatz 1 eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer ein. Sie stellen den zuständigen nationalen Behörden auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihrer Antworten zur Verfügung.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

Artikel 15a

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten legen fest, welche Sanktionen, gegebenenfalls einschließlich strafrechtlicher Sanktionen, bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung dieser Richtlinie zu verhängen sind, und treffen die zu deren Durchsetzung erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein und können für den gesamten Zeitraum einer Verletzung angewendet werden, auch wenn die Verletzung in der Folge abgestellt wurde. Die Mitgliedstaaten teilen der Kommission diese Vorschriften bis zum 25. Mai 2011 mit und melden ihr unverzüglich etwaige spätere Änderungen, die diese Vorschriften betreffen.

(2) Unbeschadet etwaiger gerichtlicher Rechtsbehelfe stellen die Mitgliedstaaten sicher, dass die zuständige nationale Behörde und gegebenenfalls andere nationale Stellen befugt sind, die Einstellung der in Absatz 1 genannten Verstöße anzuordnen.

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen nationalen Regulierungsbehörden und gegebenenfalls andere nationale Stellen über die erforderlichen Untersuchungsbefugnisse und Mittel verfügen, einschließlich der Befugnis, sämtliche zweckdienliche Informationen zu erlangen, die sie benötigen, um die Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften zu überwachen und durchzusetzen.

(4) Zur Gewährleistung einer wirksamen grenzübergreifenden Koordinierung der Durchsetzung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften und zur Schaffung harmonisierter Bedingungen für die Erbringung von Diensten, mit denen ein grenzüberschreitender Datenfluss verbunden ist, können die zuständigen nationalen Regulierungsbehörden Maßnahmen erlassen.

Die nationalen Regulierungsbehörden übermitteln der Kommission rechtzeitig vor dem Erlass solcher Maßnahmen eine Zusammenfassung der Gründe für ein Tätigwerden, der geplanten Maßnahmen und der vorgeschlagenen Vorgehensweise. Die Kommission kann hierzu nach Anhörung der ENISA und der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten Kommentare oder Empfehlungen abgeben, insbesondere um sicherzustellen, dass die vorgesehenen Maßnahmen ein ordnungsmäßiges Funktionieren des Binnenmarktes nicht beeinträchtigen. Die nationalen Regulierungsbehörden tragen den Kommentaren oder Empfehlungen der Kommission weitestgehend Rechnung, wenn sie die Maßnahmen beschließen.

Artikel 16

Übergangsbestimmungen

(1) Artikel 12 gilt nicht für Ausgaben von Teilnehmerverzeichnissen, die vor dem Inkrafttreten der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits in gedruckter oder in netzunabhängiger elektronischer Form produziert oder in Verkehr gebracht wurden.

(2) Sind die personenbezogenen Daten von Teilnehmern von Festnetz- oder Mobil-Sprachtelefondiensten in ein öffentliches Teilnehmerverzeichnis gemäß der Richtlinie 95/46/EG und gemäß Artikel 11 der Richtlinie 97/66/EG aufgenommen worden, bevor die nach der vorliegenden Richtlinie erlassenen inner-

staatlichen Rechtsvorschriften in Kraft treten, so können die personenbezogenen Daten dieser Teilnehmer in der gedruckten oder elektronischen Fassung, einschließlich Fassungen mit Umkehrsuchfunktionen, in diesem öffentlichen Verzeichnis verbleiben, sofern die Teilnehmer nach Erhalt vollständiger Informationen über die Zwecke und Möglichkeiten gemäß Artikel 12 nicht etwas anderes wünschen.

Artikel 17[17]

Umsetzung

(1) Die Mitgliedstaaten setzen vor dem 31. Oktober 2003 die Rechtsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Rechts-Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen, sowie aller späteren Änderungen dieser Vorschriften.

Artikel 18

Überprüfung

Die Kommission unterbreitet dem Europäischen Parlament und dem Rat spätestens drei Jahre nach dem in Artikel 17 Absatz 1 genannten Zeitpunkt einen Bericht über die Durchführung dieser Richtlinie und ihre Auswirkungen auf die Wirtschaftsteilnehmer und Verbraucher, insbesondere in Bezug auf die Bestimmungen über unerbetene Nachrichten, unter Berücksichtigung des internationalen Umfelds. Hierzu kann die Kommission von den Mitgliedstaaten Informatio-

---

[17] Artikel 4 der Richtlinie 2009/136/EG betr. geänderte bzw. eingefügte Art. 1 Abs. 1, Art. 2, 3, Art 4 Abs. 1a und 3–5, Art. 5 Abs. 3, Art. 6 Abs. 3, Art. 13, 14a, Art. 15 Abs. 1b und Art. 15a:
„Umsetzung
(1) Die Mitgliedstaaten erlassen und veröffentlichen bis zum 25. Mai 2011 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit.
Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.
(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen."

nen einholen, die ohne unangemessene Verzögerung zu liefern sind. Gegebenenfalls unterbreitet die Kommission unter Berücksichtigung der Ergebnisse des genannten Berichts, etwaiger Änderungen in dem betreffenden Sektor sowie etwaiger weiterer Vorschläge, die sie zur Verbesserung der Wirksamkeit dieser Richtlinie für erforderlich hält, Vorschläge zur Änderung dieser Richtlinie.

Artikel 19

Aufhebung

Die Richtlinie 97/66/EG wird mit Wirkung ab dem in Artikel 17 Absatz 1 genannten Zeitpunkt aufgehoben.

Verweisungen auf die aufgehobene Richtlinie gelten als Verweisungen auf die vorliegende Richtlinie.

Artikel 20

Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft.

Artikel 21

Adressaten

Diese Richtlinie ist an alle Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 12. Juli 2002.

Im Namen des Europäischen Parlaments	Im Namen des Rates
Der Präsident	*Der Präsident*
P. COX	*T. PEDERSEN*

2. Europäische Kommission

Beschluss 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates

(Bekannt gegeben unter Aktenzeichen K[2010] 593)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], insbesondere auf Artikel 26 Absatz 4,

nach Anhörung des Europäischen Datenschutzbeauftragten,

in Erwägung nachstehender Gründe:

(1) Nach der Richtlinie 95/46/EG müssen die Mitgliedstaaten dafür Sorge tragen, dass die Übermittlung personenbezogener Daten in ein Drittland nur dann erfolgen kann, wenn das betreffende Drittland ein angemessenes Schutzniveau gewährleistet und vor der Übermittlung die aufgrund der anderen Bestimmungen der Richtlinie erlassenen Vorschriften der Mitgliedstaaten beachtet werden.

(2) Artikel 26 Absatz 2 der Richtlinie 95/46/EG gestattet jedoch den Mitgliedstaaten, die Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten in Drittländer, die kein angemessenes Datenschutzniveau gewährleisten, zu genehmigen, sofern bestimmte Garantien vorliegen. Solche Garantien können sich insbesondere aus einschlägigen Vertragsklauseln ergeben.

(3) Nach der Richtlinie 95/46/EG ist das Datenschutzniveau unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenübermittlung oder einer Reihe von Datenübermittlungen eine Rolle spielen. Die gemäß dieser Richtlinie eingesetzte Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten hat Leitlinien für die Erstellung solcher Beurteilungen veröffentlicht.

[1] ABl. L 281 vom 23.11.1995, S. 31.

(4) Standardvertragsklauseln sollten sich nur auf den Datenschutz beziehen. Dem Datenexporteur und dem Datenimporteur ist es daher freigestellt, weitere geschäftsbezogene Klauseln aufzunehmen, die sie für vertragsrelevant halten, sofern diese nicht im Widerspruch zu den Standardvertragsklauseln stehen.

(5) Dieser Beschluss sollte die nationalen Genehmigungen unberührt lassen, die von den Mitgliedstaaten nach ihren eigenen Rechtsvorschriften zur Umsetzung von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilt werden können. Dieser Beschluss sollte lediglich die Wirkung haben, dass die Mitgliedstaaten die darin aufgeführten Standardvertragsklauseln als angemessene Garantien anerkennen müssen; sie sollte daher andere Vertragsklauseln unberührt lassen.

(6) Die Entscheidung 2002/16/EG der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG[2] soll einem in der Europäischen Union niedergelassenen für die Datenverarbeitung Verantwortlichen die Übermittlung personenbezogener Daten an einen Auftragsverarbeiter, der in einem Drittland niedergelassen ist, das kein angemessenes Datenschutzniveau gewährleistet, erleichtern.

(7) Seit Erlass der Entscheidung 2002/16/EG wurden viele Erfahrungen gesammelt. Der Bericht über die Durchführung der Entscheidungen über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer[3] zeigt darüber hinaus, dass ein wachsendes Interesse an solchen Standardvertragsklauseln für die internationale Übermittlung personenbezogener Daten in Drittländer, die kein angemessenes Datenschutzniveau gewährleisten, besteht. Zudem wurden Vorschläge zur Aktualisierung der in der Entscheidung 2002/16/EG aufgeführten Standardvertragsklauseln gemacht, um der rasch expandierenden Datenverarbeitungstätigkeit weltweit Rechnung zu tragen und Aspekte zu erfassen, die in der Entscheidung bisher nicht geregelt worden sind[4].

(8) Dieser Beschluss sollte sich darauf beschränken festzulegen, dass die aufgeführten Vertragsklauseln von einem für die Datenverarbeitung Verantwortlichen, der in der Europäischen Union niedergelassen ist, verwendet werden können, um angemessene Garantien im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an einen Auftragsverarbeiter, der in einem Drittland niedergelassen ist, zu gewährleisten.

---

2 ABl. L 6 vom 10.1.2002, S. 52.

3 SEK(2006) 95 vom 20.1.2006.

4 Vonseiten der Internationalen Handelskammer (ICC), des Japan Business Council in Europe (JBCE), des EU-Ausschusses der Amerikanischen Handelskammer in Belgien (Amcham) und der Federation of European Direct Marketing Associations (FEDMA).

(9) Dieser Beschluss sollte daher nicht für die Übermittlung personenbezogener Daten durch für die Verarbeitung Verantwortliche, die in der Europäischen Union niedergelassen sind, an für die Verarbeitung Verantwortliche außerhalb der Europäischen Union gelten, die in den Anwendungsbereich der Kommissionsentscheidung 2001/497/EG vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG fallen[5].

(10) Mit diesem Beschluss sollte die Verpflichtung gemäß Artikel 17 Absatz 3 der Richtlinie 95/46/EG umgesetzt werden; sie sollte den Inhalt eines solchen Vertrags beziehungsweise Rechtsakts unberührt lassen. Einige der Standardvertragsklauseln, vor allem diejenigen bezüglich der Pflichten des Datenexporteurs, sollten jedoch übernommen werden, um die Bestimmungen zu verdeutlichen, die in einen Vertrag zwischen einem für die Datenverarbeitung Verantwortlichen und einem Auftragsverarbeiter aufgenommen werden können.

(11) Die Kontrollstellen der Mitgliedstaaten spielen eine Schlüsselrolle in diesem Vertragsmechanismus, weil sie sicherstellen, dass personenbezogene Daten nach der Übermittlung angemessen geschützt werden. In Ausnahmefällen, in denen Datenexporteure es ablehnen oder nicht in der Lage sind, dem Datenimporteur angemessene Anweisungen zu geben, und in denen eine hohe Wahrscheinlichkeit besteht, dass den betroffenen Personen ein schwerwiegender Schaden entsteht, sollten die Standardvertragsklauseln es den Kontrollstellen ermöglichen, Datenimporteure und Unterauftragsverarbeiter einer Prüfung zu unterziehen und gegebenenfalls Entscheidungen zu treffen, denen Datenimporteure und Unterauftragsverarbeiter Folge leisten müssen. Die Kontrollstellen sollten befugt sein, eine Datenübermittlung oder eine Reihe von Datenübermittlungen auf der Grundlage der Standardvertragsklauseln zu untersagen oder zurückzuhalten; dies gilt für jene Ausnahmefälle, für die feststeht, dass sich eine Übermittlung auf Vertragsbasis wahrscheinlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die den betroffenen Personen angemessenen Schutz bieten sollen.

(12) Standardvertragsklauseln sollten die technischen und organisatorischen Sicherheitsmaßnahmen vorsehen, die Datenverarbeiter in einem Drittland ohne angemessenes Schutzniveau anwenden sollten, um einen Schutz zu gewährleisten, der den durch die Verarbeitung entstehenden Risiken und der Art der zu schützenden Daten angemessen ist. Die Parteien sollten diejenigen technischen und organisatorischen Maßnahmen im Vertrag vorsehen, die unter Berücksichtigung des anwendbaren Datenschutzrechts, des Stands der Technik und der bei ihrer Durchführung entstehenden Kosten erforderlich sind, um personenbezogene Daten gegen die zufällige oder unrechtmäßige Zerstörung oder den zufälligen

[5] ABl. L 181 vom 4.7.2001, S. 19.

Verlust, die Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung zu schützen.

(13) Um den Datenstrom aus der Europäischen Union zu erleichtern, ist es wünschenswert, dass Auftragsverarbeiter, die Datenverarbeitungsleistungen für mehrere für die Verarbeitung Verantwortliche in der Europäischen Union erbringen, die Möglichkeit erhalten, ungeachtet des Mitgliedstaats, von dem die Datenübermittlung ausgeht, die gleichen technischen und organisatorischen Sicherheitsmaßnahmen anzuwenden, insbesondere wenn der Datenimporteur von verschiedenen Einrichtungen des in der Europäischen Union niedergelassenen Datenexporteurs Daten zur Weiterverarbeitung erhält; in diesem Fall sollte das Recht des Mitgliedstaats Anwendung finden, in dem der Datenexporteur niedergelassen ist.

(14) Es ist angebracht, die Informationen festzulegen, die von den Parteien in dem Vertrag über die Übermittlung unbedingt mitgeteilt werden sollten. Die Mitgliedstaaten sollten weiterhin die Befugnis haben, die Informationen im Einzelnen festzulegen, die von den Parteien zu liefern sind. Die Wirkung dieses Beschlusses sollte im Lichte der Erfahrung geprüft werden.

(15) Der Datenimporteur sollte die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und entsprechend dessen Anweisungen sowie den in den Klauseln enthaltenen Pflichten verarbeiten. Ohne die vorherige schriftliche Einwilligung des Datenexporteurs sollte der Datenimporteur die personenbezogenen Daten nicht an Dritte weitergeben. Der Datenexporteur sollte den Datenimporteur während der Dauer der Datenverarbeitungsdienste anweisen, die Daten gemäß seinen Anweisungen, dem anwendbaren Datenschutzrecht und den in den Klauseln beschriebenen Pflichten zu verarbeiten.

(16) Im Bericht über die Durchführung der Entscheidungen über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer wurde die Festlegung von Standardvertragsklauseln über die anschließende Weiterübermittlung von einem Datenverarbeiter in einem Drittland an einen anderen Datenverarbeiter (Vergabe eines Unterauftrags für die Verarbeitung) empfohlen, um dem Globalisierungstrend in den Geschäftspraktiken und Gepflogenheiten bei der Datenverarbeitung Rechnung zu tragen.

(17) Dieser Beschluss sollte spezifische Standardvertragsklauseln über die Vergabe eines Unterauftrags über Datenverarbeitungsdienste an in Drittländern niedergelassene Auftragsverarbeiter (Unterauftragsverarbeiter) durch einen in einem Drittland niedergelassenen Datenverarbeiter (den Datenimporteur) enthalten. Ferner sollte dieser Beschluss Bedingungen vorsehen, die bei der Vergabe von Unteraufträgen über Datenverarbeitungsdienste zu erfüllen sind, damit gewährleistet ist, dass die übermittelten personenbezogenen Daten auch bei einer Weiterübermittlung an einen Unterauftragsverarbeiter geschützt sind.

(18) Darüber hinaus sollte die Vergabe von Unteraufträgen über Datenverarbeitungsdienste ausschließlich Tätigkeiten betreffen, die in dem Vertrag zwischen dem Datenexporteur und dem Datenimporteur, der die Standardvertragsklauseln gemäß diesem Beschluss enthält, vereinbart worden sind, und keine anderen Verarbeitungstätigkeiten oder Verarbeitungszwecke, so dass das Zweckbindungsprinzip gemäß der Richtlinie 95/46/EG gewahrt bleibt. Sollte sich der Unterauftragsverarbeiter nicht an seine Datenverarbeitungspflichten nach dem Vertrag halten, sollte der Datenimporteur gegenüber dem Datenexporteur verantwortlich sein. Die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die außerhalb der Europäischen Union niedergelassen sind, sollte nicht die Tatsache berühren, dass für die Verarbeitungstätigkeiten das anwendbare Datenschutzrecht gilt.

(19) Standardvertragsklauseln müssen einklagbar sein, und zwar nicht nur durch die Organisationen, die Vertragsparteien sind, sondern auch durch die betroffenen Personen, insbesondere wenn ihnen als Folge eines Vertragsbruchs Schaden entsteht.

(20) Die betroffene Person sollte berechtigt sein, gegen den Datenexporteur, der für die Verarbeitung der übermittelten personenbezogenen Daten verantwortlich ist, vorzugehen und von diesem gegebenenfalls Schadenersatz zu erlangen. In Ausnahmefällen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, sollte die betroffene Person auch berechtigt sein, gegen den Datenimporteur vorzugehen und von diesem wegen Verstoßes des Datenimporteurs oder eines seiner Unterauftragsverarbeiter gegen eine der in Klausel 3 Absatz 2 genannten Pflichten gegebenenfalls Schadenersatz zu erlangen. In Ausnahmefällen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, sollte die betroffene Person zudem berechtigt sein, gegen den Unterauftragsverarbeiter vorzugehen und von diesem gegebenenfalls Schadenersatz zu erlangen. Eine solche Haftpflicht des Unterauftragsverarbeiters sollte auf dessen Verarbeitungstätigkeiten nach den Vertragsklauseln beschränkt sein.

(21) Wird eine Streitigkeit zwischen einer betroffenen Person, die sich auf die Drittbegünstigtenklausel beruft, und dem Datenimporteur nicht gütlich beigelegt, sollte der Datenimporteur der betroffenen Person die Wahl lassen zwischen einem Schlichtungsverfahren oder einem Gerichtsverfahren. Inwieweit die betroffene Person tatsächlich wählen kann, hängt von dem Vorhandensein zuverlässiger und anerkannter Schlichtungsverfahren ab. Falls die Kontrollstelle des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, solche Schlichtungsverfahren vorsieht, sollte diese Möglichkeit angeboten werden.

(22) Auf den Vertrag sollte das Recht des Mitgliedstaats angewandt werden, in dem der Datenexporteur niedergelassen ist und in dem ein Drittbegünstigter die

Einhaltung des Vertrags gerichtlich durchsetzen kann. Betroffene Personen sollten, wenn sie dies wünschen und das nationale Recht es zulässt, berechtigt sein, sich von Vereinigungen oder sonstigen Einrichtungen vertreten zu lassen. Das gleiche Recht sollte auch für sämtliche Datenschutzbestimmungen jedes Vertrags mit einem Unterauftragsverarbeiter über die Verarbeitung personenbezogener Daten gelten, die nach den Vertragsklauseln von einem Datenexporteur an einen Datenimporteur übermittelt worden sind.

(23) Da dieser Beschluss nur Anwendung findet, wenn ein in einem Drittland niedergelassener Datenverarbeiter einen in einem Drittland niedergelassenen Unterauftragsverarbeiter mit seinen Verarbeitungsdiensten beauftragt, sollte er keine Anwendung finden, wenn ein in der Europäischen Union niedergelassener Auftragsverarbeiter, der personenbezogene Daten im Auftrag eines in der Europäischen Union niedergelassenen für die Verarbeitung Verantwortlichen verarbeitet, einen in einem Drittland niedergelassenen Unterauftragsverarbeiter mit der Verarbeitung beauftragt. In diesem Fall steht es den Mitgliedstaaten frei zu entscheiden, ob sie die Tatsache berücksichtigen möchten, dass bei der Vergabe eines Verarbeitungsauftrags an einen in einem Drittland niedergelassenen Unterauftragsverarbeiter die in diesem Beschluss vorgesehenen und in Standardvertragsklauseln festzuschreibenden Grundsätze und Garantien mit dem Ziel zur Anwendung gebracht wurden, die Rechte der von der Datenübermittlung zwecks Unterauftragsverarbeitung betroffenen Person angemessen zu schützen.

(24) Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die durch Artikel 29 der Richtlinie 95/46/EG eingesetzt wurde, hat eine Stellungnahme zu dem Schutzniveau abgegeben, das die Standvertragsklauseln im Anhang zu diesem Beschluss bieten; die Stellungnahme wurde bei der Ausarbeitung des vorliegenden Beschlusses berücksichtigt.

(25) Die Entscheidung 2002/16/EG sollte aufgehoben werden.

(26) Die im vorliegenden Beschluss enthaltenen Maßnahmen entsprechen der Stellungnahme des Ausschusses, der durch Artikel 31 der Richtlinie 95/46/EG eingesetzt wurde –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die Standardvertragsklauseln im Anhang gelten als angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte nach Artikel 26 Absatz 2 der Richtlinie 95/46/EG.

Artikel 2

Dieser Beschluss betrifft ausschließlich den Schutz, der durch die im Anhang aufgeführten Standardvertragsklauseln bei der Übermittlung personenbezogener Daten an Auftragsverarbeiter gewährleistet wird. Die Anwendung anderer nationaler Vorschriften zur Durchführung der Richtlinie 95/46/EG, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, bleibt davon unberührt.

Der vorliegende Beschluss gilt für die Übermittlung personenbezogener Daten durch für die Verarbeitung Verantwortliche, die in der Europäischen Union niedergelassen sind, an Empfänger außerhalb der Europäischen Union, die ausschließlich als Auftragsverarbeiter fungieren.

Artikel 3

Für die Zwecke dieses Beschlusses gelten die folgenden Begriffsbestimmungen:

a) Der Begriff „besondere Datenkategorien“ bezeichnet die in Artikel 8 der Richtlinie 95/46/EG genannten Daten;

b) der Begriff „Kontrollstelle“ bezeichnet die Behörde gemäß Artikel 28 der Richtlinie 95/46/EG;

c) der Begriff „Datenexporteur“ bezeichnet den für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten übermittelt;

d) der Begriff „Datenimporteur“ bezeichnet den in einem Drittland niedergelassenen Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur nach dessen Anweisungen und den Vorschriften dieses Beschlusses personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung in dessen Auftrag zu verarbeiten, und der nicht dem System eines Drittlands unterliegt, das ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG bietet;

e) der Begriff „Unterauftragsverarbeiter“ bezeichnet den Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Standardvertragsklauseln im Anhang und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

f) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, für den für die Verarbeitung Verantwortlichen gelten;

g) der Ausdruck „technische und organisatorische Sicherheitsmaßnahmen“ bezeichnet Maßnahmen zum Schutz personenbezogener Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung.

Artikel 4

(1) Unbeschadet ihrer Befugnisse, tätig zu werden, um die Einhaltung nationaler Vorschriften gemäß den Kapiteln II, III, V und VI der Richtlinie 95/46/EG zu gewährleisten, können die zuständigen Kontrollstellen in den Mitgliedstaaten ihre Befugnisse ausüben und zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung in Drittländer verbieten oder aussetzen, wenn

a) feststeht, dass der Datenimporteur oder Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Artikel 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten,

b) eine zuständige Behörde festgestellt hat, dass der Datenimporteur oder ein Unterauftragsverarbeiter die Standardvertragsklauseln im Anhang nicht eingehalten hat, oder

c) eine hohe Wahrscheinlichkeit besteht, dass die im Anhang enthaltenen Standardvertragsklauseln derzeit oder künftig nicht eingehalten werden und die Fortsetzung der Übermittlung den betroffenen Personen einen schwerwiegenden Schaden zufügen könnte.

(2) Das Verbot oder die Aussetzung gemäß Absatz 1 wird aufgehoben, sobald die Gründe für das Verbot oder die Aussetzung nicht mehr vorliegen.

(3) Wenn die Mitgliedstaaten Maßnahmen gemäß den Absätzen 1 und 2 ergreifen, informieren sie unverzüglich die Kommission, die ihrerseits die Informationen an die anderen Mitgliedstaaten weiterleitet.

Artikel 5

Die Kommission bewertet die Umsetzung des Beschlusses drei Jahre nach seiner Erlassung anhand der verfügbaren Informationen. Sie legt dem durch Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschuss einen Bericht über ihre Erkenntnisse vor. Sie fügt sämtliche Belege bei, die für die Beurteilung der Angemessenheit der Standardvertragsklauseln des Anhangs von Bedeutung sein könnten, sowie etwaige Belege dafür, dass der Beschluss in diskriminierender Weise angewandt wird.

Artikel 6

Dieser Beschluss gilt ab dem 15. Mai 2010.

Artikel 7

(1) Die Entscheidung 2002/16/EG wird ab dem 15. Mai 2010 aufgehoben.

(2) Ein vor dem 15. Mai 2010 gemäß der Entscheidung 2002/16/EG geschlossener Vertrag zwischen einem Datenexporteur und einem Datenimporteur bleibt so lange in Kraft, wie die Übermittlungen und die Datenverarbeitung aufgrund dieses Vertrags unverändert weiterlaufen und von diesem Beschluss erfasste personenbezogene Daten weiterhin zwischen den Vertragsparteien übermittelt werden. Beschließen die Vertragsparteien diesbezügliche Änderungen oder vergeben sie einen Unterauftrag über Verarbeitungsvorgänge, die unter den Vertrag fallen, sind sie verpflichtet, einen neuen Vertrag zu schließen, in dem die Standardvertragsklauseln im Anhang berücksichtigt sind.

Artikel 8

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 5. Februar 2010

Für die Kommission
Jacques BARROT
Vizepräsident

ANHANG

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur): .....

Anschrift: .....

Tel.: ..... Fax: ..... E-Mail: .....

Weitere Angaben zur Identifizierung der Organisation

.....

(„Daten**exporteur**“)

und

Bezeichnung der Organisation (Datenimporteur): .....

Anschrift: .....

Tel.: ..... Fax: ..... E-Mail: .....

Weitere Angaben zur Identifizierung der Organisation:

.....

(„Daten**importeur**“)

(die „Partei“, wenn eine dieser Organisationen gemeint ist, die „Parteien“, wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[6];

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten

[6] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs[7]

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

[7] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i. alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii. jeden zufälligen oder unberechtigten Zugang und

   iii. alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Ver-

tragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich:

.....

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss[8]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich:

.....

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen

[8] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Für den Datenexporteur:

Name (ausgeschrieben): .....

Funktion: .....

Anschrift: .....

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Für den Datenimporteur:

Name (ausgeschrieben): .....

Funktion: .....

Anschrift: .....

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Anhang 1

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Die Mitgliedstaaten können entsprechend den nationalen Verfahren Zusatzangaben, die in diesem Anhang enthalten sein müssen, ergänzen.

Datenexporteur

Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):

.....

.....

.....

Datenimporteur

Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):

.....

.....

.....

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):

.....

.....

.....

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

.....

.....

.....

Besondere Datenkategorien (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):

.....

.....

.....

Verarbeitung

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):

.....

.....

.....

DATENEXPORTEUR
Name: .....

Unterschrift des/der Bevollmächtigten: .....

DATENIMPORTEUR
Name: .....

Unterschrift des/der Bevollmächtigten: .....

Anhang 2

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

.....

.....

.....

.....

BEISPIEL FÜR EINE ENTSCHÄDIGUNGSKLAUSEL (FAKULTATIV)

Haftung

Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist.

Die Entschädigung ist abhängig davon, dass

a) der Datenexporteur den Datenimporteur unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und

b) der Datenimporteur die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten[9].

[9] Der Absatz über die Haftung ist fakultativ.

3. Artikel 29-Datenschutzgruppe

Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting (WP 171)

Angenommen am 22. Juni 2010

Inhaltsverzeichnis

Zusammenfassung

1. Einleitung
2. Online-Werbung auf Basis von Behavioural Targeting
   - 2.1. Vertriebssysteme zur Sendung von Werbung auf Basis von Behavioural Targeting
   - 2.2. Tracking-Technologien
   - 2.3. Erstellen von Profilen, Kennungsarten
3. Rechtsrahmen
   - 3.1. Einleitung
   - 3.2. Der Anwendungsbereich von Artikel 5 Absatz 3 und von Richtlinie 95/46/EG
     - 3.2.1. Materieller Anwendungsbereich von Artikel 5 Absatz 3
     - 3.2.2. Materieller Anwendungsbereich der Richtlinie 95/46/EG: Verarbeitung personenbezogener Daten
     - 3.2.3. Zusammenspiel zwischen den beiden Richtlinien
     - 3.2.4. Territorialer Anwendungsbereich von Artikel 5 Absatz 3 und Richtlinie 95/46/EG
   - 3.3. Rollen und Verantwortlichkeiten der verschiedenen Akteure
4. Verpflichtung zur vorherigen Einholung der Einwilligung in Kenntnis der Sachlage
   - 4.1. Die Verpflichtung zur Einholung der vorherigen Einwilligung der betroffenen Personen im Fall von Werbung auf Basis von Behavioural Targeting
     - 4.1.1. Einwilligung über die Browser-Einstellungen
     - 4.1.2. Einwilligung und die Ausübung von Opt-out-Optionen
     - 4.1.3. Vorherige Mechanismen der Einwilligung durch Opt-in sind besser für eine Einwilligung in Kenntnis der Sachlage geeignet
     - 4.1.4. Einwilligung in Kenntnis der Sachlage: Kinder
   - 4.2. Die Informationspflicht im Zusammenhang mit Werbung auf Basis von Behavioural Targeting
     - 4.2.1. Welche Informationen müssen gegeben werden und von wem?

5. Sonstige Verpflichtungen und Grundsätze im Sinne der Richtlinie 95/46/EG
   5.1. Verpflichtungen bezüglich besonderer Kategorien personenbezogener Daten
   5.2. Einhaltung der Grundsätze in Bezug auf die Qualität der Daten
   5.3. Rechte der betroffenen Person
   5.4. Sonstige Verpflichtungen
6. Schlussfolgerungen und Empfehlungen
   6.1. Geltende Rechtsvorschriften
   6.2. Zuständigkeit, territorialer Anwendungsbereich – Niederlassung
   6.3. Rollen und Verantwortlichkeiten
   6.4. Verpflichtungen und Rechte

Zusammenfassung

Werbung auf Basis von Behavioural Targeting besteht in der Verfolgung von Nutzern, während sie im Internet surfen und das allmähliche Erstellen ihrer Profile, um dann ihren Interessen entsprechende Werbung einzublenden. Die Artikel-29-Arbeitsgruppe zweifelt nicht den möglichen wirtschaftlichen Nutzen von Werbung auf Basis von Behavioural Targeting für die Stakeholder an, ist jedoch der festen Überzeugung, dass solche Praktiken nicht auf Kosten der Rechte von Personen auf Privatsphäre und Datenschutz ausgeübt werden dürfen. Der EU-Rechtsrahmen zum Datenschutz legt bestimmte Schutzklauseln fest. Er ist einzuhalten. Zur Erleichterung und Förderung der Einhaltung, legt die vorliegende Stellungnahme den Rechtsrahmen dar, der von den Personen anzuwenden ist, die im Bereich der Werbung auf Basis von Behavioural Targeting tätig sind.

In der Stellungnahme wird insbesondere festgestellt, dass Betreiber von Werbenetzwerken durch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation gebunden sind, der vorschreibt, dass das Platzieren von Cookies oder ähnlichen Instrumenten auf den Endgeräten des Nutzers oder das Einholen von Informationen über solche Instrumente nur mit der Einwilligung der Nutzer in Kenntnis der Sachlage gestattet ist. In der Stellungnahme wird angemerkt, dass die Einstellungen der derzeit verfügbaren Browser und Opt-out-Mechanismen lediglich unter sehr eingeschränkten Umständen einer Einwilligung gleichkommen. In der Stellungnahme werden die Betreiber von Werbenetzwerken dazu aufgefordert, vorab Opt-in-Mechanismen zu schaffen, die eine positiv bejahende Handlung der betroffenen Personen erforderlich machen, mit der diese ihre Einwilligung in den Erhalt von Cookies oder ähnlichen Instrumenten und in die Überwachung ihrer Internet-Surfgewohnheiten zum Zweck des Versands maßgeschneiderter Werbung erteilen. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass die Einwilligung des Nutzers nur in den Erhalt eines Cookies auch seine Einwilligung in das nachfolgende Lesen des Cookies zur Folge haben könnte und

damit in die Überwachung seines Internet-Surfens. Zur Erfüllung der Anforderungen von Artikel 5 Absatz 3 wäre es folglich nicht erforderlich, für jedes Lesen des Cookies die Einwilligung einzuholen. Damit sich Nutzer der Überwachung jedoch bewusst sind, sollten die Betreiber von Werbenetzwerken: i) den Umfang der Einwilligung zeitlich begrenzen; ii) ein einfaches Zurückziehen der Einwilligung ermöglichen und iii) sichtbare Zeichen schaffen, die eine Überwachung anzeigen. Dieser Ansatz würde das Problem lösen, dass Nutzer mit zahlreichen Hinweisen belastet werden, während gleichzeitig sichergestellt würde, dass das Versenden von Cookies und die folgende Überwachung der Surfgewohnheiten zum Zwecke des Einblendens maßgeschneiderter Werbung nur möglich wären, wenn die betroffene Person ihre Einwilligung in Kenntnis der Sachlage erteilt hat.

Da Werbung auf Basis von Behavioural Targeting auf der Verwendung von Kennungen beruht, die die Erstellung sehr detaillierter Benutzerprofile erlaubt, die in den meisten Fällen als personenbezogene Daten gelten, ist auch Richtlinie Nr. 95/46/EG anwendbar. Die Stellungnahme erklärt, wie die Betreiber von Werbenetzwerken die sich aus dieser Richtlinie ergebenden Verpflichtungen insbesondere in Bezug auf das Auskunftsrecht und das Recht auf Berichtigung, Löschung und Speicherung usw. erfüllen sollten. Unter Berücksichtigung der Tatsache, dass die Anbieter von Online-Inhalten möglicherweise einen Teil der Verantwortung für die Datenverarbeitung tragen, die im Zusammenhang mit Werbung auf der Grundlage von Behavioural Targeting stattfindet, werden die Anbieter von Online-Inhalten in der Stellungnahme dazu aufgefordert, mit den Betreibern von Werbenetzwerken die Verantwortung für das Informieren der Betroffenen zu teilen. Es werden Kreativität und Innovation in dem Bereich gefördert. Angesichts der Natur der Werbung auf Basis von Behavioural Targeting ist Transparenz eine Schlüsselvoraussetzung dafür, dass die Betroffenen dazu in der Lage sind, in die Erhebung und Verarbeitung ihrer personenbezogenen Daten einzuwilligen und eine tatsächliche Wahl zu treffen. In der Stellungnahme wird die Informationspflicht von Betreibern von Werbenetzwerken/Anbietern von Online-Inhalten gegenüber den betroffenen Personen unter besonderer Bezugnahme auf die Datenschutzrichtlinie für elektronische Kommunikation aufgeführt, die verlangt, dass der Nutzer „klare und umfassende Informationen“ erhält.

Die Stellungnahme analysiert und klärt die Verpflichtungen, die durch den geltenden Rechtsrahmen festgesetzt sind. Sie schreibt jedoch nicht vor, wie diese Verpflichtungen technologisch umzusetzen sind. Stattdessen wird die Industrie in der Stellungnahme mehrmals dazu aufgefordert, mit der Artikel-29-Arbeitsgruppe in einen Dialog zu treten, um technische und sonstige Mittel zur schnellstmöglichen Einhaltung des in der Stellungnahme dargelegten Rechtsrahmens zu unterbreiten. Deshalb wird die Artikel-29-Arbeitsgruppe Kontakt mit den Stakeholdern aufnehmen und sie zur Mitarbeit auffordern. Es wird begrüßt, wenn auch Organisationen, die nicht direkt konsultiert werden, einen Beitrag an das Sekretariat der Artikel-29-Arbeitsgruppe senden.

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[1],

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

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

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

Online-Werbung ist eine Haupteinnahmequelle für eine große Reihe von Online-Diensten und stellt einen wichtigen Faktor für das Wachstum und die Expansion der Internetwirtschaft dar. Die spezielle Vorgehensweise der Werbung auf Basis von Behavioural Targeting ruft jedoch wichtige Bedenken in Bezug auf den Datenschutz und die Privatsphäre hervor. Die grundlegende Internettechnologie ermöglicht es Betreibern von Werbenetzwerken, betroffene Personen über verschiedene Websites und über einen längeren Zeitraum hinweg zu verfolgen. Informationen, die über das Surf-Verhaltung der betroffenen Personen erhoben werden, werden für die Erstellung extensiver Profile über die Interessen der betroffenen Personen analysiert. Solche Profile können dazu genutzt werden, den betroffenen Personen maßgeschneiderte Werbung zu senden.

Angesichts der wachsenden Verwendung von Werbung auf Basis von Behavioural Targeting, die auf Tracking-Cookies und ähnlichen Instrumenten basiert und dem Ausmaß, in dem in die Privatsphäre der Menschen eingedrungen wird, hat die Artikel-29-Arbeitsgruppe beschlossen, den Fokus dieser Stellungnahme auf die Online-Werbung auf Basis von Behavioural Targeting über mehrere Websites hinweg zu legen. Dieser Schwerpunkt wird unbeschadet zukünftiger Stellungnahmen gelegt, die möglicherweise andere Werbetechnologien analysieren.

[1] ABl. L 281 vom 23.11.1995, S. 31.

Mit dieser Stellungnahme möchte die Artikel-29-Arbeitsgruppe den Rechtsrahmen erläutern, der für diejenigen Personen anwendbar ist, die im Bereich der Werbung auf Basis von Behavioural Targeting tätig sind. Sie fordert auch die Industrie dazu auf, technische und sonstige Mittel zur schnellstmöglichen Einhaltung des in der Stellungnahme dargelegten Rechtsrahmens vorzuschlagen und bezüglich solcher Mittel mit der Artikel-29-Arbeitsgruppe in einen Dialog zu treten. Schließlich wird die Artikel-29-Arbeitsgruppe die Situation bewerten und die erforderlichen und angemessenen Maßnahmen ergreifen, um die Einhaltung des im Folgenden dargelegten Rechtsrahmens sicherzustellen.

2. Online-Werbung auf Basis von Behavioural Targeting

Interaktive Medienwerbung bezieht sich auf ein breites Spektrum von Methoden, die darauf abzielen, eine stärker personenbezogene Werbung zu schaffen. Die Methoden können in verschiedene Kategorien klassifiziert werden. Dazu gehören unter anderem kontextbezogene Werbung, segmentierte Werbung und Werbung auf Basis von Behavioural Targeting.

Unter ***Werbung auf Basis von Behavioural Targeting*** versteht man Werbung, die auf der Beobachtung des Verhaltens von Personen über einen Zeitraum hinweg basiert. Werbung auf Basis von Behavioural Targeting versucht, die Charakteristika dieses Verhaltens durch die Handlungen (wiederholte Besuche von Websites, Interaktionen, Schlüsselwörter, Produktion von Online-Inhalten usw.) zu untersuchen, um ein konkretes Profil zu erstellen und den betroffenen Personen dann Werbung zu senden, die auf ihre aus den Daten erschlossenen Interessen zugeschnitten ist.

Während kontextbezogene[2] und segmentierte Werbung[3] „Schnappschüsse" dessen verwenden, was die betroffenen Personen auf einer bestimmten Website ansehen oder dort machen oder bekannte persönliche Merkmale der Nutzer, gibt Werbung auf Basis von Behavioural Targeting den Werbetreibenden unter Umständen ein sehr detailliertes Bild über das Online-Leben der betroffenen Person mit Angaben zu vielen der Websites und der speziellen Seiten, die sie besucht haben, zur Verweildauer bei bestimmten Artikeln oder Posten, zur Reihenfolge, in der sie diese besucht haben usw..

[2] Unter kontextbezogener Werbung versteht man Werbung, bei der Werbeanzeigen in Abstimmung mit den gerade von der betroffenen Person besuchten Inhalten ausgewählt werden. Bei Suchmaschinen kann der Inhalt aus den Schlüsselwörtern der Suche, der vorangegangenen Suchanfrage oder der IP-Adresse des Suchenden geschlossen werden, sofern diese einen Hinweis auf die wahrscheinliche geografische Lage gibt.

[3] Werbung, die aufgrund bekannter persönlicher Merkmale der betroffenen Person (Alter, Geschlecht, Standort usw.) ausgewählt wird, die die betroffene Person bei der Anmeldung oder Registrierung angegeben hat.

2.1. Vertriebssysteme zur Sendung von Werbung auf Basis von Behavioural Targeting

Werbung auf Basis von Behavioural Targeting umfasst die folgenden Rollen: *(a) Betreiber des Werbenetzwerks*, als die wichtigsten Inverkehrbringer von Werbung auf Basis von Behavioural Targeting, da sie die Anbieter von Online-Inhalten mit den Werbetreibenden zusammenbringen, *(b) Werbetreibende*, die bei einem bestimmten Empfängerkreis Werbung für ein Produkt oder eine Dienstleistung machen wollen und *c) Anbieter von Online-Inhalten*, die als Eigentümer von Websites Einnahmen erzielen wollen, indem sie Werbeplatz auf ihrer/ihren Website/s verkaufen[4].

Die Werbung über Werbenetzwerke funktioniert im Wesentlichen wie folgt: Der Anbieter von Online-Inhalten reserviert auf seiner Website Bildraum, auf dem Werbung eingeblendet werden kann und überlässt den Rest des Werbeprozesses einem Betreiber oder mehreren Betreibern eines Werbenetzwerks. Diese sind dann dafür verantwortlich, Werbung mit der größtmöglichen Wirkung an die Anbieter von Online-Inhalten zu liefern. Die Betreiber des Werbenetzwerks kontrollieren die Targeting-Technologie und die assoziierten Datenbanken. Je umfangreicher das Werbenetzwerk ist, desto mehr Ressourcen hat es zur Überwachung der Nutzer und zur „Verfolgung" ihrer Gewohnheiten[5]. Der Werbetreibende verhandelt üblicherweise mit mindestens einem Netzwerk. Er kennt nicht zwingend die Identität aller Anbieter von Online-Inhalten (wenn überhaupt eines), die seine Werbung einblenden. Gleichzeitig kann ein Anbieter von Online-Inhalten Verträge mit verschiedenen Werbenetzwerken haben, indem er beispielsweise verschiedene Stellen auf der Website für unterschiedliche Werbenetzwerke reserviert.

Die Praxis, dass Werbenetzwerke über ein Versteigerungssystem[6] zusammenarbeiten, ist immer weiter verbreitet.

---

[4] Werbung auf Basis von Behavioural Targeting kann nicht nur über Werbenetzwerke erfolgen, sondern auch über Onsite-Werbung. Bei dieser Methode nennt der Werbetreibende dem Anbieter von Online-Inhalten die Zielgruppe, die angesprochen werden soll. Die Angaben basieren auf Kriterien, die über demographische Informationen wie die traditionelle Dreiergruppe aus „Altersgruppe, Geschlecht und Land" hinaus auch wesentlicher präziser sein können (wie beispielsweise Schlüsselwörter und Interessen). Der Anbieter von Online-Inhalten sorgt dann dafür, dass die Werbung der gewünschten Zielgruppe präsentiert wird, wobei er Targeting-Technologien anwendet und die Platzierung und Verteilung der Werbung kontrolliert. Dies wird in einigen Plattformen sozialer Netzwerke angewendet, die es zulassen, dass die Nutzer über ihre Interessen als Zielgruppe ermittelt werden.

[5] New York Times, „To Aim Ads, Web is Keeping Closer Eye on You", 10. März 2008. In dem Artikel werden Statistiken über die Häufigkeit aufgeführt, mit der große Werbenetzwerke individuelle Website-Besuche nachverfolgen. Im Fall des Werbenetzwerks von Yahoo! wurde ein durchschnittlicher Nutzer (USA) Ende 2007 angeblich 2 520 Mal im Monat verfolgt.
http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=1&scp=3&sq=%22They%20know%20more%20than%20you%20think%22&st=cse

[6] Die meisten großen Netzwerke haben eine strukturelle Zusammenarbeit mit vielen anderen, sekundären Netzwerken. Siehe zum Beispiel:
Liste der Partner von Google Adsense:
URL:http://www.google.com/support/adsense/bin/answer.py?answer=94149,
Liste der Partner von Yahoo!,: URL:http://info.yahoo.com/privacy/us/yahoo/thirdparties/
Das funktioniert folgendermaßen: Das primäre Netzwerk bietet den Werbeplatz auf dem Webserver verschiedenen Werbenetzwerken an und entscheidet sich für das beste Angebot.

2.2. Tracking-Technologien

Die meisten Tracking- und Werbetechnologien, die für Werbung auf Basis von Behavioural Targeting herangezogen werden, nutzen die eine oder andere Form der clientseitigen Verarbeitung. Sie nutzen Informationen vom Browser und dem Endgerät des Nutzers.Insbesondere die wichtigste Tracking-Technologie, die für die Überwachung der Nutzer im Internet herangezogen wird, basiert auf „Tracking-Cookies". Cookies ermöglichen es, das Internet-Surfen eines Nutzers über einen ausgedehnten Zeitraum und theoretisch auch über mehrere Domänen[7] hinweg zu verfolgen.

Das läuft üblicherweise folgendermaßen ab: normalerweise platziert der Betreiber des Werbenetzwerks einen Tracking-Cookie auf dem Endgerät der betroffenen Person[8], wenn diese das erste Mal eine Website aufruft, die eine Werbung des Netzwerks einblendet. Der Cookie ist ein kurzer alphanumerischer Text, der durch den Betreiber des Netzwerks auf dem Endgerät der betroffenen Person gespeichert (und später abgerufen) wird[9]. Im Zusammenhang mit der Werbung auf Basis von Behavioural Targeting ermöglicht es der Cookie dem Betreiber des Werbenetzwerks einen ehemaligen Besucher zu erkennen, der die Website erneut besucht oder der eine andere Website besucht, die eine Partnerschaft mit dem Werbenetzwerk hat. Solche wiederholten Besuche ermöglichen es dem Betreiber des Werbenetzwerks, ein Profil des Besuchers zu erstellen, das dann zum Einblenden personalisierter Werbung verwendet wird. Da diese Tracking-Cookies von einer anderen Partei als dem Webserver platziert werden, der den Hauptinhalt der Webseite darstellt (d. h. dem Anbieter von Online-Inhalten) werden sie häufig als „Third-Party-Cookies" bezeichnet.

Cookies sind an eine Domäne gebunden: ein Cookie kann nur durch eine Website gelesen oder geändert werden, die von einer ähnlichen Domäne stammt[10] (wenn z. B. ein Cookie von dem Werbeprovider a.mysite.com platziert wird, kann er von

---

7 Andere Tracking-Technologien basieren beispielsweise auf der Nutzung der IP-Adresse oder der Browser-Signatur. Die Electronic Frontier Foundation hat die Identifizierbarkeit von individuellen Browser-Signaturen (User Agent) einschließlich der verwendeten Software, der Version, Sprache und der installierten Plug-ins untersucht; URL: http://panopticlick.eff.org/). In Bezug auf die IP-Adressen hat ein US-Unternehmensgründer kürzlich bekannt gegeben, dass er über eine Datenbank von 65 Millionen IP-Adressen mit den jeweiligen Namen und Adressen-Daten verfügt; URL: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=123280.

8 Wenn eine betroffene Person verschiedene Browser benutzt, sind die Cookies für jeden Browser unterschiedlich.

9 Dieser alphanumerische Text kann einer Vielzahl von Zwecken dienen, wie beispielsweise der Speicherung von Präferenzen, dem Speichern von Sitzungsinformationen oder der Identifizierung von betroffenen Personen durch eine eindeutige Kennung.

10 Es gibt jedoch einfache Lösungen für kooperierende Parteien, die diese Einschränkungen umschiffen und gemeinsame Cookies nutzen wollen. Der Besitzer einer Domäne kann seinen DNS so konfigurieren, dass einem Dritten die Nutzung einer seiner Sub-Domänen erlaubt wird. Der Dritte kann dann bestimmte Cookies mit dem Eigentümer der Domäne gemeinsam nutzen. Bei anderen Techniken stellt Javascript zusätzliche Webanfragen bei wieder anderen Servern und ermöglicht noch mehr Parteien das Vernetzen oder Synchronisieren ihrer Tracking-Daten (http://blog.kruxdigital.com/2010/02/24/cookie-synching/).

b.mysite.com gelesen werden, aber nicht von dem Werbeprovider c.sonstiger.com). Cookies haben eine unterschiedliche Lebensdauer. Diese Lebensdauer kann bei weiteren Besuchen auf derselben Site möglicherweise verlängert werden oder auch nicht (es ist eine Design-Entscheidung des Programmierers). „Dauerhafte Cookies" haben entweder ein genaues Ablaufdatum, das weit in der Zukunft liegt oder bis sie manuell gelöscht werden.

Die meisten Internet-Browser bieten die Möglichkeit, Third-Party-Cookies zu blockieren. Einige Browser unterstützen „private" Browser-Sitzungen, die automatisch alle erstellten Cookies zerstören, wenn das Browser-Fenster geschlossen wird[11].

Einige Werbenetzwerke ersetzen oder ergänzen die herkömmlichen Tracking-Cookies durch/mit neue/n, verbesserte/n Tracking-Technologien wie „Flash-Cookies" (lokale gemeinsame Objekte)[12]. Flash-Cookies können nicht über die normalen Datenschutz-Einstellungen eines Web-Browsers gelöscht werden. Es wurde berichtet, dass Flash-Cookies ausdrücklich genutzt wurden, um „herkömmliche Cookies" zu ersetzen, die von der betroffenen Person abgelehnt oder gelöscht worden waren[13].

Diese Praxis ist als *Respawning* bekannt. Wenn in der vorliegenden Stellungnahme der Begriff „Cookie" verwendet wird, bezieht er sich – sofern nichts anderes angegeben ist – auf alle Technologien, die auf dem Prinzip beruhen, Informationen auf den Endgeräten des Nutzers zu speichern oder Zugriff auf diese zu nehmen.

Wie oben dargelegt, kann ein einziges Werbe-Netzwerk normalerweise nur einen Teil des Internet-Surf-Verhaltens der betroffenen Person überwachen, da seine Tracking-Fähigkeit auf die Anbieter von Online-Inhalten beschränkt ist, mit dem es verlinkt ist. In der jüngsten Vergangenheit wurde jedoch ein anderer Ansatz getestet, bei dem das Werbe-Netzwerk eine Partnerschaft mit einem Internet-Dienstanbieter einging, um den Browser-Inhalt des Nutzers zu überwachen und Tracking-Cookies bei jeden unverschlüsselten Web-Verkehr einzufügen[14]. Der

---

[11] Die neuesten Versionen vieler beliebter Browser (z. B. Internet Explorer 8, Google Chrome, Firefox, Safari usw.) unterstützen Browsing-Sitzungen, die automatisch alle Cookies löschen, die während der Sitzung installiert wurden.

[12] W3C entwickelt auch gerade einen „DOM Speicher"-Standard, der die Schaffung eines großen lokalen Datenspeichers über Skripte auf dem Computer des Nutzers ermöglichen wird.

[13] Flash-Cookies sind dazu in der Lage, Informationen über Einstellungen zu speichern und die Wünsche des Nutzers zu umgehen. Siehe Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, „Flash-Cookies and Privacy" (10. August 2009). Verfügbar unter SSRN: http://ssrn.com/abstract=1446862

[14] Das Unternehmen Phorm beispielsweise hat über seine Technologie namens Webwise eine Dienstleistung für Werbung auf Basis von Behavioural Targeting angeboten, das Deep Packet Inspection nutzt, um die von Internet-Nutzern besuchten Seiten zu untersuchen. Phorm hat mit Internet-Dienstanbietern Partnerschaftsabkommen getroffen, um diese Dienstleistung anbieten zu können.

Artikel-29-Arbeitsgruppe ist keine derzeitige Anwendung dieser Technologie in der EU bekannt, sie ist aber der Ansicht, dass die Anwendung dieser Technologie unbeschadet der Zwecke, für die diese Daten genutzt werden, ernsthafte rechtliche Fragestellungen aufwirft, die über die Verarbeitung personenbezogener Daten hinausgeht. Die Analyse dieser Werbe-Technologie fällt nicht in den Geltungsbereich dieser Stellungnahme.

2.3. Erstellen von Profilen, Kennungsarten

Es gibt zwei hauptsächliche Ansätze für das Erstellen von Nutzerprofilen: *i)* **Prädiktive Profile** werden erstellt, indem das individuelle und das kollektive Nutzerverhalten über einen längeren Zeitraum hinweg beobachtet wird, insbesondere durch Überwachung der besuchten Seiten und der angesehenen und angeklickten Werbung und daraus Rückschlüsse gezogen werden. *ii)* **Explizite Profile** werden aus personenbezogenen Daten erstellt, die die betroffenen Personen selbst beispielsweise bei der Registrierung an einen Webdienst liefern. Es können auch beide Ansätze kombiniert werden. Darüberhinaus können prädiktive Profile später in explizite Profile umgewandelt werden, wenn eine betroffene Person Anmeldedaten für eine Website angibt[15].

Werbe-Netzwerke erstellen prädiktive Profile, indem sie Tracking-Techniken, Cookiebasierte Technologien und Data-Mining-Software miteinander kombinieren. Das Geschlecht und die Altersgruppe können über die von der betroffenen Person besuchten Seiten und über die Werbung erschlossen werden, die von der betroffenen Person bevorzugt angeklickt wird. Ein Profil, das auf der Analyse der auf dem Endgerät der betroffenen Person gespeicherten Cookies basiert, kann mit Hilfe von erhobenen Daten angereichert werden, die von dem Verhalten von betroffenen Personen abgeleitet werden, die in anderen Zusammenhängen ähnliche Verhaltensmuster aufweisen. Systeme der Online-Werbung ordnen betroffene Personen häufig über ihre Interessen oder Vertriebskategorien in Segmente ein (Beispiele hierfür sind „Gärtnern“, „Körperpflege“, „Elektronik“ usw.).

Der Standort der betroffenen Person ist ebenfalls eine primäre Quelle des zielgerichteten Erstellens von Profilen. Er kann zum Beispiel über die IP-Adresse des Endgeräts oder über WIFI-Zugangspunkte[16] erschlossen werden.

---

[15] Einige Werbenetzwerke ermöglichen es registrierten Nutzern zumindest bis zu einem gewissen Grad, ihre assoziierten prädiktiven Profile anzusehen und zu bearbeiten.

[16] Zusätzliche Informationen über den Standort können von anderen Quellen erhoben und für das Erstellen von Profilen genutzt werden.

3. Rechtsrahmen

3.1. Einleitung

Artikel 5 Absatz 1 der Richtlinie 2002/58[17] schützt die Vertraulichkeit der Kommunikation im Allgemeinen. Der Schutz der Vertraulichkeit der Kommunikation im konkreten Fall der Verwendung von Cookies und ähnlichen Instrumenten ist in erster Linie in Artikel 5 Absatz 3 niedergelegt. Diese Stellungnahme bezieht sich auf die geänderte Richtlinie 2002/58 (nachstehend „Datenschutzrichtlinie für elektronische Kommunikation" oder „geänderte Datenschutzrichtlinie für elektronische Kommunikation" genannt) und verweist auf diese. Die geänderte Datenschutzrichtlinie für elektronische Kommunikation muss nicht vor Mai 2011 durch die Mitgliedstaaten in einzelstaatliches Recht umgesetzt werden. Die Artikel-29-Arbeitsgruppe bezieht sich jedoch bereits auf die geänderte Datenschutzrichtlinie für elektronische Kommunikation, da die Richtlinie auch nach der Umsetzung der Richtlinie gültig sein soll. Außerdem möchte die Artikel-29-Arbeitsgruppe den Stakeholdern deutlich machen, dass sie den geänderten Artikel 5 Absatz 3 vollumfänglich erfüllen müssen. In diesem Zusammenhang ist auch der Erwägungsgrund 66 von Bedeutung, der angenommen wurde, als die Datenschutzrichtlinie für elektronische Kommunikation im Jahr 2009 geändert wurde sowie Erwägungsgründe 24 und 25 der Datenschutzrichtlinie für elektronische Kommunikation.

Angesichts der Bedeutung von Artikel 5 Absatz 3 ist es sinnvoll, den geänderten Text hier wiederzugeben und die Änderungen, die in Bezug auf den vorherigen Text durchgeführt wurden, kenntlich zu machen:

> *Die Mitgliedstaaten stellen sicher, dass die ~~Benutzung elektronischer Kommunikationsnetze für die~~ Speicherung von Informationen oder de~~n~~r Zugriff auf Informationen, die* ***bereits*** *im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur ~~unter der Bedingung~~ gestattet ist, ~~dass~~* ***wenn*** *der betreffende Teilnehmer oder Nutzer* ***auf der Grundlage von klaren und umfassenden Informationen, die er*** *gemäß der Richtlinie 95/46/EG ~~klare und umfassende Informationen insbesondere~~* ***u. a.*** *über die Zwecke der Verarbeitung erhält****, seine Einwilligung gegeben hat.*** *~~und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern.~~ Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung ~~oder Erleichterung~~ der Übertragung einer Nachricht über ein elektronisches Kommunikations-*

[17] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates (vom 2. November 2009) zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

netz ist oder~~, soweit~~ ***wenn*** *dies unbedingt erforderlich ist,* ***damit der Anbieter eines Dienstes der Informationsgesellschaft, der~~ um einen~~*** *vom Teilnehmer oder Nutzer ausdrücklich gewünscht~~en Dienst der Informationsgesellschaft~~* ***wurde, diesen Dienst*** *zur Verfügung~~ zu~~ stellen* ***kann****.*

Zusätzlich zur Datenschutzrichtlinie für elektronische Kommunikation findet die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend „Richtlinie 95/46/EG" genannt) bei Angelegenheiten Anwendung, die nicht ausdrücklich durch die Datenschutzrichtlinie für elektronische Kommunikation geregelt sind, sobald personenbezogene Daten verarbeitet werden[18].

3.2. Der Anwendungsbereich von Artikel 5 Absatz 3 und von Richtlinie 95/46/EG

Für diejenigen, die im Bereich der Werbung auf Basis von Behavioural Targeting tätig sind, ist es hilfreich zu wissen, warum sie zur Einhaltung von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation bzw. zur Einhaltung der Richtlinie 95/46/EG verpflichtet sind. Hierzu muss der Anwendungsbereich beider Richtlinien betrachtet werden. Dazu wird die Artikel-29-Arbeitsgruppe zuerst auf den materiellen Anwendungsbereich beider Richtlinien (3.2.1 und 3.2.2) und auf ihr Zusammenspiel (3.2.3) Bezug nehmen und dann auf den territorialen Anwendungsbereich beider Richtlinien (3.2.4).

3.2.1. Materieller Anwendungsbereich von Artikel 5 Absatz 3

Artikel 5 Absatz 3 macht es erforderlich, die Einwilligung in Kenntnis der Sachlage einzuholen, um Informationen rechtmäßig zu speichern oder Zugriff auf Informationen zu nehmen, die auf dem Endgerät eines Teilnehmers oder Nutzers gespeichert sind[19]. Unter Berücksichtigung der Tatsache, dass (i) Tracking-Cookies „Informationen" sind, die auf dem Endgerät der betroffenen Person gespeichert sind und dass (ii) die Betreiber des Werbenetzwerks Zugriff auf diese Informationen nehmen, wenn die betroffenen Personen eine Partner-Website besuchen, ist Artikel 5 Absatz 3 vollumfänglich anwendbar. Folglich müssen die Be-

[18] Siehe Artikel 1 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation, der Folgendes festlegt: „Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar."

[19] Die Datenschutzrichtlinie für elektronische Kommunikation verweist auf Teilnehmer und Nutzer. Der Begriff „Teilnehmer" umfasst sowohl natürliche Personen oder betroffene Personen (wie in Richtlinie 95/46/EG auf sie Bezug genommen wird) als auch juristische Personen. Das Wort „Nutzer" bezieht sich auf betroffene Personen, die elektronische Kommunikationsdienste nutzen, ohne diese notwendigerweise abonniert zu haben. Aus Gründen der Konsistenz wird in dieser Stellungnahme soweit wie möglich der Begriff „betroffene Person" verwendet.

stimmungen von Artikel 5 Absatz 3 bei der Platzierung von Cookies oder von ähnlichen Instrumenten (unbeschadet ihrer Art)[20] und bei jeder nachfolgenden Nutzung der vorher platzierten Cookies, mit der Zugriff auf Informationen der betroffenen Partei genommen werden soll, eingehalten werden.

Artikel 5 Absatz 3 gilt für „Informationen" (gespeicherte Informationen und/oder Informationen, auf die Zugriff genommen wird). Er macht hier keinen Unterschied. Für die Anwendung dieser Bestimmung ist es nicht erforderlich, dass es sich bei den Informationen um personenbezogene Daten im Sinne der Richtlinie 95/46/EG handelt. Erwägungsgrund 24 fängt die Rationale dieses Ansatzes ein, indem er Folgendes feststellt: „*Die Endgeräte von Nutzern … 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*". Die in Artikel 5 Absatz 3 niedergelegten Verpflichtungen werden durch den Schutz eines Bereichs bedingt, der als Teil der Privatsphäre der betroffenen Person angesehen wird und nicht dadurch, ob diese Informationen personenbezogene Daten sind oder nicht.

Die Arbeitsgruppe hat bereits in ihrer Stellungnahme1/2008[21] dargelegt, dass Artikel 5 Absatz 3 eine allgemeine Bestimmung ist, die nicht nur auf elektronische Kommunikationsdienste anwendbar ist, sondern auch auf andere Dienste, in denen diese Techniken verwendet werden. Darüber hinaus findet Artikel 5 Absatz 3 unabhängig davon Anwendung, ob es sich bei der das Cookie platzierenden Stelle um einen für die Verarbeitung Verantwortlichen oder um einen Auftragsverarbeiter handelt.

3.2.2. Materieller Anwendungsbereich der Richtlinie 95/46/EG: Verarbeitung personenbezogener Daten

Wenn die erhobenen Informationen als Ergebnis der Platzierung eines Cookies oder ähnlichen Instruments und des Abrufens der Informationen als personenbezogene Daten angesehen werden könne n, findet zusätzlich zu Artikel 5 Absatz 3 auch die Richtlinie 95/46/EG Anwendung.

Die Artikel-29-Arbeitsgruppe merkt an, dass die in dieser Stellungnahme beschriebenen Methoden der Werbung auf Basis von Behavioural Targeting häufig die Verarbeitung personenbezogener Daten mit sich bringen, wie sie in Artikel 2 der Richtlinie 95/46/EG definiert und durch die Artikel-29-Arbeitsgruppe ausge-

[20] Artikel 5 Absatz 3 ist technologisch neutral. Er ist folglich nicht nur auf Cookies anzuwenden, sondern auch auf alle sonstigen Technologien, die dazu genutzt werden, Informationen zu speichern oder Zugang zu Informationen zu erhalten, die auf den technischen Geräten von Personen gespeichert sind (Spyware, Malware, usw.).

[21] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, angenommen am 04.04.2008.

legt wurden[22]. Hierfür gibt es mehrere Gründe: *i)* Werbung auf Basis von Behavioural Targeting umfasst üblicherweise das Sammeln von IP-Adressen und die Verarbeitung eindeutiger Kennungen (durch den Cookie). Die Verwendung solcher Instrumente mit einer eindeutigen Kennung ermöglicht die Verfolgung von Nutzern eines bestimmten Computers, selbst wenn dynamische IP-Adressen verwendet werden. Anders ausgedrückt ermöglicht die Verwendung solcher Instrumente das „Auswählen" einzelner betroffener Personen, selbst wenn ihr wirklicher Name nicht bekannt ist. *ii)* Darüber hinaus *beziehen sich* die Informationen, die im Zusammenhang mit Werbung auf Basis des Behavioural Targeting erhoben werden, auf die persönlichen Merkmale oder das Verhalten einer Person (d. h. es sind Informationen über die persönlichen Merkmale und das Verhalten) und sie werden dazu genutzt, diese bestimmte Person zu beeinflussen[23]. Diese Ansicht wird weiter bestärkt, wenn man die Möglichkeit in Betracht zieht, dass die Profile jederzeit mit direkt identifizierbaren Informationen verknüpft werden können, die die betroffene Person selbst angibt, wie z. B. mit einer Registrierung verbundene Informationen. Andere Szenarien, die zu einer Identifizierbarkeit führen könnten, sind Zusammenschlüsse, Datenverluste, und die steigende Verfügbarkeit im Internet von personenbezogenen Daten in Verbindung mit IP-Adressen.

3.2.3. Zusammenspiel zwischen den beiden Richtlinien

Finden beide Richtlinien Anwendung, muss geklärt werden, welche Bestimmungen der jeweiligen Richtlinie anzuwenden sind. Diesbezüglich legt Erwägungsgrund 10 der Datenschutzrichtlinie für elektronische Kommunikation fest, dass Richtlinie 95/46/EG „*für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten* [gilt], *die von der vorliegenden Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte des Einzelnen*".

Dies ist eine Anwendung des Grundsatzes, dass das speziellere Gesetz *(lex specialis)* dem allgemeineren Gesetz *(lex generalis)* vorgeht.

Gemäß oben Stehendem ist Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, der sich mit der Einwilligung in Kenntnis der

---

[22] Siehe die Auslegung zum Begriff „personenbezogene Daten" der Artikel-29-Arbeitsgruppe in der Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", angenommen am 20.06.2007.

[23] In ihrer Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, angenommen am 4. April 2008, bestätigt die Artikel-29-Arbeitsgruppe, dass Cookies und IP-Adressen in den meisten Fällen als personenbezogene Daten einzustufen sind. Die vorgenannte Richtlinie stellte Folgendes fest: „Wenn ein Cookie eine eindeutige Benutzerkennung enthält, handelt es sich bei dieser Kennung eindeutig um personenbezogene Daten. Dauerhafte Cookies oder ähnliche Mittel mit einer eindeutigen Benutzerkennung ermöglichen die Verfolgung der Benutzer eines bestimmten Computers selbst bei Verwendung dynamischer IP-Adressen. Die Verhaltensdaten, die durch den Einsatz dieser Mittel generiert werden, ermöglichen eine noch stärkere Fokussierung auf die persönlichen Merkmale der betreffenden Person".

Sachlage befasst, direkt anwendbar. Richtlinie 95/46/EG ist vollumfänglich anwendbar mit Ausnahme der Bestimmungen, die in der Datenschutzrichtlinie für elektronische Kommunikation direkt behandelt werden. Dies gilt in erster Linie für Artikel 7 der Richtlinie 95/46/EG zu den Rechtsgrundlagen für die Datenverarbeitung[24]. Die verbleibenden Bestimmungen der Richtlinie 95/46/EG einschließlich der Grundsätze bezüglich der Datenqualität, der Rechte der betroffenen Personen (wie das Auskunftsrecht, das Recht auf Löschung und das Widerspruchsrecht), der Vertraulichkeit, der Sicherheit der Verarbeitung und der internationalen Datenübermittlungen sind vollumfänglich anzuwenden.

3.2.4. Territorialer Anwendungsbereich von Artikel 5 Absatz 3 und Richtlinie 95/46/EG

Der territorial Anwendungsbericht des vorgenannten Rechtsrahmens wird durch eine Kombination von Artikel 3 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation[25] mit Artikel 4 Absatz 1 Buchstaben a und c der Richtlinie 95/46/EG[26] bestimmt.

In früheren Stellungnahmen hat die Artikel-29-Arbeitsgruppe Vorgaben zum Begriff der Niederlassung und der Verwendung der Mittel gemäß Artikel 4 Absatz 1 Buchstaben a beziehungsweise c als Determinanten für die Anwendung der Richtlinie 95/46/EG[27] gemacht. Diese Vorgaben sind für Betreiber eines Werbenetzwerks vollumfänglich anwendbar.

3.3. Rollen und Verantwortlichkeiten der verschiedenen Akteure

Wie oben dargelegt, umfasst die Werbung auf Basis von Behavioural Targeting unterschiedliche Akteure, einschließlich der Betreiber von Werbenetzwerken, der Anbieter von Online-Inhalten und der Werbetreibenden. Es ist wichtig, ihre jeweiligen Rollen zu bewerten, um ihre Verpflichtungen gemäß den geltenden

---

[24] Das Prinzip der Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise im Sinne von Artikel 6 Absatz 1 Buchstabe a kann auch als Bestandteil von Artikel 5 Absatz 3gesehen werden, da Treu und Glauben auf Transparenz verweist und diese fordert.

[25] Der Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation ist in den Artikel 3 Absatz 1 der Richtlinie festgelegt, gemäß dem Artikel 5 Absatz 3 für die Speicherung und den Zugang zu Informationen in den Endgeräten der betroffenen Personen anzuwenden ist, die öffentliche Kommunikationsnetze in der EU nutzen.

[26] Die beiden Kriterien, welche die Anwendung der Richtlinie (oder genauer der nationalen Gesetze, die sie durchführen) bedingen, sind (i) gemäß Artikel 4 Absatz 1 Buchstabe a die Ausführung der Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen und (ii) der für die Verarbeitung Verantwortliche ist gemäß Artikel 4 Absatz 1 Buchstabe c nicht im Gebiet der EU niedergelassen und greift zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurück, die im Hoheitsgebiet der EU gelegen sind.

[27] Siehe WP 56 vom 30. Mai 2002 über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU und jüngeren Datums Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, angenommen am 4. April 2008.

Datenschutzvorschriften festzulegen. In dieser Hinsicht führt die Artikel-29-Arbeitsgruppe Folgendes aus:

In Bezug auf Betreiber von Werbenetzwerken:

Erstens, die Verpflichtungen gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation finden auf diejenigen Anwendung, die Cookies auf den Endgeräten der betroffenen Personen platzieren und/oder Informationen von Cookies abrufen, die bereits auf diesen Geräten gespeichert sind. Gemäß Artikel 5 Absatz 3 ist es unerheblich ob die Stelle, die den Cookie platziert oder abruft, ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter ist. Im Zusammenhang mit Werbung auf Basis von Behavioural Targeting verpflichtet eine solche Interpretation den Betreiber des Werbenetzwerks zur Einholung der Einwilligung in Kenntnis der Sachlage.

Zweitens, agieren Betreiber eines Werbenetzwerks gleichzeitig als für die Verarbeitung Verantwortliche, wenn Werbung auf Basis von Behavioural Targeting die Verarbeitung personenbezogener Daten umfasst. Dies ist sehr wichtig, da dann zusätzliche Verpflichtungen gemäß Richtlinie 95/46/EG Anwendung finden. Betreiber von Werbenetzwerken haben die vollständige Kontrolle über die Zwecke und die Mittel der Verarbeitung.

Sie „mieten" Platz auf den Websites der Anbieter von Online-Inhalten, um Werbung einzublenden, sie platzieren und lesen Cookie-bezogene Informationen und sammeln in den meisten Fällen IP-Adressen und sonstige Daten, die der Browser möglicherweise offenlegt. Darüber hinaus verwenden die Betreiber des Werbenetzwerks Informationen, die sie über das Surfverhalten von Internetnutzern gewonnen haben, um Profile zu erstellen und die Werbung auszuwählen und zu liefern, die auf der Grundlage dieses Profils eingeblendet werden soll. In dem Fall agieren sie eindeutig als für die Verarbeitung Verantwortliche.

In Bezug auf Anbieter von Online-Inhalten:

Anbieter von Online-Inhalten vermieten unter anderem Platz auf ihren Websites, damit Werbenetzwerke ihre Werbung platzieren. Sie konfigurieren ihre Websites so, dass die Browser von Besuchern automatisch zur Internetseite des Betreibers von Werbenetzwerken umgeleitet werden (die dann einen Cookie versendet und gezielte Werbung einblendet). Deshalb stellt sich die Frage bezüglich ihrer Verantwortung in Bezug auf die Datenverarbeitung.

Wie die Artikel-29-Arbeitsgruppe kürzlich darlegte[28], hängt es von den Bedingungen der Zusammenarbeit zwischen dem Anbieter von Online-Inhalten und

[28] Stellungnahme 1/2010 zum Begriff „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", angenommen am 16.02.2010.

dem Betreiber des Werbenetzwerks ab, ob der Anbieter von Online-Inhalten gemeinsam mit dem Betreiber des Werbenetzwerks als für die Verarbeitung Verantwortlicher angesehen wird. Diesbezüglich merkt die Artikel-29-Arbeitgruppe an, dass der Beitrag von Anbietern von Online-Inhalten in einem typischen Szenario, in dem Betreiber von Werbenetzwerken gezielte Werbung einblenden, darin besteht, ihre Websites so zu konfigurieren, dass der Browser eines Besuchers der Internetseite von Anbietern von Online-Inhalten automatisch auf die Internetseite des Betreibers von Werbenetzwerken umgeleitet wird. Dabei übermittelt der Browser des Nutzers seine IP-Adresse an den Betreiber des Werbenetzwerks, der darauf den Cookie und die gezielte Werbung versendet. Es muss angemerkt werden, dass es bei diesem Szenario nicht die Anbieter von Online-Inhalten sind, die die IP-Adresse des Besuchers an den Betreiber des Werbenetzwerks weiterleiten. Stattdessen ist es der Browser des Besuchers, der diese Information automatisch an den Betreiber des Werbenetzwerks weiterleitet. Dies ist jedoch nur der Fall, weil der Anbieter von Online-Inhalten seine Internetseite so konfiguriert hat, dass ein Besucher seiner Seite automatisch zur Website des Betreibers des Werbenetzwerks umgeleitet wird. Anders ausgedrückt, *löst* der Anbieter von Online-Inhalten die Übermittlung der IP-Adresse aus. Das ist der erste erforderliche Schritt zur Ermöglichung der folgenden Verarbeitung, die der Betreiber des Werbenetzwerks ausübt, um gezielte Werbung einzublenden. Folglich ist es nicht die natürliche Person, die die Übermittlung auslöst, auch wenn die Datenübermittlung technisch gesehen, von dem Browser der Person ausgelöst wird, die die Seite des Anbieters von Online-Inhalten besucht. Diese Person wollte nur die Seite des Anbieters von Online-Inhalten besuchen. Sie wollte nicht die Website des Betreibers des Werbenetzwerks besuchen. Dieser Fall tritt derzeit häufig ein.

Unter Berücksichtigung des oben Stehenden ist die Artikel-29-Arbeitsgruppe der Ansicht, dass die Anbieter von Online-Inhalten durch die nationale Umsetzung der Richtlinie 95/46/EG und/oder des nationalen Rechts eine gewisse Verantwortung für die Datenverarbeitung tragen[29]. Diese Verantwortung deckt nicht alle Verarbeitungstätigkeiten ab, die zur Einblendung von Werbung auf Basis von Behavioural Targeting erforderlich sind, wie beispielsweise die Verarbeitung, welche der Betreiber des Online-Werbenetzwerks ausführt. Sie beruht in der Erstellung von Profilen, die dann für den Versand gezielter Werbung genutzt werden. Die Verantwortung des Anbieters von Online-Inhalten deckt jedoch die erste Phase ab, also den anfänglichen Teil der Datenverarbeitung. Es handelt sich hierbei um die Übermittlung der IP-Adresse, die stattfindet, wenn die Website des Anbieters

[29] Die Artikel-29-Arbeitsgruppe merkt an, dass sich die Informationspflicht und mögliche weitere Verpflichtungen auch aus allgemeinen Rechtsgrundsätzen (Vertrags- und Deliktsrecht) und aus verbraucherschutzrechtlichen Vorschriften zwischen Unternehmen und Verbrauchern ergeben können, die im Zusammenhang mit unlauteren Geschäftspraktiken stehen, wie beispielsweise Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken imbinnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates („Richtlinie über unlautere Geschäftspraktiken“).

von Online-Inhalten besucht wird. Dies liegt daran, dass die Anbieter von Online-Inhalten diese Übermittlung vereinfachen und die Zwecke mitbestimmen, für die sie ausgeführt wird, d. h. das Versenden gezielter Werbung an die Besucher. Zusammengefasst tragen die Anbieter von Online-Inhalten aus diesen Gründen für diese Tätigkeiten einen Teil der Verantwortung als für die Verarbeitung Verantwortliche. Diese Verantwortung kann jedoch nicht die Einhaltung eines Großteils der Verpflichtungen erforderlich machen, die sich aus diesen Richtlinien ergeben.

In dieser Hinsicht muss der Rechtsrahmen flexibel ausgelegt werden, indem nur die einschlägigen Bestimmungen angewendet werden. Anbieter von Online-Inhalten speichern keine personenbezogenen Informationen. Also würde die Anwendung einiger der Verpflichtungen aus der Richtlinie wie z. B. das Auskunftsrecht keinen Sinn machen. Wie weiter unten dargelegt wird, ist die Verpflichtung zur Unterrichtung der Personen über die Datenverarbeitung auf die Anbieter von Online-Inhalten jedoch vollumfänglich anwendbar.

Zusätzlich zu oben Stehendem sind Anbieter von Online-Inhalten gemäß der vorgenannten Stellungnahme der Artikel-29-Arbeitsgruppe gemeinsam für die Verarbeitung Verantwortliche, wenn sie personenbezogene Daten ihrer Besucher wie Name, Adresse, Alter, Standort usw. erheben und an den Betreiber des Werbenetzwerks übermitteln. In dem Maße, in dem Anbieter von Online-Inhalten als für die Verarbeitung Verantwortliche handeln, sind sie in Bezug auf den Teil der durch sie kontrollierten Datenverarbeitung durch die Verpflichtungen aus Richtlinie 95/46/EG gebunden. In dieser Hinsicht „müssen [Anbieter von Online-Inhalten zusammen mit den Betreibern von Werbenetzwerken] *sicherstellen, dass sie trotz der (technischen) Komplexität des Systems des Behavioural Targeting in der Lage sind, angemessene Methoden zur Erfüllung ihrer Verpflichtungen und zur Gewährleistung der Rechte der betroffenen Personen zu finden*“[30].

Zusammenfassend gesagt, sollte es Anbietern von Online-Inhalten bewusst sein, dass sie durch das Schließen eines Vertrags mit Werbenetzwerken, aufgrund dessen personenbezogene Daten ihrer Besucher den Betreibern von Online-Werbenetzwerken zur Verfügung stehen, einen Teil Verantwortung gegenüber ihren Besuchern übernehmen. Das Ausmaß ihrer Verantwortung sowie das Ausmaß, in dem sie für die Verarbeitung Verantwortliche werden, sollte von Fall zu Fall abhängig von den besonderen, in dem Dienstleistungsvertrag niedergelegten Bedingungen der Zusammenarbeit mit den Betreibern von Werbenetzwerken untersucht werden. Entsprechend sollten in dem Dienstleistungsvertrag zwischen dem Anbieter von Online-Inhalten und dem Betreiber des Werbenetzwerks die Rollen und Verantwortungen beider Parteien im Rahmen ihrer in dem Vertrag beschriebenen Zusammenarbeit niedergelegt werden.

[30] Stellungnahme 1/2010 zum Begriff „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

In Bezug auf Werbetreibende:

Wenn eine betroffene Person eine Werbung anklickt und die Website des Werbetreibenden besucht, kann dieser nachverfolgen, welche Kampagne zu dem Anklicken der Werbung im Internet geführt hat. Wenn der Werbetreibende die Zielinformationen (z. B. bestimmte demographische Daten wie „junge Mütter" oder Interessengruppen wie „Extremsportanhänger") erfasst, und diese mit dem Internet-Surfverhalten der betroffenen Person oder den Registrierungsdaten verknüpft, ist der Werbetreibende für diesen Teil der Datenverarbeitung ein unabhängiger für die Verarbeitung Verantwortlicher.

Diese Stellungnahme legt den Schwerpunkt auf die Tätigkeiten der Datenverarbeitung, die von Betreibern von Werbenetzwerken und von Anbietern von Online-Inhalten ausgeübt werden und im Einblenden gezielter Werbung beruhen. Sie nimmt nicht Stellung zu den möglichen zusätzlichen Datenverarbeitungsoperationen, die möglicherweise durch die oben genannten Werbetreibenden ausgeführt werden können.

4. Verpflichtung zur vorherigen Einholung der Einwilligung in Kenntnis der Sachlage

Die allgemeine Vorschrift im ersten Abschnitt von Artikel 5 Absatz 3 verpflichtet die Mitgliedstaaten dazu, „[sicherzustellen], *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*". Dieser Artikel wurde bei der Änderung der Datenschutzrichtlinie für elektronische Kommunikation im Jahr 2009 geändert. Die Änderungen in der geänderten Fassung stellen das Erfordernis der vorherigen Einwilligung des Nutzers in Kenntnis der Sachlage klar und verstärken es[31]. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass die unten stehende rechtliche Analyse sowohl für die aktuelle Fassung von Artikel 5 Absatz 3 einschlägig und gültig ist, als auch für die geänderte Fassung von Artikel 5 Absatz 3.

Der folgende Abschnitt zeigt verschiedene Möglichkeiten auf, wie die Verpflichtungen aus Artikel 5 Absatz 3 erfüllt werden können. Nach einer Erörterung der Einwilligung gibt die Stellungnahme eine Orientierungshilfe zur Informationspflicht.

[31] Dies wird auf zwei Arten gemacht: Erstens, indem die Wörter „Recht, diese Verarbeitung zu verweigern" durch das Erfordernis zur Einholung der „Einwilligung" gemäß Richtlinie 95/46/EG ersetzt werden und zweitens durch die Verwendung der Worte „auf der Grundlage von".

4.1. Die Verpflichtung zur Einholung der vorherigen Einwilligung der betroffenen Personen im Fall von Werbung auf Basis von Behavioural Targeting

Gemäß Artikel 5 Absatz 3 ist einem Betreiber eines Werbenetzwerks die Speicherung von Informationen oder der Zugriff auf Informationen, die im Endgerät des Nutzers gespeichert sind, gestattet, wenn er: *i)* dem Nutzer gemäß Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung gegeben hat und *ii)* die Einwilligung des Nutzers zur Speicherung von Informationen oder zum Zugriff auf Informationen in seinem Endgerät erhalten hat, nachdem der Betreiber des Werbenetzwerks die unter *i)* geforderten Informationen erteilt hat.

Aus dem Wortlaut von Artikel 5 Absatz 3 ergibt sich, dass: *i)* die Einwilligung eingeholt werden muss, *bevor* der Cookie platziert wird und/oder auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden, was üblicherweise als vorherige Einwilligung bezeichnet wird und *ii)* eine Einwilligung in Kenntnis der Sachlage nur dann eingeholt werden kann, wenn *dem Nutzer* vorher Informationen über das Versenden und die Zwecke des Cookies *erteilt wurden*. In diesem Zusammenhang muss berücksichtigt werden, dass eine Einwilligung ungeachtet der jeweiligen Umstände, nur dann gültig ist, wenn sie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt ist. Die Einwilligung muss vor Erhebung der personenbezogenen Daten eingeholt werden, damit die betroffenen Personen voll und ganz erkennen, dass sie einwilligen und in was sie einwilligen. Darüber hinaus muss eine Einwilligung zurückziehbar sein.

In den nächsten Unterabschnitten wird analysiert, ob eine Einwilligung über Browser-Einstellungen oder über Opt-out-Optionen des Betreibers eines Werbenetzwerks den Anforderungen von Artikel 5 Absatz 3 entspricht.

4.1.1. Einwilligung über die Browser-Einstellungen

Anbieter von Online-Inhalten und Betreiber von Werbenetzwerken, die im Bereich der Werbung auf Basis von Behavioural Targeting tätig sind, platzieren Tracking-Cookies auf den Endgeräten der betroffenen Personen, wenn diese eine Website besuchen, die Teil des Werbenetzwerks ist. Dies ist der Fall, wenn der Browser des Nutzers nicht so eingestellt ist, dass er Cookies ablehnt. Sobald der Cookie platziert ist und die betroffene Person auf der Internetseite mit der Werbung surft, wird es ihr in der Praxis ermöglicht, Wissen über die Cookies zu erlangen und darüber, wie der Browser eingestellt werden muss, um diese zu kontrollieren. Diese Informationen werden durch die Anbieter von Online-Inhalten und die Betreiber von Werbenetzwerken erteilt. Diese für die Verarbeitung Verantwortlichen erteilen die Informationen üblicherweise in ihren allgemeinen Geschäftsbedingungen und/oder in ihren Datenschutzvorschriften über Third-Party-

Cookies, die für Werbung auf Basis von Behavioural Targeting verwendet werden. Die Informationen können die grundlegenden Verwendungen/Zwecke dieser Cookies umfassen und Angaben darüber, wie sie mit Hilfe der Browser-Einstellungen vermieden werden können. Diese Praxis entspricht den Anforderungen von Artikel 5 Absatz 3 jedoch nicht; insbesondere nicht in seiner geänderten Fassung, welche die Betonung auf die vorherige Erteilung von Information und die vorherige Einholung der Einwilligung legt (vor Beginn der Verarbeitung).

Erwägungsgrund 66 der geänderten Datenschutzrichtlinie für elektronische Kommunikation weist darauf hin, dass die Einwilligung des Nutzers auch über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung, „*wenn es technisch durchführbar und wirksam ist, […] im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG*“ ausgedrückt werden kann. Dies stellt keine Ausnahme von Artikel 5 Absatz 3 dar, sondern ist eher eine Erinnerung daran, dass eine Einwilligung in dieser technologischen Umgebung auf verschiedene Arten erteilt werden kann – wenn es technisch durchführbar und wirksam ist und im Einklang mit den entsprechenden sonstigen Bedingungen für eine gültige Zustimmung steht. In diesem Zusammenhang ist es wichtig, die Bedingungen zu bestimmen, unter denen die Browser-Einstellungen den Anforderungen von Richtlinie 95/46/EG entsprechen und damit eine gültige Einwilligung „*im Einklang mit Richtlinie 95/46/EG*“ darstellen. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass dies aus den folgenden Gründen nur unter sehr eingeschränkten Umständen der Fall ist:

Erstens, basierend auf der Definition und den Bedingungen für eine gültige Einwilligung *gemäß* Artikel 2 Buchstabe h der Richtlinie 95/46/EG, kann man allgemein gesprochen nicht einfach davon ausgehen, dass eine betroffene Person ihre Einwilligung gegeben hat, nur weil sie einen Browser oder eine andere Anwendung erworben/verwendet hat, die die Sammlung und Verarbeitung von Informationen standardmäßig ermöglicht. Der durchschnittlichen betroffenen Person sind die Verfolgung ihres Internet-Verhaltens, die Zwecke der Verfolgung usw. nicht bewusst. Sie weiß nicht unbedingt, wie Cookies mit Hilfe von Browser-Einstellungen abgelehnt werden können, selbst wenn dies in den Datenschutzvorschriften niedergelegt ist. Es ist ein Trugschluss, davon auszugehen, dass die Untätigkeit einer betroffenen Person (sie hat den Browser nicht so eingestellt, dass er Cookies ablehnt), generell einen klaren und eindeutigen Hinweis auf ihre Wünsche darstellt. Wie in der vorgenannten Stellungnahme 1/2008 der Artikel-29-Arbeitsgruppe dargelegt wurde, „*Die Verantwortung für deren [Cookie] Verarbeitung kann nicht auf die Verantwortung des Benutzers reduziert werden, bestimmte Vorsichtsmaßnahmen in seinen Browser-Einstellungen zu treffen*“. Von den vier wichtigsten Browsern blockiert derzeit nur einer standardmäßig Third-Party-Cookies, sobald der Browser installiert wurde. Bei den drei anderen großen Browsern lässt die Standard-Einstellung alle Cookies zu. In diesen Fällen werden die Cookies versendet und die Informationen vor der Einholung einer Einwilli-

gung gesammelt. Diese Vorgehensweise steht folglich mit der Erfordernis der vorherigen Einwilligung im Widerspruch[32].

Zweitens, wenn eine Einwilligung in Kenntnis der Sachlage über die Browser-Einstellung möglich sein soll, darf es nicht möglich sein, die Wahl der betroffenen Person zu „umgehen", die sie bei der Einstellung des Browsers getroffen hat. In der Praxis ist das „Respawnen" gelöschter Cookies durch sogenannte Flash-Cookies jedoch leicht möglich, was dem Betreiber von Werbenetzwerken die Möglichkeit gibt, den Nutzer weiterhin zu überwachen. Die Verfügbarkeit und die steigende Verwendung solcher Technologien stellt eine Herausforderung an die Browser-Einstellungen dar, eine gültige, wirksame Einwilligung in Kenntnis der Sachlage einzuholen.

Schließlich, eine Einwilligung in die Annahme von Cookies in großen Mengen auf Grund der Browser-Einstellungen impliziert, dass der Nutzer eine zukünftige Verarbeitung akzeptiert, möglicherweise, ohne die Zwecke oder die Verwendung der Cookies zu kennen. Eine Einwilligung in großem Umfang für zukünftige Verarbeitungen ohne Kenntnis der Umstände der Verarbeitung kann keine gültige Einwilligung darstellen[33].

Damit Browser oder andere Anwendungen eine gültige Einwilligung „erteilen" können, müssen die oben dargelegten Probleme gelöst werden. Das heißt, dass:

(a) Browser oder andere Anwendungen, die Third-Party-Cookies standardmäßig ablehnen und die eine positiv bejahende Handlung der betroffenen Person benötigen, um sowohl die Einstellung der Cookies als auch die fortdauernde Übermittlung von Informationen zu akzeptieren, die auf den Cookies bestimmter Websites gespeichert sind, könnten einer gültigen und wirksamen Einwilligung entsprechen. Bei Browser-Einstellungen dagegen, die so festgelegt sind, dass sie alle Cookies annehmen, würde die Einwilligung den Anforderungen von Artikel 5 Absatz 3 nicht entsprechen, da eine solche Einwilligung keine wirkliche Willensbekundung der betroffenen Person wäre.

---

32 Eine weitere Komplikation ergibt sich daraus, dass die drei vorgenannten Browser selbst dann bestehende Cookie-Informationen weiterversenden, wenn der Browser so eingestellt wurde, dass er (neue) Third-Party-Cookies ablehnt. Anders ausgedrückt, die Informationen von Cookies, die platziert wurden, bevor der Browser auf Ablehnung von Cookies eingestellt wurde, werden dem Betreiber von Werbenetzwerken weiterhin zugesandt. Derzeit ermöglicht es lediglich einer der großen Browser, sowohl die Einstellung alsauch die Übermittlung der Daten von Third-Party-Cookies (also einschließlich das Cookies, die platziert wurden, bevor der Browser auf Ablehnung von Cookies eingestellt wurde), zu blockieren. Folglich können auch Cookies, die als First-Party-Cookie (beim Besuchen einer einzelnen Website beispielsweise oder einer Suchmaschine oder der Site eines sozialen Netzwerks) einstellt wurden, auch dann noch durch die Site gelesen werden, wenn der Nutzer eine Site besucht, die mit der ersten Website eine Partnerschaft eingegangen ist.

33 Wie in dem Arbeitspapier der Artikel-29-Arbeitsgruppe über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der europäischen Richtlinie 95/46/EG vom 24. Oktober 1995, angenommen am 25.11.2005 im Zusammenhang mit der zukünftigen Datenübermittlung niedergelegt wurde: „Dadurch, dass eine ausdrückliche vorherige Willensbekundung verlangt wird, wird faktische eine Regelungausgeschlossen, bei der sich eine Person erst gegen die Übermittlung aussprechen kann, nachdem sie bereits stattgefunden hat: die Einholung der Einwilligung für den konkreten Fall, bevor eine Übermittlung stattfinden kann, ist konkret vorgeschrieben".

Eine solche Einwilligung würde weder den konkreten Fall betreffen, noch würde sie vorher (vor der Verarbeitung) erfolgen. Auch wenn eine bestimmte betroffene Person tatsächlich entschieden haben könnte, dass sie die Einstellung zur Annahme aller Third-Party-Cookies beibehalten will, wäre es nicht realistisch, wenn Betreiber von Werbenetzwerken davon ausgingen, dass die große Mehrheit der betroffenen Personen, die ihre Browser so eingestellt haben, dass sie Cookies annehmen, diese Wahl tatsächlich getroffen haben.

(b) Browser, zusammen oder in Verbindung mit anderen Informationsmitteln, einschließlich der Kooperation zwischen Betreibern von Werbenetzwerken und Anbietern von Online-Inhalten sollten klare, umfassende und vollständig sichtbare Informationen erteilen, um sicherzustellen, dass die Einwilligung in voller Kenntnis der Sachlage erfolgt. Damit die Bedingungen von Artikel 5 Absatz 3 der Richtlinie 95/46/EG erfüllt werden, müssen die Browser im Namen der Betreiber von Werbenetzwerken zweckdienliche Informationen über die Zwecke der Cookies und die weitere Verarbeitung übermitteln. Allgemeine Warnungen ohne einen genauen Hinweis auf das Werbenetzwerk, welches den Cookie platziert, sind folglich nicht ausreichend.

Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass eine Einwilligung nicht als in Kenntnis der Sachlage im Sinne von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation und angesichts von Artikel 2 Buchstabe h der Richtlinie 95/46/EG erteilt gelten kann, sofern die oben genannten Bedingungen zur Erteilung von Informationen nicht erfüllt sind und es dem Nutzer nicht erleichtert wird, Cookies abzulehnen (indem erklärt wird, wie dies getan werden kann).

Angesichts der Bedeutung von Browser-Einstellungen bei der Gewährleistung, dass betroffene Personen ihre Einwilligung in die Speicherung von Cookies und in die Verarbeitung ihrer Informationen wirksam geben, scheint es von größter Bedeutung zu sein, dass Browser standardmäßig über Datenschutz-Einstellungen verfügen. Anders ausgedrückt sollten sie die Einstellung „keine Annahme und keine Übermittlung von Third-Party-Cookies“ haben. Zur Vervollständigung und für eine größere Effizienz, sollten die Browser so eingestellt sein, dass Nutzer vor der Installation des Browser oder dem Herunterladen eines Updates von einem Assistenten durch ein Datenschutz-Programm geführt werden. Außerdem sollten Browser es den Nutzern ermöglichen, Wahlmöglichkeiten auf einfache Weise während der Nutzung des Browsers wahrzunehmen. Die Artikel-29-Arbeitsgruppe fordert die Entwickler von Browsern dazu auf, schnell in Aktion zu treten und sich mit den Betreibern von Werbenetzwerken abzusprechen.

4.1.2. Einwilligung und die Ausübung von Opt-out-Optionen

Betreiber von Werbenetzwerken bieten in steigendem Maße „Opt-out“-Mechanismen an, die es Nutzern ermöglichen, sich gegen den Erhalt von gezielter Wer-

bung zu entscheiden[34]. In dem Fall muss die betroffene Person auf die Website des/der Betreiber(s) des Werbenetzwerks gehen und ihm/ihnen gegenüber angeben, dass sie nicht wünscht, für Zwecke der gezielten Werbung verfolgt zu werden. Mit diesen Mechanismen sollen die vorgenannten Probleme bezüglich der Einwilligung durch Browser-Einstellungen bis zu einem gewissen Grad behoben werden.

Solche Cookie-basierten Opt-out-Mechanismen werden insoweit begrüßt und gefördert, als sie die aktuellen technischen Möglichkeiten der Nichtbeteiligung der betroffenen Personen erleichtern. Sie stellen jedoch nicht prinzipiell eine Einwilligung der betroffenen Person dar. Lediglich in sehr spezifischen Einzelfällen könnte eine implizierte Einwilligung argumentiert werden. Dies könnte der Fall sein, wenn ein erfahrener Nutzer, dem die Praxis der Werbung auf Basis von Behavioural Targeting bekannt ist und der weiß, dass er die Möglichkeit des Opt-out hat, sich dennoch willentlich gegen das Opt-out entscheidet (insbesondere, wenn er dies tut, bevor ihm ein Cookie zugesandt wurde). Dieser Mechanismus ist jedoch keine angemessene Weise zur Einholung der Einwilligung des durchschnittlichen Nutzers. Die Gründe ähneln denjenigen, die im Zusammenhang mit den Browser-Einstellungen genannt wurden:

Erstens fehlt Nutzern im Allgemeinen das grundlegende Verständnis für die Datenerhebung, für die Verwendung der Daten, für die entsprechende Technologie und noch wichtiger dafür wo und wie sie sich dagegen entscheiden können. Folglich nutzen nicht deshalb so wenige Personen die Opt-out-Option, weil sie sich in Kenntnis der Sachlage für eine Einwilligung in Werbung auf Basis von Behavioural Targeting entschieden haben, sondern weil ihnen nicht bewusst ist, dass sie bereits dadurch einwilligen, dass sie keinen Gebrauch von dem Opt-out machen.

Zweitens bedeutet Einwilligung eine aktive Teilnahme der betroffenen Person vor der Erhebung und Verarbeitung der Daten. Die Opt-out-Mechanismen bedeuten häufig eine „Nicht"-Reaktion der betroffenen Person, nachdem eine solche Verarbeitung bereits begonnen hat. Darüber hinaus gibt es unter den Opt-out-Mechanismen keine aktive Teilnahme. Der Wunsch der betroffenen Person wird lediglich angenommen oder impliziert. Das entspricht aber nicht den Anforderungen an eine rechtlich wirksame Einwilligung.

Angesichts des oben Stehenden ist die Artikel-29-Arbeitsgruppe der Ansicht, dass Cookiebasierte Opt-out-Mechanismen dem durchschnittlichen Nutzer kein wirksames Mittel in die Hand geben, in die Werbung auf Basis von Behavioural Targeting einzuwilligen. In dieser Hinsicht entsprechend sie nicht den Anforderungen von Artikel 5 Absatz 3.

[34] Siehe beispielsweise die Opt-out-Option der Network Advertising Initiative, welche die Möglichkeit des Opt-out von verschiedenen Netzwerken bietet: http://www.networkadvertising.org/managing/opt_out.asp

4.1.3. Vorherige Mechanismen der Einwilligung durch Opt-in sind besser für eine Einwilligung in Kenntnis der Sachlage geeignet

Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass Opt-in-Mechanismen, die eine positive bejahende Handlung der betroffenen Person erforderlich machen, um ihre Einwilligung anzuzeigen, bevor der Cookie an die betroffene Person gesendet wird, Artikel 5 Absatz 3 mehr entsprechen. In Bezug auf die Einwilligung als Rechtsgrundlage für die Verarbeitung hat die Artikel-29-Arbeitsgruppe diese Ansicht kürzlich bestätigt: „*Die technologischen Entwicklungen fordern auch eine genaue Erwägung der Einwilligung. In der Praxis wird Artikel 7 der Richtlinie 95/46/EG nicht immer richtig angewendet. Dies ist insbesondere im Umfeld des Internet der Fall, wo eine stillschweigende Einwilligung nicht immer zu einer eindeutigen Einwilligung führt (wie dies in Artikel 7 Buchstabe a der Richtlinie gefordert wird). Wenn die Position der betroffenen Person jedoch ‚ex ante', also vor der Verarbeitung ihrer personenbezogenen Daten durch Dritte, gestärkt wird, muss die Einwilligung ausdrücklich (und deshalb ein Opt-in) für alle Verarbeitungen erfolgen, die auf der Einwilligung basieren.*"[35]

In einer früheren Stellungnahme[36], in der diese Fragestellung behandelt wurde, hat die Arbeitsgruppe die Verwendung spezieller Mitteilungen empfohlen: „*Bei Cookies, dass der Benutzer darüber unterrichtet wird, wenn … ein Cookie empfangen, speichern oder senden will. Diese Mitteilung sollte in allgemein verständlicher Sprache erklären, welche Information zu welchem Zweck in diesem Cookie gespeichert werden soll und wie lange das Cookie gilt.*" Nachdem die betroffene Person diese Mitteilung erhalten hat, sollte sie die Möglichkeit haben, anzugeben, ob sie für die Zwecke der Werbung auf Basis von Behavioural Targeting die Erstellung eines Profils wünscht.

Der Artikel-29-Arbeitsgruppe sind die derzeitigen praktischen Probleme im Hinblick auf die Einholung der Einwilligung bewusst, insbesondere, wenn die Einwilligung jedes Mal erforderlich ist, wenn ein Cookie für Zwecke der gezielten Werbung gelesen wird. Zur Vermeidung dieses Problems und in Übereinstimmung mit Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation („*… das Ablehnungsrecht [Cookies] können einmalig für die Nutzung verschiedener in dem Endgerät des Nutzers … zu installierender Instrumente angeboten werden und auch die zukünftige Verwendung derartiger Instrumente umfassen*"), kann die Einwilligung in den Cookie als Einwilligung nicht nur in das Versenden des Cookies als gültig betrachtet werden, sondern auch in die daraus folgende, sich aus dem Cookie ergebende Datenerhebung. Anders ausgedrückt würde die Einwilligung in das Platzieren des Cookies und in die Verwendung der Informa-

35 Die Artikel-29-Arbeitsgruppe erkennt die Arbeiten einiger Gruppen wie The Future of Privacy an, welche sich für die Verwendung von Icons für Informationszwecke einsetzen.

36 Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17en.pdf.

tionen zum Versand gezielter Werbung das folgende „Lesen" des Cookies einschließen, das jedes Mal stattfindet, wenn der Nutzer einen Website-Partner des Betreibers des Werbenetzwerks besucht, der den Cookie ursprünglich platziert hat.

Unter Berücksichtigung jedoch, dass *i)* diese Praxis bedeuten würde, dass Personen einwilligen „für immer" überwacht zu werden und *ii)* sie einfach „vergessen" könnten, dasssie beispielsweise vor einem Jahr in die Überwachung eingewilligt haben, ist die Artikel-29-Arbeitsgruppe der Ansicht, dass einige Schutzmechanismen integriert werden sollten. Die Artikel-29-Arbeitsgruppe schlägt insbesondere drei Vorgehensweisen vor:

Erstens eine zeitliche Einschränkung der Geltungsdauer der Einwilligung. Die Einwilligung in eine Überwachung sollte nicht „für immer", sondern nur für einen begrenzten Zeitraum gültig sein, z. B. für ein Jahr. Nach Ablauf dieser Frist müssten die Betreiber von Werbenetzwerken eine neue Einwilligung einholen. Dies könnte erreicht werden, indem Cookies nur eine begrenzte Lebensdauer haben, nachdem sie auf dem Endgerät des Nutzers platziert wurden (das Ablaufdatum sollte nicht verlängert werden).

Zweitens würden die dargelegten Risiken durch zusätzliche Informationen weiter abgeschwächt werden. Darauf wird weiter unten in Abschnitt 4.2.1 eingegangen.

Drittens kann eine freiwillig erteilte Einwilligung jederzeit zurückgezogen werden. Die betroffenen Personen sollten die Möglichkeit haben, ihre Einwilligung in eine Überwachung für Zwecke der Werbung auf Basis von Behavioural Targeting einfach zurückzuziehen. In dieser Hinsicht ist die Verpflichtung, klare Informationen über diese Möglichkeit zu erteilen, von grundlegender Bedeutung (siehe unten unter Abschnitt 4.2).

Die Artikel-29-Arbeitsgruppe fordert die Werbe-Industrie zur Umsetzung des oben Stehenden oder zur Einführung alternativer Methoden auf, die Folgendes beinhalten: eine vorherige positiv bejahende Handlung der Nutzer in Bezug auf eine Einwilligung i) in die Speicherung des Cookies und ii) in die Verwendung des Cookies, um ihn über die Websites hinweg für die Einblendung von Werbung auf Basis von Behavioural Targeting zu verfolgen. Die Methoden können auch die Gestaltung des Browser und der Browser-Technologie betreffen.

4.1.4. Einwilligung in Kenntnis der Sachlage: Kinder

In der Stellungnahme 2/2009 hat sich die Artikel-29-Arbeitsgruppe mit dem Schutz der personenbezogenen Daten von Kindern[37] befasst. Die Probleme in

[37] Stellungnahme zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf

Bezug auf die Einholung einer Einwilligung in Kenntnis der Sachlage werden weiter verstärkt, wenn Kinder betroffen sind. Zusätzlich zu den oben (und unten) dargelegten Bedingungen für eine gültige Einwilligung, muss die Einwilligung von Kindern in manchen Fällen von ihren Eltern oder sonstigen gesetzlichen Vertretern erteilt werden, um gültig zu sein. In dem Fall heißt das, dass die Betreiber von Werbenetzwerken die Eltern darüber informieren müssten, dass sie Informationen über die Kinder erheben und verwenden und die Einwilligung vor der Erhebung und weiteren Verwendung der Informationen für Zwecke des Behavioural Targeting bei Kindern, einholen.[38].

Angesichts des oben Stehenden und unter Berücksichtigung der Verwundbarkeit von Kindern ist die Artikel-29-Arbeitsgruppe der Ansicht, dass Betreiber von Werbenetzwerken keine Interessenkategorien für Zwecke der Werbung auf Basis von Behavioural Targeting oder zur Beeinflussung von Kindern anbieten sollten.

4.2. Die Informationspflicht im Zusammenhang mit Werbung auf Basis von Behavioural Targeting

Transparenz ist eine Schlüsselvoraussetzung dafür, dass natürliche Personen in die Erhebung und weitere Verarbeitung ihrer Daten einwilligen können. Wie oben dargelegt wurde, ist es möglich, dass die Nutzer in Bezug auf Werbung auf Basis von Behavioural Targeting die Technologie hinter der Werbung auf Basis von Behavioural Targeting nicht kennen oder nicht verstehen oder nicht einmal wissen, dass sie gezielt mit solchen Arten der Werbung bedient werden. Es ist deshalb von größter Wichtigkeit, dass eine ausreichende und wirksame Informierung sichergestellt wird, die die Internet-Nutzer erreicht. Die betroffenen Personen können nur dann ihre Wahl treffen, wenn sie informiert sind.

4.2.1. Welche Informationen müssen gegeben werden und von wem?

Artikel 5 Absatz 3 legt fest, dass der Nutzer Informationen „*gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitungen*“ erhält. Artikel 10 der Richtlinie 95/46/EG betrifft die Bereitstellung dieser Informationen.[39]

In Bezug auf Werbung auf Basis von Behavioural Targeting sollten die betroffenen Personen *unter anderem* über die Identität des Betreibers des Werbenetzwerks und über die Zweckbestimmungen der Verarbeitung informiert werden.

---

[38] Dies ist zusätzlich zu den geltenden Rechtsvorschriften und Normen im Bereich der Werbung.

[39] Es wird insbesondere die Bereitstellung der folgenden Informationen gefordert: die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung sowie die Empfänger der Daten und das Vorliegen des Auskunftsrechts insoweit als solche weiteren Informationen erforderlich sind, um eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Die betroffene Person sollte klare Informationen darüber erhalten, dass der Cookie es dem Betreiber des Werbenetzes ermöglicht, Informationen über Besuche auf anderen Websites, über die ihnen gezeigte Werbung, die angeklickte Werbung, die Zeitwahl usw. zu sammeln.

Die Verwendungen des Cookies zur Erstellung von Profilen zum Zwecke der Bereitstellung gezielter Werbung sollten einfach verständlich erklärt werden. Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation verlangt, dass Mitteilungen auf „klare und umfassende" Weise gemacht werden. Aussagen wie „Werbetreibende und sonstige Dritte können auch ihre eigenen Cookies oder Action Tags verwenden" sind eindeutig unzureichend.

In Bezug auf die Art der Informationserteilung verlangt Erwägungsgrund 25, dass sie „*so benutzerfreundlich wie möglich*" ist. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass das interaktive Anzeigen eines Minimums an Informationen auf leicht sichtbare und verständliche Weise direkt auf dem Bildschirm der wirkungsvollste Weg wäre, diesen Grundsatz einzuhalten[40]. Es ist wichtig, dass die Informationen leicht zugänglich und sehr gut sichtbar sind. Diese grundlegenden Informationen dürfen nicht in den allgemeinen Geschäftsbedingungen und Datenschutzvorschriften versteck werden.

Die Artikel-29-Arbeitsgruppe erkennt an, dass es technisch gesehen, verschiedene Wege der Informationserteilung geben mag und begrüßt Kreativität in diesem Bereich. Sie ist sich bewusst, dass einige der Betreiber von Werbenetzwerken mit der Entwicklung neuer Wege zur Bereitstellung von Informationen begonnen haben und begrüßt dies. Ein Beispiel für solche Entwicklungen, die die Arbeitsgruppe sowohl positiv als auch notwendig findet, sind Icons, die auf der Website des Anbieters von Online-Inhalten rund um die Werbung platziert werden und Links zu weiteren Informationen bereitstellen.

Unter Berücksichtigung der in Abschnitt 4.1.3 dargelegten Möglichkeit für natürliche Personen, einmalig in die Überwachung einzuwilligen und damit auch in das zukünftige Ablesen des Cookies, findet es die Artikel-29-Arbeitsgruppe sehr wichtig, dass Betreiber von Werbenetzwerken Wege finden, die Personen *in regelmäßigen Abständen* über die Überwachung zu informieren. Wenn die betroffenen Personen nicht auf klare und eindeutige Weise und mit Hilfe einfacher Mittel an die Überwachung erinnert werden, ist es sehr wahrscheinlich, dass es ihnen nach einer Weile nicht mehr bewusst ist, dass die Überwachung weiterhin stattfindet und dass sie in diese eingewilligt haben. Diesbezüglich würde es die Arti-

[40] Dies entspricht der vorherigen Stellungnahme der Artikel-29-Arbeitsgruppe, siehe Empfehlung WP 43 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, angenommen am 17. Mai 2001, verfügbar unter:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf

kel-29-Arbeitsgruppe sehr unterstützen, wenn ein Symbol und damit verbundene Nachrichten die Konsumenten darauf aufmerksam machen würden, dass ein Betreiber eines Werbenetzwerks ihr Internet-Surf-Verhalten zur Einblendung gezielter Werbung überwacht. Dieses Symbol wäre sehr hilfreich, nicht nur um natürliche Personen an die Überwachung zu erinnern, sondern auch um zu kontrollieren, ob sie weiter überwacht werden oder ob sie ihre Einwilligung zurückziehen wollen.

Eine weitere einschlägige Frage ist *wer die Informationen bereitstellen sollte* – sollte es Aufgabe des Anbieters von Online-Inhalten oder des Betreibers eines Werbenetzwerks sein oder die Aufgabe von beiden? Als Ergebnis sollten die betroffenen Personen leicht zugängliche und gut sichtbare Informationen erhalten. Wie weiter dargelegt wird, scheint hierfür die Zusammenarbeit zwischen dem Anbieter von Online-Inhalten und dem Betreiber des Werbenetzwerks von grundlegender Bedeutung zu sein.

Die Artikel-29-Arbeitsgruppe merkt an, dass gemäß dem Wortlaut von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation die den Cookie versendende und ablesende Stelle zur Bereitstellung der erforderlichen Informationen und zur Einholung der Einwilligung der betroffenen Person verpflichtet ist. Wenn Anbieter von Online-Inhalten gemeinsam für die Verarbeitung Verantwortliche sind, z. B. wenn sie direkt identifizierbare Informationen an Betreiber von Werbenetzwerken senden, sind sie auch dazu verpflichtet, die betroffenen Personen über die Datenverarbeitung zu informieren.

Wie in Abschnitt 3.3 angemerkt wurde, teilen Anbieter von Online-Inhalten die Verantwortung für die Datenverarbeitung, die im Zusammenhang mit dem Einblenden von Werbung auf Basis von Behavioural Targeting steht, darüber hinaus mit den Betreibern von Werbenetzwerken. Genauer gesagt, deckt diese Verantwortung den ersten Teil der Verarbeitung ab, also die Übermittlung der IP-Adresse an den Betreiber eines Werbenetzwerks, der dann stattfindet, wenn eine Person die Website des Anbieters von Online-Inhalten besucht und auf die Website des Betreibers des Werbenetzwerks umgeleitet wird.

Als Ergebnis dieser Verantwortung haben Anbieter von Online-Inhalten bestimmte Verpflichtungen gegenüber den betroffenen Personen, die sich in erster Linie aus der Richtlinie 95/46/EG[41] ergeben. Die Artikel-29-Arbeitsgruppe ist insbesondere der Ansicht, dass die Anbieter von Online-Inhalten durch die Ver-

[41] Darüber hinaus merkt die Artikel-29-Arbeitsgruppe an, dass die Anbieter von Online-Inhalten auch aus allgemeinen Rechtsgrundsätzen (Vertrags- und Deliktsrechts) und aus verbraucherschutzrechtlichen Vorschriften zwischen Unternehmen und Verbrauchern für die Informierung natürlicher Personen verantwortlich sind, insoweit als die Datenverarbeitung und die Überwachung als Ergebnis der Umleitung an den Betreiber von Werbenetzwerken erfolgt.

pflichtung gebunden sind, die betroffenen Personen über die Datenverarbeitung zu informieren, die als Ergebnis der Umleitung ihrer Browser stattfindet und über die Zwecke, für die diese Information später durch die Betreiber des Werbenetzwerks verwendet werden. Die Information sollte sich nicht nur auf die Übermittlung der IP-Adresse für die Zwecke der Einblendung von Werbung beziehen, sondern auch auf die weitere Datenverarbeitung, die durch die Betreiber von Online-Werbenetzwerken vorgenommen wird. Hierzu zählt auch das Speichern von Cookies.

Die Artikel-29-Arbeitsgruppe schlägt natürlich nicht vor, dass Informationen zweimal erteilt werden müssen (einmal durch den Betreiber des Online-Werbenetzwerks und dann durch den Anbieter von Online-Inhalten). Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass in diesem Bereich ein eindeutiger Bedarf an Zusammenarbeit zwischen den Betreibern von Werbenetzwerken und den Anbietern von Online-Inhalten vorliegt. Sie sollen entscheiden, durch wen und wie die Informationen erteilt werden. Die Artikel-29-Arbeitsgruppe fordert folglich die Betreiber von Werbenetzwerken und die Anbieter von Online-Inhalten dazu auf, keine Anstrengung zu scheuen, um wirksame Mitteilungen bereitzustellen und unter Internet-Nutzern den größten Wissensstand darüber zu gewährleisten, wie Werbung auf Basis von Behavioural Targeting in jeder bestimmten Situation funktioniert. Der Bedarf an diesem Zusammenspiel wird weiter unterstrichen, wenn man bedenkt, dass die Betreiber von Werbenetzwerken üblicherweise für die betroffenen Personen unsichtbar sind. Die Interaktion der Nutzer findet stattdessen mit der besuchten Website statt, also mit der Website des Anbieters von Online-Inhalten. Aus diesem Grund ist es aus der Sicht der Nutzer der direktere Weg, wenn sie eine Mitteilung von der Website des Anbieters von Online-Inhalten erhalten. Dies kann auf unterschiedliche Weise geschehen; beispielsweise wenn der Anbieter von Online-Inhalten Platz auf seiner Website bereitstellt, auf dem die Betreiber von Werbenetzwerken die erforderlichen Informationen einstellen können.

Die Datenschutz-Behörden werden bei der Ausübung ihrer Tätigkeit angemessene Sensibilisierungsmaßnahmen zu diesen Praktiken und den entsprechenden Rechten der betroffenen Personen berücksichtigen.

5. Sonstige Verpflichtungen und Grundsätze im Sinne der Richtlinie 95/46/EG

Zusätzlich zu Artikel 5 Absatz 3 müssen die für die Datenverarbeitung Verantwortlichen die Einhaltung aller Verpflichtungen aus Richtlinie 957/46/EG gewährleisten, die sich nicht mit Artikel 5 Absatz 3 überschneiden. Sie müssen unter anderem Folgendes sicherstellen:

5.1. Verpflichtungen bezüglich besonderer Kategorien personenbezogener Daten

Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugen oder die Gewerkschaftszugehörigkeit hervorgehen sowie Daten über Gesundheit oder Sexualleben gelten gemäß Artikel 8 der Richtlinie 95/46/EG als sensible Daten. Die Artikel-29-Arbeitsgruppe sieht als große Gefahr eine mögliche Verletzung der Rechte in Bezug auf die personenbezogenen Daten natürlicher Personen, wenn diese Art von Informationen für die Zwecke der Werbung auf Basis von Behavioural Targeting genutzt werden. Jedes mögliche auf sensiblen Daten beruhende Targeting der betroffenen Personen, eröffnet die Möglichkeit für Missbrauch. Darüber hinaus sollte angesichts der Sensibilität solcher Informationen und der möglicherweise peinlichen Situationen, die sich daraus ergeben können, dass natürliche Personen Werbung erhalten, die beispielsweise ihre sexuellen Vorlieben oder politischen Aktivitäten offenlegen, das Anbieten/die Verwendung von Interessenkategorien entmutigt werden, die sensible Daten offenlegen.

Wenn Betreiber von Werbenetzwerken aber dennoch Interessenkategorien anbieten und verwenden, die sensible Daten offenlegen, müssen sie Artikel 8 der Richtlinie 95/46/EG einhalten. Wenn ein Betreiber eines Werbenetzwerks beispielsweise das Verhalten einer natürlichen Personen verarbeitet, um sie in eine Interessenkategorie zu „platzieren", die ihre besonderen sexuellen Vorlieben angibt, würde er gemäß Artikel 8 der Richtlinie 95/46/EG sensible Daten verarbeiten. Der genannte Artikel verbietet die Verarbeitung sensibler Daten mit Ausnahme bestimmter, besonderer Umstände. In diesem Zusammenhang wäre die einzige mögliche Rechtsgrundlage, welche die Datenverarbeitung rechtmäßig machen würde, die vorherige Opt-in-Einwilligung *gemäß* Artikel 8 Absatz 2 Buchstabe a. Die Anforderung einer vorherigen Erteilung der Einwilligung durch die betroffene Person bedeutet, dass ein Mechanismus des Opt-out der Einwilligung auf keinen Fall den gesetzlichen Erfordernissen entsprechen würde. Es bedeutet auch, dass eine solche Einwilligung nicht durch die Browser-Einstellungen eingeholt werden könnte. Zur rechtmäßigen Erhebung und Verarbeitung dieser Art von Informationen müssten die Betreiber von Werbenetzwerken Mechanismen zur Einholung einer ausdrücklichen, vorherigen Einwilligung einrichten, die unabhängig von der sonstigen Einwilligung für die Verarbeitung im Allgemeinen ist.

5.2. Einhaltung der Grundsätze in Bezug auf die Qualität der Daten

Artikel 6 der Richtlinie 95/46/EG legt bestimmte Grundsätze fest, die durch den für die Datenverarbeitung Verantwortlichen eingehalten werden müssen. Hier sind die Folgenden von besonderer Bedeutung:

Es ist der Artikel-29-Arbeitsgruppe bewusst, dass Profile, die für Zwecke der Werbung auf Basis von Behavioural Targeting gesammelt und genutzt werden, potentiell für andere Zwecke als Werbung genutzt werden können. Sie könnten möglicherweise für die Entwicklung neuer Dienste verwendet werden, deren Natur bislang noch nicht bekannt ist.

Oben Stehendes hängt darüber hinaus von der Einhaltung von Artikel 6 Absatz 1 Buchstabe b ab, der den ***Zweckbegrenzungs-Grundsatz*** festlegt. Dieser Grundsatz verbietet die Verarbeitung personenbezogener Daten, die nicht mit den Zwecken vereinbar sind, die die ursprüngliche Erhebung rechtmäßig gemacht haben. Anders ausgedrückt würde die unvereinbare sekundäre Verwendung der für Zwecke der Werbung auf Basis von Behavioural Targeting gesammelten und gespeicherten Informationen gegen Artikel 6 Buchstabe b der Richtlinie 95/46/EG verstoßen. Wenn die Betreiber von Werbenetzwerken beispielsweise einer Unternehmensgruppe angehören, die vielfältige Dienste anbietet, kann der Betreiber des Werbenetzwerks die für Werbung auf Basis von Behavioural Targeting erhobenen Daten im Prinzip nicht für solche andere Dienste verwenden (sofern nicht nachgewiesen werden kann, dass die Zwecke vereinbar sind). Aus denselben Gründen dürfen die Betreiber von Werbenetzwerken die für Zwecke der Werbung auf Basis von Behavioural Targeting gesammelten Informationen nicht mit anderen Informationen anreichern.

Wenn Betreiber von Werbenetzwerken Informationen, die sie für Werbung auf Basis von Behavioural Targeting gesammelt haben, für sekundäre, unvereinbare Zwecke wie z. B. Across-Dienste, nutzen wollen, benötigen Sie *gemäß* Artikel 7 der Richtlinie 95/46/EC zusätzliche Rechtsgrundlagen. Folglich müssen sie die betroffenen Personen informieren und ihre Einwilligung *gemäß* Artikel 7 Buchstabe a einholen.

Artikel 6 Absatz 1 Buchstabe e schreibt vor, dass Daten gelöscht werden müssen, wenn sie für die Realisierung der Zwecke, für die sie erhoben wurden, nicht länger erforderlich sind. (***Speicherungsgrundsatz***). Die Einhaltung dieses Grundsatzes verlangt eine Einschränkung der Speicherungsdauer von Informationen. Entsprechend müssen Unternehmen genaue Zeitrahme nennen und auch einhalten, während derer die Daten gespeichert sind.

Demzufolge müssen Informationen über das Verhalten der Nutzer gelöscht werden, wenn sie nicht länger für das Erstellen eines Profils benötigt werden. Uneingeschränkte oder zu lange Speicherungsfristen verstoßen gegen Artikel 6 Absatz 1 Buchstabe e der Richtlinie. Die Artikel-29-Arbeitsgruppe hat festgestellt, dass die großen Betreiber von Werbenetzwerken unterschiedliche Speicherungsfristen haben. Manche haben uneingeschränkte Speicherungsfristen und andere begrenzen diese auf die Dauer von drei Monaten.

Also fordert die Artikel-29-Arbeitsgruppe die Betreiber von Werbenetzwerken dazu auf, Vorgehensweisen einzuführen, mit denen gewährleistet wird, dass die Informationen, die jedes Mal beim Ablesen eines Cookies gesammelt werden, unverzüglich gelöscht oder anonymisiert werden, sobald sie nicht mehr gespeichert werden müssen. Jeder für die Datenverarbeitung Verantwortliche muss rechtfertigen können, warum eine bestimmte Speicherungsdauer erforderlich ist. Die Artikel-29-Arbeitsgruppe fordert die Betreiber von Werbenetzwerken zur Angabe von Gründen zur Rechtfertigung der Speicherungsdauer auf, die sie angesichts der Zwecke für die Datenverarbeitung für erforderlich halten.

Wenn eine natürliche Person um die Löschung ihres Profils bittet oder von ihrem Recht auf Zurückziehung der Einwilligung Gebrauch macht, ist der Betreiber des Werbenetzwerks dazu verpflichtet, die die betroffene Person betreffenden Daten unverzüglich zu löschen, da er nicht mehr länger über eine Rechtsgrundlage (d. h. die Einwilligung) für die Verarbeitung verfügt.

5.3. Rechte der betroffenen Person

Die für die Datenverarbeitung Verantwortlichen sollten es den von der Verarbeitung betroffenen Personen ermöglichen, ihr in den Artikeln 12 und 14 der Datenschutzrichtlinie niedergelegtes Auskunfts-, Berichtigungs-, Löschungs- und Widerspruchsrecht auszuüben.

Der Artikel-29-Arbeitsgruppe sind die Initiativen der Betreiber von Werbenetzwerken bekannt, die Zugriff auf die Interessenkategorien anbieten, in die die betroffenen Personen aufgrund der Identifikationsnummer des Cookies eingeordnet wurden[42]. Diese neuen Tools ermöglichen den Nutzern nicht nur den Zugriff auf die sie betreffenden Interessenkategorien, sondern auch die Änderung oder Löschung derselben.

Die Artikel-29-Arbeitsgruppe begrüßt diese Initiativen, die dazu beitragen, die Rechte der Personen auf einen leichten Zugriff und auf Änderung ihrer personenbezogenen Daten wirksam zu machen. Die Artikel-29-Arbeitsgruppe drängt die Betreiber von Werbenetzwerken dazu, Verfahren einzuführen, mit denen die Personen über diese Tools informiert werden und mit denen diese für die betroffenen Personen so sichtbar wie möglich gemacht werden, so dass der durchschnittliche Nutzer tatsächlich zu ihrer Nutzung befähigt wird.

---

42 Siehe den Ad Interest Manager von Yahoo unter: http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/
Siehe auch die Funktionsweise der interessenbezogenen Werbung von Google unter:
http://www.google.com/ads/preferences/html/about.html.

5.4. Sonstige Verpflichtungen

Artikel 17 der Richtlinie sieht vor, dass der für die Datenverarbeitung Verantwortliche die ***technischen und organisatorischen Maßnahmen*** durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Weitergabe und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. Die Einhaltung der Sicherheitsvorschriften macht es erforderlich, dass die Betreiber von Werbenetzwerken technische und organisatorische Maßnahmen umsetzen, die dem Stand der Technik entsprechen, um die Sicherheit und Vertraulichkeit der Informationen zu gewährleisten.

Gemäß Artikel 18 der Richtlinie 95/46/EG können die für die Datenverarbeitung Verantwortlichen zur ***Meldung der Verarbeitung*** an die Datenschutzbehörde verpflichtet sein, sofern sie von dieser Pflicht nicht befreit sind. Entsprechend müssen die Betreiber von Werbenetzwerken die Verarbeitung melden, sofern dies gemäß innerstaatlichem Recht vorgeschrieben ist. Darüber hinaus müssen die Betreiber von Werbenetzwerken bei einer Übermittlung der Daten in ein Land außerhalb der EU, beispielsweise an einen Server in einem Drittland, die Einhaltung der Vorschriften zur Übermittlung personenbezogener Daten in Drittländer sicherstellen (Artikel 25 und 26 der Richtlinie 95/46/EG).

6. Schlussfolgerungen und Empfehlungen

Die Techniken der Werbung auf Basis von Behavioural Targeting ermöglichen es Werbetreibenden und insbesondere den Betreibern von Werbenetzwerken, im Internet surfende Personen zu verfolgen, um Profile zu erstellen und diese für gezielte Werbung zu nutzen. In den meisten Fällen ist es den betroffenen Personen nicht einmal bewusst, dass dies passiert.

Die Artikel-29-Arbeitsgruppe ist zutiefst beunruhigt über die Auswirkungen, die diese immer weiter verbreitete Praxis auf die Privatsphäre und den Datenschutz hat. Während die Datenschutzgesetzgebung für die Ausübung dieser Praxis unter anderem die Einholung der Einwilligung der betroffenen Personen fordert, ist es in Wahrheit eher zweifelhaft, dass die Durchschnittsperson weiß, dass sie für die Einblendung gezielter Werbung überwacht wird, geschweige denn, dass sie ihre Einwilligung hierfür erteilen würde.

Bislang haben die Versuche der Industrie versagt, Informationen zu erteilen und den Personen di Kontrolle zu erleichtern, ob sie überwacht werden wollen oder nicht. Häufig unklar verfasste Mitteilungen in den allgemeinen Geschäftsbedingungen oder in den Datenschutzvorschriften erfüllen die Vorschriften der Datenschutzgesetzgebung nicht. In einigen Mitgliedstaaten hat die Industrie Anstren-

gungen unternommen, die geltenden Gesetze durch Selbstkontrolle zu ergänzen. Solche Anstrengungen sind willkommen, da sie die allgemeinen Grundsätze des Rechtsrahmens genauer darlegen. Die Artikel-29-Arbeitsgruppe ist jedoch der Ansicht, dass noch ein weiter Weg zurückzulegen ist. Die Industrie sollte ihre Anstrengungen zur Einhaltung der wiedererstarkten, geltenden Rechtsvorschriften intensivieren.

Mit dieser Stellungnahme möchte die Artikel-29-Arbeitsgruppe den Stakeholdern und insbesondere den Betreibern von Werbenetzwerken und den Anbietern von Online-Inhalten Orientierungshilfe bei der Einhaltung des geltenden Rechtsrahmens geben, wie er in der vorliegenden Stellungnahme ausgelegt wird. Deshalb legt die vorliegende Stellungnahme die Ansichten der Artikel-29-Arbeitsgruppe zur Auslegung des geltenden Datenschutz-Rechtsrahmens in Bezug auf die Praxis der Werbung auf Basis von Behavioural Targeting dar. Sie ruft die Industrie auch dazu auf, technische und sonstige Mittel zur Einhaltung des in der Stellungnahme dargelegten Rechtsrahmens vorzulegen und bezüglich dieser Mittel in einen Meinungsaustausch mit der Artikel-29-Arbeitsgruppe zu treten. Am Ende eines festgelegten „Diskussionszeitraums" bewertet die Artikel-29-Arbeitsgruppe die Situation und ergreift die notwendigen und geeigneten Maßnahmen. In der Zwischenzeit fordert die Artikel-29-Arbeitsgruppe die betroffenen Parteien zur Umsetzung der nachfolgenden Empfehlungen auf.

6.1. Geltende Rechtsvorschriften

- Der EU-Rechtsrahmen für die Nutzung von Cookies ist hauptsächlich in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation niedergelegt[43].

- Artikel 5 Absatz 3 findet immer dann Anwendung, wenn „Informationen" wie Cookies auf dem Endgerät des Internet-Nutzers gespeichert oder abgelesen werden. Es wird nicht vorausgesetzt, dass es sich hierbei um personenbezogene Daten handelt.

- Darüber hinaus findet die Richtlinie 95/46/EG immer dann auf Angelegenheiten Anwendung, die nicht ausdrücklich durch die Datenschutzrichtlinie für elektronische Kommunikation abgedeckt sind, wenn personenbezogene Daten verarbeitet werden. Werbung auf Basis von Behavioural Targeting basiert auf der Nutzung von Kennungen, die die Erstellung sehr detaillierter Nutzer-Profile ermöglichen, die in den meisten Fällen als personenbezogene Daten gelten.

[43] Die geänderte Datenschutzrichtlinie für elektronische Kommunikation muss bis zum Mai 2011 umgesetzt werden.

6.2. Zuständigkeit, territorialer Anwendungsbereich – Niederlassung

- Die Richtlinie 95/46/EG findet auf die Datenverarbeitung Anwendung, die stattfindet, wenn Anbieter von Online-Inhalten und Betreiber von Werbenetzwerken gemäß Artikel 4 Absatz 1 Buchstaben a und c der Richtlinie (95/46/EG) und gemäß Artikel 3 der Datenschutzrichtlinie für elektronische Kommunikation Werbung auf Basis von Behavioural Targeting betreiben. Die bestehenden Vorgaben der Artikel-29-Arbeitsgruppe zu diesem Thema sind vollumfänglich anwendbar.

6.3. Rollen und Verantwortlichkeiten

- ***Betreiber von Werbenetzwerken*** sind durch die Verpflichtungen von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation insoweit gebunden, als sie Cookies auf den Endgeräten der betroffenen Personen platzieren und/oder Informationen von Cookies abrufen, die bereits auf diesen Geräten gespeichert sind. Sie sind insoweit auch für die Datenverarbeitung Verantwortliche als sie die Zwecke und die grundlegenden Mittel der Datenverarbeitung bestimmen.

- ***Anbieter von Online-Inhalten*** tragen in Bezug auf die erste Phase der Verarbeitung, also wenn sie durch die Art der Erstellung ihrer Website die Übermittlung der IP-Adresse an den Betreiber des Werbenetzwerks auslösen (was die weitere Verarbeitung ermöglicht), eine bestimmte Verantwortung, die mit der eines für die Datenverarbeitung Verantwortlichen verwandt ist. Diese Verantwortung bringt einige, eingeschränkte Datenschutz-Verpflichtungen (siehe unten) mit sich. Wenn Anbieter von Online-Inhalten darüber hinaus direkt identifizierbare, personenbezogene Daten an die Betreiber von Werbenetzwerken übermitteln, gelten sie als gemeinsam für die Datenverarbeitung Verantwortliche.

6.4. Verpflichtungen und Rechte

In Bezug auf Betreiber von Werbenetzwerken:

- Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, der die Verpflichtung zur Einholung der vorherigen Einwilligung in Kenntnis der Sachlage festlegt, findet auf die Betreiber von Werbenetzwerken Anwendung.

- Einwilligungen können nur unter sehr eingeschränkten Umständen über die Browser-Einstellungen eingeholt werden. Insbesondere, wenn der Browser so eingestellt ist, dass er standardmäßig alle Cookies zurückweist (wenn der Browser auf diese Option eingestellt wurde) und der Nutzer die Einstellung so

geändert hat, dass er Cookies akzeptiert, nachdem der Nutzer vollumfänglich über den Namen des für die Datenverarbeitung Verantwortlichen, die Verarbeitung, die Ziele der Verarbeitung und die erhobenen Daten informiert wurde. Folglich muss entweder der Browser allein oder in Verbindung mit anderen Mitteln klare, umfassende und vollständig sichtbare Informationen über die Verarbeitung übermitteln.

- Die Betreiber von Werbenetzwerken sollten mit Browser-Herstellern/Entwicklern zusammenarbeiten und sie zur Einführung von Privacy-by-Design in Browser ermutigen.

- Cookie-basierte Opt-out-Mechanismen stellen im Allgemeinen keinen angemessenen Mechanismus zur Einholung der Einwilligung in Kenntnis der Sachlage dar. In den meisten Fällen wird die Einwilligung des Nutzers impliziert, wenn er von der Opt-out-Möglichkeit nicht Gebrauch macht. Tatsächlich machen aber nicht deshalb nur so wenige Leute von der Opt-out-Möglichkeit Gebrauch, weil sie sich in Kenntnis der Sachlage für eine Einwilligung in die Werbung auf Basis des Behavioural Targeting entschieden haben, sondern weil sie nicht wissen, dass eine Verarbeitung stattfindet und erst recht nicht, wie sie von dem Opt-out Gebrauch machen können.

- Die Betreiber von Werbenetzwerken sollten schnell von Opt-out-Mechanismen Abstand nehmen und vorherige Opt-in-Mechanismen einführen. Mechanismen zur Einholung einer gültigen Einwilligung in Kenntnis der Sachlage sollten eine positiv bejahende Handlung der betroffenen Person erforderlich machen, mit der diese ihre Einwilligung in den Erhalt von Cookies und in die darauffolgende Überwachung ihrer Surf-Gewohnheiten zur Einblendung maßgeschneiderter Werbung erteilt.

- In Übereinstimmung mit Erwägungsgrund 25 der Datenschutzrichtlinie für elektronische Kommunikation könnte die Einwilligung eines Nutzers in den Erhalt eines Cookies auch seine Einwilligung in das nachfolgende Lesen des Cookies zurFolge haben und folglich in die Überwachung seines Internet-Surfens. Es wäre nicht erforderlich, für jedes Lesen des Cookies die Einwilligung einzuholen. Um sicherzustellen, dass den betroffenen Personen bewusst bleibt, dass sie überwacht werden, sollten die Betreiber von Werbenetzwerken: *i)* den Umfang der Einwilligung zeitlich begrenzen; *ii)* ein einfaches Zurückziehen der Einwilligung in dieÜberwachung für Zwecke der Werbung auf Basis von Behavioural Targeting ermöglichen und *iii)* ein Symbol oder andere Tools erstellen, die auf allen Websites sichtbar sein sollten, auf denen die Überwachung stattfindet (die Website-Partner des Betreibers des Werbenetzwerks). Dieses Symbol sollte die Personen nicht nur an die Überwachung erinnern, sondern ihnen auch bei der Entscheidung helfen, ob sie weiterhin überwacht werden möchten oder ob sie ihre Einwilligung zurückziehen wollen.

- Die Betreiber von Werbenetzwerken sollten die Einhaltung der Verpflichtungen sicherstellen, die sich aus der Richtlinie 95/46/EG ergeben und die sich nicht direkt mit Artikel 5 Absatz 3 überschneiden. Dazu gehören der Zweckbegrenzungs-Grundsatz und die Sicherheitsverpflichtungen.

- Darüber hinaus sollten die Betreiber von Werbenetzwerken den Personen die Ausübung ihrer Rechte auf Auskunft, Berichtigung und Löschung ermöglichen. Die Artikel-29-Arbeitsgruppe begrüßt es, dass manche Betreiber von Werbenetzwerken den betroffenen Personen den Zugriff auf und die Änderung der Interessenkategorien ermöglichen, in die sie eingeordnet wurden.

- Die Betreiber von Werbenetzwerken sollten Speicherungs-Strategien nutzen, die sicherstellen, dass die Informationen, die jedes Mal gesammelt werden, wenn ein Cookie gelesen wird, automatisch nach einer begründeten Zeitspanne gelöscht werden (die für die Verarbeitung erforderlich ist). Dies findet auch auf alternative Tracking-Technologien Anwendung, die im Zusammenhang mit Werbung auf Basis von Behavioural Targeting genutzt werden, wie beispielsweise JavaScript und auf der Browser-Umgebung des Nutzers installiert sind.

Betreiber von Werbenetzwerken und Anbieter von Online-Inhalten:

- Die Bereitstellung sehr gut sichtbarer Informationen ist eine Grundvoraussetzung für die Gültigkeit einer Einwilligung. Das Erwähnen der Praxis der Werbung auf Basis von Behavioural Targeting in den allgemeinen Geschäftsbedingungen und/oder den Datenschutzvorschriften kann niemals ausreichen. Unter Berücksichtigung des niedrigen Kenntnisstands über die Praxis der Werbung auf Basis von Behavioural Targeting sollten diesbezüglich Anstrengungen zur Änderung der Situation unternommen werden.

- Die Betreiber von Werbenetzwerken und die Anbieter von Online-Inhalten sind gemäß Artikel 10 der Richtlinie 95/46/EG zur Bereitstellung von Informationen an die Nutzer verpflichtet. Konkret heißt das, dass sie sicherstellen sollten, dass die Personen mindestens erfahren, wer (d. h. welche Stelle) für die Platzierung des Cookies und die Erhebung der entsprechenden Informationen zuständig ist. Darüber hinaus sollten sie auf einfache Weise darüber informiert werden, (a) dass der Cookie für die Erstellung von Profilen genutzt wird; (b) welche Art Informationen gesammelt werden, um diese Profile zu erstellen; (c) dass die Profile zur Schaltung maßgeschneiderter Werbung genutzt werden und (d), dass der Cookie die Identifizierung des Nutzers über zahlreiche Websites ermöglicht.

- Die Betreiber von Werbenetzwerken/die Anbieter von Online-Inhalten sollten die Informationen interaktiv direkt auf dem Bildschirm anbieten, wenn nötig

über „layered“ Mitteilungen. Auf jeden Fall sollten sie leicht zugänglich und sehr gut sichtbar sein.

- Gute Beispiele sind Icons, die auf der Website des Anbieters von Online-Inhalten um die Werbung platziert sind und Links zu weiteren Informationen angeben. Die Artikel-29-Arbeitsgruppe drängt die Betreiber von Werbenetzwerken, die Anbieter von Online-Inhalten und die Industrie zu Kreativität auf diesem Bereich.

Brüssel, den 22. Juni 2010

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (WP 176)

Angenommen am 12. Juli 2010

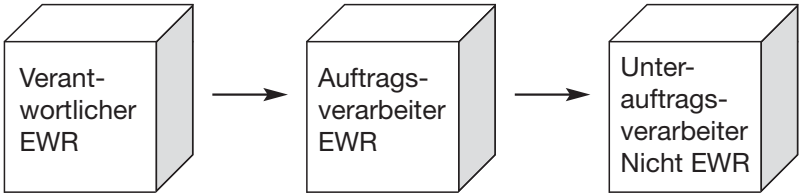
Am 5. Februar 2010 erließ die Europäische Kommission einen Beschluss mit geänderten Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten (Klauseln für die Verträge zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern).

Der neue Beschluss 2010/87/EU regelt die Übermittlung von Daten zwischen für die Verarbeitung Verantwortlichen aus dem EWR und Auftragsverarbeitern, die außerhalb des EWR niedergelassen sind, und legt die Bedingungen für die Vergabe eines Unterauftrags für die Verarbeitung durch einen außerhalb des EWR niedergelassenen Auftragsverarbeiter an einen ebenfalls außerhalb des EWR niedergelassenen Unterauftragsverarbeiter fest.

Die Artikel-29-Datenschutzgruppe hat folgende häufig gestellte Fragen (FAQ) zusammengestellt und beantwortet, um bestimmte Aspekte der Anwendung der neuen Standardvertragsklauseln zu klären, die am 15. Mai 2010 in Kraft getreten sind. Diese Unterlage gibt den harmonisierten Standpunkt der europäischen Kontrollstellen wieder.

Die Liste der häufig gestellten Fragen ist nicht abschließend, sie wird bei Bedarf aktualisiert.

I. Fragen zur Beauftragung eines im EWR niedergelassenen Auftragsverarbeiters



1) Sind die Standardvertragsklauseln des Beschlusses 2010/87/EU zu verwenden, wenn ein im EWR niedergelassener für die Verarbeitung Verantwortlicher einem ebenfalls im EWR niedergelassenen Auftragsverarbeiter personenbezogene Daten übermittelt, der diese dann an einen Unterauftragsverarbeiter außerhalb des EWR weiter übermittelt?

Nein. Wie es in Erwägungsgrund 23 des Kommissionsbeschlusses heißt, gilt der Beschluss nur, wenn ein in einem Drittland niedergelassener Auftragsverarbeiter einen in einem Drittland niedergelassenen Unterauftragsverarbeiter mit seinen Verarbeitungsdiensten beauftragt.

2) Dürfen die Standardvertragsklauseln des Beschlusses 2010/87/EU dennoch verwendet werden, wenn ein im EWR niedergelassener für die Verarbeitung Verantwortlicher einem ebenfalls im EWR niedergelassenen Auftragsverarbeiter personenbezogene Daten übermittelt, der diese dann an einen Unterauftragsverarbeiter außerhalb des EWR weiter übermittelt?

Nein, das ist nicht möglich.

Zunächst kann der im EWR niedergelassene Auftragsverarbeiter nicht als Datenimporteur im Sinne des Beschlusses 2010/87/EU gelten, da er definitionsgemäß außerhalb des EWR niedergelassen sein muss.

Zweitens sind die Pflichten, die ein Datenimporteur gemäß den Vertragsklauseln des Beschlusses 2010/87/EU zu erfüllen hat, für einen im EWR niedergelassenen Auftragsverarbeiter unangemessen (besonders in Bezug auf das anwendbare Recht und die Vorschriften über die Haftung des Auftragsverarbeiters).

Drittens kann der im EWR niedergelassene Auftragsverarbeiter nicht als Datenexporteur im Sinne des Beschlusses 2010/87/EU gelten, da der Datenexporteur definitionsgemäß ein für die Datenverarbeitung Verantwortlicher ist.

Fazit: Die Datenschutzgruppe vertritt den Standpunkt, dass die Verwendung der Standardvertragsklauseln des Beschlusses 2010/87/EU für einen im EWR niedergelassenen Auftragsverarbeiter unangemessen ist.

3) Was kann in diesem Fall als Rechtsgrundlage für die Übermittlung von Daten von einem im EWR niedergelassenen Auftragsverarbeiter an einen nicht im EWR niedergelassenen Unterauftragsverarbeiter dienen?

Solange kein neues Rechtsinstrument verabschiedet ist, das speziell für diesen Fall gilt und die internationale Vergabe von Aufträgen durch in der EU niedergelassene Auftragsverarbeiter an Unterauftragsverarbeiter in einem Drittland vorsieht (siehe Arbeitsdokument 161), sieht die Datenschutzgruppe drei Möglichkeiten (die Wahl ist dem jeweiligen Unternehmen überlassen):

a. Direktverträge zwischen im EWR niedergelassenen für die Verarbeitung Verantwortlichen und nicht im EWR niedergelassenen Auftragsverarbeitern

b. Klarer Auftrag des im EWR niedergelassenen für die Verarbeitung Verantwortlichen an den im EWR niedergelassenen Auftragsverarbeiter, die Standardvertragsklauseln des Beschlusses 2010/87/EU im Namen des Ersteren zu verwenden

c. Ad-hoc-Verträge.

a. Direktverträge zwischen einem im EWR niedergelassenen für die Verarbeitung Verantwortlichen und einem nicht im EWR niedergelassenen Auftragsverarbeiter

Der im EWR niedergelassene für die Verarbeitung Verantwortliche kann direkt mit dem nicht im EWR niedergelassenen Auftragsverarbeiter einen Vertrag auf der Grundlage der Standardvertragsklauseln schließen. In diesem Fall muss der nicht im EWR niedergelassene Auftragsverarbeiter als Datenimporteur und nicht als Unterauftragsverarbeiter die Klauseln des Beschlusses 2010/87/EU unterzeichnen. Das Vertragsverhältnis zwischen dem im EWR niedergelassenen für die Verarbeitung Verantwortlichen und dem im EWR niedergelassenen Auftragsverarbeiter wird dann in der Dienstleistungsvereinbarung zwischen den beiden Parteien geregelt, in der die Anweisungen des im EWR niedergelassenen für die Verarbeitung Verantwortlichen für den im EWR niedergelassenen Auftragsverarbeiter sowie sämtliche einschlägigen Bestimmungen des Artikels 16 und 17 der EU-Richtlinie enthalten sind.

b. Klarer Auftrag des im EWR niedergelassenen für die Verarbeitung Verantwortlichen an den im EWR niedergelassenen Auftragsverarbeiter, die Standardvertragsklauseln des Beschlusses 2010/87/EU im Namen des Ersteren zu verwenden

Eine Alternativlösung, die ähnliche Rechtswirkung aber andere Modalitäten hat als die erste Lösung, bestünde darin, in der Dienstleistungsvereinbarung ausdrücklich festzuhalten, dass der im EWR niedergelassene Auftragsverarbeiter beauftragt ist, im Namen des im EWR niedergelassenen für die Verarbeitung Verantwortlichen einen Vertrag mit den Standardvertragsklauseln des Beschlusses 2010/87/EU mit dem nicht im EWR niedergelassenen Unterauftragsverarbeiter zu schließen. Der für die Verarbeitung Verantwortliche gilt weiterhin als Datenexporteur, der Unterauftragsverarbeiter als Datenimporteur.

Ersterer sollte sich ferner vorher mit den Anhängen 1 und 2 der Standardvertragsklauseln des Beschlusses 2010/87/EU einverstanden erklären.

Wie in der FAQ II Absatz 1 erklärt, hat der Datenexporteur zu entscheiden, ob der Auftrag generell (wodurch die Vergabe eines Unterauftrags für die Verarbeitung der in den Anhängen 1 und 2 genannten Daten erlaubt wird) oder spezifisch erteilt werden soll (Auftrag speziell für die Vergabe der einzelnen Unteraufträge).

c. Ad-hoc-Verträge

Gemäß dem zweiten Teil des Erwägungsgrundes 23 des Kommissionsbeschlusses „*steht es den Mitgliedstaaten frei zu entscheiden, ob sie die Tatsache berücksichtigen möchten, dass bei der Vergabe eines Verarbeitungsauftrags an einen in einem Drittland niedergelassenen Unterauftragsverarbeiter die in dieser Entscheidung vorgesehenen und in Vertragsklauseln festzuschreibenden Grundsätze und Garantien mit dem Ziel zur Anwendung gebracht wurden, die Rechte der von der Datenübermittlung zwecks Unterauftragsverarbeitung betroffenen Person angemessen zu schützen.*“

Der Ad-hoc-Vertrag enthält daher die Grundsätze und Garantien der Standardvertragsklauseln im Beschluss 2010/87/EU (wie die Drittbegünstigtenklausel). Im Prinzip sollten für den im EWR niedergelassenen für die Verarbeitung Verantwortlichen und den nicht im EWR niedergelassenen Unterauftragsverarbeiter die Pflichten und Haftungsbestimmungen gelten, die in den Standardvertragsklauseln des Beschlusses 2010/87/EU vorgesehen sind. Welches Recht für den im EWR niedergelassenen Auftragsverarbeiter gilt, sollte nach der EU-Richtlinie bestimmt werden. Der im EWR niedergelassene Auftragsverarbeiter darf insbesondere nicht von der Haftung gegenüber der von der Verarbeitung betroffenen Person, zu der er nach den innerstaatlichen Vorschriften zur Umsetzung der EU-Richtlinie 95/46/EG verpflichtet ist, entbunden werden. Gleichzeitig wird es nach dem Vertrag möglich sein, dass der im EWR niedergelassene Auftragsverarbeiter das Recht seines Landes in Bezug auf technische und sicherheitstechnische Maßnahmen anwendet, während der nicht im EWR niedergelassene Unterauftragsverarbeiter die Geltung des innerstaatlichen Rechts des für die Verarbeitung Verantwortlichen anerkennen muss.

Die Kontrollstellen dürfen die ihnen vorgelegten Ad-hoc-Verträge prüfen und haben das Recht, die Datenübermittlung auf der Grundlage dieser Verträge zu genehmigen.

II. Fragen zur Beauftragung eines nicht im EWR tätigen Auftragsverarbeiters

1) Kann der für die Verarbeitung Verantwortliche mit seiner vorherigen schriftlichen Zustimmung (Klausel 11 Absatz 1) die Vergabe von Unteraufträgen generell erlauben oder muss die Vergabe jedes Unterauftrags einzeln genehmigt werden?

Die Standardvertragsklauseln des Beschlusses 2010/87/EU lassen dies offen. Nach Ansicht der Datenschutzgruppe muss der für die Verarbeitung Verantwortliche entscheiden, ob eine generelle vorherige Zustimmung ausreicht oder ob für jeden Unterauftrag erneut eine Zustimmung erteilt werden muss.

Bei der Entscheidung wird es wahrscheinlich auf die Rahmenbedingungen der Verarbeitung, die Art der Daten (sensibel oder nicht) und den jeweiligen für die Verarbeitung Verantwortlichen ankommen. Einige für die Verarbeitung Verantwortliche werden sicherlich beschließen, dass die Identität jedes Unterauftragsverarbeiters zuvor ausführlich überprüft werden muss, während andere die vorherige schriftliche Einwilligung (Klausel 5 Buchstabe h), die Pflicht zur Mitteilung der Klausel (Klausel 5 Buchstabe j) und die Garantie eines mindestens ebenso hohen Schutzniveaus (Klausel 11 Buchstabe 1) für ausreichend befinden werden.

2) Was ist mit dem Ausdruck „eine Kopie des Unterauftrags über die Datenverarbeitung" (Klausel 5 Buchstabe j) genau gemeint?

Gemeint ist ein Auftrag im Sinne von Klausel 11 Absatz 1 (eine schriftliche Vereinbarung zwischen dem Datenimporteur und dem nicht im EWR niedergelassenen Unterauftragsverarbeiter, mit der diesem die gleichen Pflichten auferlegt werden, die nach den Vertragsklauseln für den Auftragsverarbeiter gelten).

Daher ist der Datenimporteur nicht automatisch dazu verpflichtet, alle Unterlagen über die Vergabe eines Unterauftrags zu übermitteln, sondern nur die Unterlagen über vertragliche Vereinbarungen über den Datenschutz (einschließlich Sicherheitsmaßnahmen).

3) Was genau ist in Artikel 7 des Beschlusses mit „Änderungen und Verarbeitungsvorgängen, die unter den Vertrag fallen" gemeint?

Gemäß Artikel 7 Absatz 2 bleibt ein gemäß der früheren Fassung der Standardvertragsklauseln (Entscheidung 2002/16/EG) geschlossener Vertrag in Kraft und muss nicht gekündigt werden, es sei denn, die Übermittlungen und die Datenverarbeitungsvorgänge aufgrund dieses Vertrags haben sich geändert. In diesem Fall sind die Vertragsparteien verpflichtet, einen neuen, auf den Standardvertragsklauseln des Beschlusses 2010/87/EU beruhenden Vertrag zu schließen.

Nach Ansicht der Datenschutzgruppe ist dies der Fall, wenn Anhang 1 zu den Standardvertragsklauseln geändert werden muss (Änderung einer Vertragspartei, einer betroffenen Person, der Datenkategorie oder der Verarbeitung).

In diesem Fall entscheiden die Vertragsparteien, ob sie einen neuen Vertrag mit den Standardvertragsklauseln des Beschlusses 2010/87/EU schließen oder den vorherigen Vertrag, der auf der Grundlage der Klauseln der Entscheidung 2002/16/EG geschlossen worden war, beibehalten. Da die neuen Standardvertragsklauseln jedoch die Standardvertragsklauseln der Entscheidung 2002/16/EG ersetzen, gelten Letztere nicht mehr als Standardvertragsklauseln, sondern als Ad-hoc-Vertrag.

4) Sind die Auftragsverarbeiter, die nicht im EWR niedergelassen sind und von einem Datenimporteur Daten erhalten (im Rahmen eines mit dem Datenexporteur geschlossenen Globalvertrags) als Unterauftragsverarbeiter zu betrachten oder als weitere Datenimporteure?

Gemäß den Standardvertragsklauseln des Beschlusses 2010/87/EU gelten sämtliche Verarbeiter, die vom Datenimporteur oder von einem Unterauftragnehmer des Datenimporteurs mit der Verarbeitung beauftragt wurden, als Unterauftragsverarbeiter.

Sind sämtliche nicht im EWR niedergelassene Auftragsverarbeiter vom Datenexporteur beauftragt, können sie die Standardvertragsklauseln als Datenimporteure unterzeichnen.

Sind nicht im EWR niedergelassene Auftragsverarbeiter vom Datenimporteur beauftragt, unterzeichnen sie die Standardvertragsklauseln als Unterauftragsverar-

beiter. In diesem Fall bleibt der Datenimporteur gemäß Klausel 11 Absatz 1 gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

5) Ist ein Vertrag zwischen dem Datenimporteur und dem Unterauftragsverarbeiter ausreichend, wenn ein Datenimporteur Daten an einen Unterauftragsverarbeiter übermittelt, der im Auftrag mehrerer Datenexporteure für den Datenimporteur Leistungen erbringt?

Nein. Es ist nicht möglich, alle Aufträge in einem einzigen Vertrag zusammenzufassen. Anhang 1 des Vertrags kann nicht für alle Aufträge gleich sein, da die Identität des Datenexporteurs und wohl auch die Datenkategorien, die betroffenen Personen und die Beschreibung der Verarbeitungsvorgänge unterschiedlich sein werden.

Die Vertragsparteien können allerdings beschließen, in jedem Vertrag auf allgemeinere Vereinbarungen Bezug zu nehmen wie auf die Standardvertragsklauseln des Beschlusses 2010/87/EU und möglicherweise auf Anhang 2 über technische Maßnahmen (wenn sie für alle Verträge identisch sind, vom Datenimporteur akzeptiert werden und die Anforderungen des Datenexporteurs erfüllen).

6) Ist die Bedingung einer schriftlichen Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter, mit der diesem die gleichen Pflichten auferlegt werden, die nach den Klauseln des Originalvertrags zwischen dem Datenexporteur und dem Datenimporteur gelten (Klausel 11 Absatz 1), erfüllt, wenn der Unterauftragsverarbeiter den zwischen dem Datenexporteur und dem Datenimporteur geschlossenen Vertrag mitunterzeichnet?

Wie aus Fußnote 9 der Standardvertragsklauseln des Beschlusses 2010/87/EU ausdrücklich hervorgeht, kann diese Anforderung dadurch erfüllt werden, dass der Unterauftragsverarbeiter den nach diesen Standardvertragsklauseln geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

In diesem Fall fügen die Vertragsparteien am Ende des Vertrags (bei der Unterschrift) Folgendes hinzu: „für den Unterauftragsverarbeiter“, „Name (vollständig)“, „Funktion“, „Anschrift“, „Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen“, „Unterschrift“, „Stempel der Organisation“.

7) Können weitere geschäftsbezogene Klauseln in die Standardvertragsklauseln aufgenommen werden?

Gemäß Klausel 10 ist es den Vertragsparteien nicht erlaubt, die Standardvertragsklauseln zu ändern. Das bedeutet allerdings nicht, dass die Parteien keine weite-

ren, geschäftsbezogenen Klauseln aufnehmen dürfen. Diese dürfen jedoch nicht im Widerspruch zu den Standardvertragsklauseln stehen.

8) Sind die Datenexporteure verpflichtet, die zwischen ihren Datenimporteuren und ihren Unterauftragsverarbeitern geschlossenen Vereinbarungen über Verarbeitungsunteraufträge den Kontrollstellen vorzulegen, auch wenn sie nicht Partei der Vereinbarung sind?

Nach Klausel 11 Absatz 4 führt der Datenexporteur ein Verzeichnis der Vereinbarungen über Verarbeitungsunteraufträge, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden, und stellt das Verzeichnis seiner Kontrollstelle bereit.

Der Datenexporteur ist nur zur Übermittlung der Vereinbarung verpflichtet, die er selbst geschlossen hat (siehe Klausel 8 Absatz 1).

V. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 47. Sitzung am 15./16. April 2010 in Granada

Die „Granada Charta“ des Datenschutzes in einer digitalen Welt[1]

– Übersetzung –

Die internationale Gemeinschaft hat sich seit langem mit Fragen des Informationszeitalters befasst. Im Laufe der letzten Jahrzehnte wurden die folgenden internationalen Dokumente verabschiedet:[2]

- Europäische Menschenrechtskonvention vom 4. November 1950
- OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten vom 23. September 1980
- Übereinkommen 108 des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten
- Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, angenommen durch Entschließung der Generalversammlung vom 14. Dezember 1990
- Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,
- Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000
- Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

[1] Aufgrund von Unvereinbarkeit mit dem nationalen Recht in Schweden hat sich die schwedische Delegation bei der Verabschiedung dieses Arbeitspapiers der Stimme enthalten.

[2] Außerdem wurden die folgenden Empfehlungen und Entschließungen veröffentlicht: International Working Group on Data Protection in Telecommunications, Zehn Gebote zum Schutz der Privatsphäre im Internet, 13.–14. September 2000, Berlin; International Working Group on Data Protection in Telecommunications, Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum“, 3.–4. März 2008, Rom, Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, Entschließung zum Datenschutz in sozialen Netzwerkdiensten, Straßburg, 17. Oktober 2008, Internationale Datenschutzkonferenz, Entschließung zum Datenschutz bei Suchmaschinen, London, 2.–3. November 2006

– APEC Leitprinzipien zum Schutz der Privatsphäre von November 2004
– Gemeinsamer Vorschlag zur Erstellung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten[3]

In einer durch Interaktivität geprägten Welt sind die Einzelnen nicht mehr bloß Nutzer, sondern Netzbürger mit unveräußerlichen Rechten. Als solche sind sie aber auch verantwortlich für Inhalte, die sie über sich und andere veröffentlichen. Der Datenschutz und der Schutz der Privatsphäre sind äußerst wichtige Bestandteile einer demokratischen Informationsgesellschaft. Die folgenden Grundsätze sollen Teilnehmern, Anbietern und öffentlichen Stellen helfen, einen freien Informationsfluss zu gewährleisten und dabei die Würde, die Privatsphäre und den Schutz der Daten der Einzelnen zu respektieren. Es ist offensichtlich, dass zwischen diesen Grundsätzen und anderen wichtigen Werten wie freie Meinungsäußerung, Sicherheit und Eigentumsrechten Spannungen auftreten können. In jedem Einzelfall muss jede Maßnahme zur Durchsetzung dieser konkurrierenden Ziele mit dem Recht auf Datenschutz und der Privatsphäre in Ausgleich gebracht werden.

Teilnehmer und Nutzer der Kommunikationsdienste sollten

1. mit Sorgfalt vorgehen, wenn sie ihre eigenen personenbezogenen Daten oder Daten anderer veröffentlichen und sich dabei bewusst sein, dass die Löschung von Daten aus dem Internet weitaus größere Schwierigkeiten bereitet als deren Veröffentlichung

2. alle notwendigen Anstrengungen unternehmen – wie beispielsweise das Einholen einer vorherigen Einwilligung – um die Rechte einer jeden Person vor der Preisgabe oder Veröffentlichung ihrer Daten zu gewährleisten und ihre oder seine Entscheidung zu respektieren, eine gegebene Einwilligung zurückzuziehen

3. das grundlegende Recht haben, dass die rechtmäßige Nutzung von Kommunikationsdiensten privat und unbeobachtet bleibt und dass sie nicht abgehört und überwacht wird

4. die Möglichkeit haben, die Dienste anonym oder unter einem Pseudonym zu nutzen. Ihnen sollte auch die Möglichkeit eingeräumt werden, verschlüsselte Kommunikationen zu nutzen, insbesondere bei der An- und Abmeldung

[3] Verabschiedet von der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre am 5. November 2009; http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2009-Madrid-InternationaleStandards.pdf?_blob=publicationFile

5. das Recht haben, den Umfang personenbezogener Informationen zu kontrollieren, und auch die Nutzung dieser personenbezogenen Informationen

6. das Recht haben, über jede geplante Verarbeitung oder sekundäre Nutzung ihrer personenbezogenen Daten informiert zu werden. Ferner muss Ihnen die Möglichkeit eingeräumt werden, ihre ausdrückliche Einwilligung zu geben (opt-in) und ihre Einwilligung für alle derartigen vorgeschlagenen Offenlegungen oder sekundäre Nutzungen nachträglich zurückzuziehen (opt-out)

7. das Recht haben, bezüglich der Sammlung und Nutzung aller Daten über die Nutzung von Dienstleistungen ihre Einwilligung zu erteilen und diese auch nachträglich zurückzuziehen.

Anbieter von Informations- und Kommunikationsdiensten sollten

1. sicherstellen, dass Nutzer von Kommunikationsdienstleistungen mit Einrichtungen ausgestattet sind, die den oben aufgezeigten Anforderungen in Bezug auf die Nutzung gerecht werden

2. gewährleisten, dass diese Einrichtungen leicht zu nutzen sind und dass sie im Nutzerhandbuch gut beschrieben werden

3. alle Anfragen von Einzelnen zu Informationen, die über diese verarbeitet und an wen diese übermittelt werden, unverzüglich und sorgfältig beantworten. Außerdem sollen die Anbieter die Nutzer mit elektronischen Hilfsmitteln ausstatten, wie zum Beispiel einem Online-Zugang zu den sie betreffenden personenbezogenen Daten

4. sicherstellen, dass alle über die Nutzer gesammelten Informationen das für eine Dienstleistung notwendige Minimum darstellen und dass dieses Minimum an Daten nicht länger als nötig für den zu leistenden Dienst gespeichert wird

5. spezielle Sicherheitsvorkehrungen zum Schutz sensibler Daten einrichten, wie zum Beispiel Verkehrsdaten und Ortungsdaten

6. das Fernmeldegeheimnis garantieren

7. angemessene technische und organisatorische Maßnahmen zur Wahrung der Sicherheit ihrer Dienste treffen

8. Teilnehmer oder registrierte Nutzer von Kommunikationsdienstleistungen im Falle eines besonderen Risikos eines Sicherheitsverstoßes, über derartige Sicherheitsvorfälle und über alle möglichen Abhilfemaßnahmen informieren.

Öffentliche Stellen[4] sollten

1. bezüglich der Verarbeitung aller personenbezogener Daten offen und transparent sein

2. von jeglicher Beobachtung, dem Abhören oder der Überwachung der Kommunikation absehen, solange dies nicht für Strafverfolgungszwecke unbedingt notwendig ist, gestützt auf eine spezifische Rechtsrundlage

3. gewährleisten, dass Einzelpersonen aller Generationen und jeglichen Bildungsstandes in der Lage sind, Zugang zu den notwendigen Kenntnissen zu erlangen, um vollständig am digitalen Kommunikationszeitalter teilnehmen zu können

4. sicherstellen, dass jeder, der nicht in der Lage ist, Mittel der elektronischen Information und Kommunikation zu nutzen oder dies nicht wünscht, die Möglichkeit hat, ohne unangemessene Nachteile Zugang zu öffentlichen Dienstleistungen hat

5. die Rechte der Nutzer und das Recht auf Datenschutz und Schutz der Privatsphäre in interaktiven Diensten durchsetzen und den Nutzern effektive Rechtsmittel zu verschaffen.

[4] Einschließlich des Gesetzgebers, wo dies angemessen ist

Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft (Revision des Arbeitspapiers der 46. Sitzung vom 7./8. September 2009 in Berlin)

– Übersetzung –

Einleitung

Für viele Menschen sind Emails das primäre Kommunikationsmittel geworden, das traditionelle Briefe sowohl für private als auch für geschäftliche Zwecke ersetzt. Bei einem Email-Account, der eine Person identifizieren und für private Kommunikation genutzt werden kann, handelt es sich nach allgemeiner Auffassung der Datenschutzbehörden um personenbezogene Daten.

Eine Person kann einen oder mehrere Email-Accounts haben, die über einen kostenlosen oder kostenpflichtigen Dienst angeboten werden; einem Angestellten kann es auch von seinem Arbeitgeber gestattet sein, eine geschäftliche Email-Adresse für private Zwecke zu nutzen. Email-Accounts, die scheinbar umsonst zu haben sind, können mit anderen Informationsdiensten, wie Breitbanddiensten und Kabelfernsehen gebündelt sein.

Was also geschieht, wenn eine Person ihren Email-Anbieter wechseln muss?

Die Analogie in der realen Welt besteht darin, aus einem Haus in ein anderes umzuziehen. Gewöhnlicherweise schicken Personen, die umziehen, Briefe an alle ihre geschäftlichen und privaten Kontakte, um diese über den Umzug zu informieren. Darüber hinaus wird die Person in der Regel mit dem Post-Zusteller vereinbaren, dass alle Briefe an die neue Adresse weitergeleitet werden – heutzutage keine einfache Angelegenheit, da viele Postzustellungsunternehmen eingebunden sein können. Die Lösung kann darin bestehen, den neuen Bewohnern für die verbleibende Post Etiketten mit der neuen Anschrift zu geben.

Wenn wir diese Analogie aus der echten Welt in die virtuelle Welt übertragen, müssen wir alle Dienste der Informationsgesellschaft in Betracht ziehen, die es mit sich bringen, eine Person anhand des Namens zu identifizieren. Dies kann die zunehmend beliebten sozialen Netzwerke umfassen und auch Accounts bei virtuellen Marktplätzen, die eine Email-Adresse zu Zwecken der Validierung nutzen und an die elektronische Güter und Belege etc. gesendet werden können. Dasselbe Problem könnte sich auch im Fall des Verschickens von SMS im Zusammenhang mit Mobiltelefonen ergeben.

Wechsel einer Email-Adresse oder eines Accounts bei Diensten der Informationsgesellschaft

Wenn eine Email-Adresse oder ein virtueller Account geschlossen wird, besteht die Möglichkeit, dass ein neuer Nutzer den Benutzernamen wieder benutzen und dessen „Vergangenheit erben" könnte. Diese Möglichkeit ist im Fall von kostenlosen „email-for-life"-Diensten (sowie bei gmail oder hotmail) ziemlich abwegig, da solche Anbieter kaum abgelaufene Accounts neu verteilen würden.

Außer wenn der Nutzer für eine Domain gezahlt hat, wird der Domain-Name aller Wahrscheinlichkeit nach mit dem Service-Provider verbunden und nicht von einem auf den anderen Anbieter übertragbar sein.

Beispielhaft muss man sich jemanden vorstellen, der einen sehr gebräuchlichen Namen hat, wie „Joe Doe", der in Portugal lebt, gmail benutzt, sich bei einem Kabelfernsehkanal anmeldet und für eine Firma namens Xpto arbeitet; Joe könnte mehrere Email-Accounts haben, wie z. B. **joedoe99@gmail.com**, **joedoe@cabletv.pt**, **joedoe@xpto.pt**. Zusätzlich könnte er eine persönliche Domain für seine Familie gekauft haben oder nutzen wie **doe.pt** und die Email-Adresse **joe@doe.pt** benutzen.

Wenn er seinen gmail-Account aufgeben möchte, kann er ziemlich sicher sein, dass sein Account **joe.doe99@gmail.com** nicht wieder vergeben wird, aber wenn er das Abonnement für das Kabelfernsehen beendet oder seinen Arbeitsplatz wechselt, dann wird er vielleicht entdecken, dass er nicht mehr in der Lage ist, auf seine Emails über die Accounts **joedoe@cabletv.pt** oder **joedoe@xpto.pt** zuzugreifen.

Auf der anderen Seite sollte die Domain **doe.pt** nicht ohne Weiteres auf einen anderen übertragbar sein, vorausgesetzt, seine Familie zahlt weiter dafür.

Wenn dagegen sein früherer Kabelfernsehanbieter einen neuen Kunden hat und sein früherer Arbeitgeber einen neuen Angestellten, der auch Joe Doe heißt, könnten sie entscheiden, seine alte Email-Adresse an diese neue Person zu vergeben. In diesem Fall wird der neue „Inhaber" wohl Email-Nachrichten und persönliche Information „erhalten", die an den ursprünglichen Inhaber gerichtet waren.

In gleicher Weise kann jeder neue Besitzer einer wieder vergebenen Domain, bei der die Bezahlung ausgelaufen ist, Email-Verkehr erhalten, der an den früheren Besitzer gerichtet ist.

Mögliche negative Folgen

Dies kann zahlreiche negative Folgen haben:

- Wenn der Nutzer Abonnements für Email-Newsletter nicht kündigt oder nicht alle Kontakte über den Wechsel seiner Adresse informiert hat, wird der neue Besitzer Informationen erhalten, die für den früheren Besitzer bestimmt sind, was zur Preisgabe personenbezogener Daten führt;
- Wenn ein Nutzer die „Passwort-vergessen"-Option eines Dritten nutzt, bei dem er sich unter der alten Email-Adresse registriert hat, würde der neue Besitzer seinen Nutzernamen und das Passwort für diese website erhalten;
- Wenn ein Beschäftigter seine Arbeitsstelle verlässt, könnte der neue Beschäftigte persönliche Nachrichten erhalten, die für den ehemaligen Beschäftigten bestimmt sind, sowie auch geschäftliche Emails für denjenigen, der den ehemaligen Beschäftigten ersetzt hat;
- Wenn der Vertrag mit einem Internet-Service-Provider beendet wird, könnte sich der neue Kunde versehentlich oder absichtlich als der ehemalige Inhaber der Email-Adresse ausgeben.

Ähnliche Erwägungen sind auf andere Dienste der Informationsgesellschaft anwendbar, wie z. B. Instant Messaging, VoIP/Internettelefonie und soziale Netzwerke, besonders wenn die Email-Adresse zur Authentifizierung genutzt wird. Wenn ein Benutzer einen Dienst beenden möchte, kann der neue Benutzer Nachrichten empfangen, die für den ehemaligen Nutzer bestimmt sind, oder – was schwerwiegender ist – versuchen, als der alte Benutzer aufzutreten.

Während die mobile Rufnummernmitnahme (mobile number portability – MNP), die Möglichkeit des Auftretens dieses Problems im Zusammenhang mit Mobiltelefonen reduzieren kann, mag die Möglichkeit zur Rufnummernmitnahme nicht immer verfügbar sein (z. B. im Fall von mangelndem Bewusstsein, Umzug in ein anderes Land, Tod des Nutzers oder bei manchen Formen von „pay-as-you-go"-Diensten). Dann besteht wieder die Möglichkeit, dass jemand anders eine kürzlich verwendete Rufnummer und das damit verbundene Erbe an SMS-Nachrichten übernimmt.

Dies ist deshalb besonders problematisch, weil SMS in der Regel in besonders vertraulichen Bereichen wie Online-Banking und E-Ticketing verwendet werden.

Obwohl die Portabiliät von Mobilfunknummern geholfen hat, diese Probleme zu behandeln, könnte der Benutzer das Gefühl haben, dass er seine Email-Adresse oder die Nummer seines Mobiltelefons, einen bestimmten Internet-Service-Provider oder Mobilfunkanbieter für immer behalten muss, um seine Privatsphäre und persönliche Sicherheit zu wahren.

Empfehlungen

Die Arbeitsgruppe hat sich schon früher mit Aspekten des Schutzes der Privatsphäre und der Sicherheit im Zusammenhang mit Telekommunikationsdiensten[1], Internetdiensten[2] und sozialen Netzwerken[3] beschäftigt.

Die Arbeitsgruppe ist der Auffassung, dass ein Anbieter von Diensten der Informationsgesellschaft (im Folgenden als „ISP" bezeichnet) Dienste anbieten sollte, die es dem Nutzer ermöglichen, jede schädigende Konsequenz, die aus der Kündigung des Vertrages resultieren könnte, zu minimieren, und gibt folgende Empfehlungen:

1. Der ISP sollte eine Übergangsphase von mindestens drei Monaten vorsehen, bevor irgendjemand die Email-Adresse, persönliche Domain oder Telefonnummer eines vormaligen Nutzers übernehmen kann.

2. Der ISP sollte dem Nutzer eine Möglichkeit bieten, dass für die Dauer der Übergangsphase Nachrichten, die an die ausgesetzte Email-Adresse oder Nummer geschickt werden, zusammen mit einer passenden automatisierten Nachricht zurückgesandt werden.

3. Der ISP sollte einen Warnhinweis anbieten, der den Nutzer über das mit dem Ende des Vertrags verbundene Risiko, seine Email-Adresse zu verlieren, informiert sowie über die mögliche Preisgabe von Daten.

4. Der ISP könnte eine Funktion wie einen „wandernden" Ordner anbieten, in dem der Nutzer die Login-Daten speichern könnte, die für Web-Dienste verwendet werden, bei denen er sich unter Nutzung seiner Email-Adresse oder Mobilfunknummer registriert hat. Wenn der Account geschlossen oder der Vertrag beendet wird, könnte er den Ordner zu einem anderen Dienst mitnehmen, oder er hätte wenigstens eine Liste aller Dienste Dritter, mit denen seine Email-Adresse oder Mobilfunknummer verbunden ist, und könnte die Email-Adresse oder Mobilfunknummer dort ändern. Dies würde erfordern, dass der Nutzer solche Informationen stets aktualisiert.

5. Dienste, die eine SMS-Authentifizierung verwenden (z. B. Online-Banking), sollten die Mobiltelefonnummer anzeigen, an die die Nachricht verschickt

---

[1] Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz (Berlin 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[2] Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP) (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf?1201702122

[3] Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – Rom Memorandum – (Rom 3./4.03.2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?1234867489

wurde. Wenn der Dienst innerhalb eines gewissen Zeitraumes keine Rückmeldung von dem Nutzer erhält, dass die Transaktion fortgeführt werden soll, sollte die betreffende Nummer als gefährdet eingestuft und so lange ausgesetzt werden, bis der Inhaber der Accounts erneut die Nummer des zu verwendenden Mobiltelefons bestätigt.

6. Im Falle von SMS-Premium- oder ähnlichen Diensten sollte von dem Dienstanbieter von Zeit zu Zeit eine kostenlose Nachricht versandt werden, um festzustellen, ob der Nutzer diesen Dienst weiter in Anspruch nehmen will. Im Falle eines Bankkontos kann dies zum Beispiel durch die Einführung eines Berechtigungsmerkmals bestätigt werden, das nur der wirkliche Nutzer kennt und auf das nur er Zugriff hat.

7. Einzelpersonen (Arbeitnehmer) sollten für das Abonnement oder die Registrierung von Diensten privater Natur, wie mailing-Listen, e-shops, soziale Netzwerke, etc. keine Email-Adressen verwenden, die Anderen zugewiesen werden könnten (z. B. geschäftliche Email-Adressen).

8. Eine Person, die eine permanente Email-Adresse haben möchte, sollte einen persönlichen Domain-Namen registrieren, der auch als Homepage, Weblog etc. genutzt werden kann. Allerdings erfordert eine persönliche Domain in der Regel eine jährliche Erneuerung, anderenfalls kann sie verloren gehen und an eine andere Person vergeben werden.

9. Arbeitgeber und andere Organisationen, die geschäftliche Email-Adressen verteilen, sollten den Mechanismus festlegen, der eingreift, wenn ein Mitarbeiter geht oder seine Funktion innerhalb des Unternehmens wechselt. Nachrichten an eine solche Adresse sollten zurückgesandt werden, oder es sollte eine automatisierte Nachricht verschickt werden, sodass der Absender weiß, dass die Adresse des Angestellten sich geändert hat oder nicht mehr besteht. Es wird empfohlen, Bezeichnungen für persönliche Email-Adressen nicht wiederzuverwenden, wenn diese bereits ehemaligen Beschäftigten zugewiesen waren.

2. 48. Sitzung am 6./7. September 2010 in Berlin

Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken

– Übersetzung –

Deep Packet Inspection (DPI) ist eine Technologie, die die Untersuchung[1] des Headers und von Teilen des Inhalts von Datenpaketen, die über Netzwerke übertragen werden, in Echtzeit oder annähernder Echtzeit erlaubt.

Ein Internet-Paket oder „Datagramm" besteht gewöhnlich aus einem „Datagramm-Kopf" und einem „Datagramm-Daten-Bereich". Der Datagramm-Kopf ist der Teil des Pakets, der Informationen wie Quell- und Ziel-IP-Adresse enthält sowie andere Details, die notwendig sind, um das Paket dorthin zu leiten, wo es hin soll, während es das Netz durchquert. Der Datagramm-Daten-Bereich wird als „Nutzdaten" bezeichnet, weil er den Inhalt dessen bildet, was der Datagramm-Kopf (den „Umschlag") gewöhnlich zustellt. „Paketkopf" bezeichnet jegliche Information, die ein Dienstleister benötigt, um eine Telekommunikations-Nachricht zustellen zu können; die Nachricht selbst wird als der Inhalt oder die Nutzdaten dieser Telekommunikations-Nachricht bezeichnet.

Während DPI nicht als eine neue Technologie angesehen werden kann, da sie schon seit Jahren im Bereich der Intrusion Detection und -Prevention-Systeme wie auch in Firewall-Systemen eingesetzt wurde, wurden in jüngerer Zeit zusätzliche Nutzungen – ermöglicht durch leistungsfähigere Computer und effizientere Algorithmen – für das Netzverkehrsmanagement, zur Kontrolle der Verbreitung illegaler oder unerwünschter Inhalte – einschließlich urheberrechtsgeschützten Materials – und sogar für die Auslieferung benutzerspezifischer Werbung an Internetnutzer diskutiert und einzuführen begonnen.

Die Anwendung dieser Technologie kann die Privatsphäre von Internetnutzern Risiken aussetzen. Insbesondere können bestimmte Nutzungsarten von DPI-Technologien durch Internet-Zugangsdiensteanbieter zu erheblichen Beeinträchtigungen der Privatsphäre von Internetnutzern führen. Zugangsdiensteanbieter sind das „Eingangstor in die virtuelle Welt"; ihnen ist es technisch möglich, den Inhalt der gesamten Kommunikation eines Internetnutzers zu überwachen. Es ist daher unerlässlich, dass Internet-Zugangsdiensteanbieter das Fernmeldegeheimnis respektieren, wie es in vielen Rechtsordnungen festgelegt ist. Darüber hinaus bieten Internet-Zugangsdiensteanbieter in vielen Fällen nicht nur Internetzugang an, sondern auch Internettelefonie und Zugang zu Medien, wie Kabelfernsehen.

[1] In der Computertechnik werden Firewalls verwendet, um legitime Datenpakete für verschiedene Typen von Verbindungen zu unterscheiden. Nur Datenpakete, die einer vordefinierten Regel genügen, werden durch die Firewall durchgelassen, andere werden zurückgewiesen. Paketfilterung, oder „normale" Packet Inspection, arbeitet auf der Vermittlungsschicht (Schicht 3) und betrachtet nur den Header eines Pakets wie die Quell- und Ziel-IP-Adresse. Deep Packet Inspection (DPI) ist eine Firewall-Technologie, die auf der Anwendungsschicht (Schicht 7) des OSI-Modells arbeitet. DPI ermöglicht die Untersuchung des Inhalts von übertragenen Datenpaketen, wie der Kommunikation über HTTP und von Internet-Telefonie (VoIP)-Inhalten.

Anbieter solcher „triple-play"-Dienste können – technisch gesehen – ein noch detaillierteres Profil des Kommunikationsverhaltens ihrer Kunden erlangen. Mit dem Entstehen neuer und innovativer Dienste wie Telemedizin können darüber hinaus mehr und mehr besonders sensible personenbezogene Daten (wie Gesundheitsdaten) über Einrichtungen übertragen werden, die von Internet-Zugangsdiensteanbietern angeboten werden.

Die Arbeitsgruppe hat erhebliche Vorbehalte gegen den Einsatz von DPI für jegliche Zwecke außer der Gewährleistung der Sicherheit von Informationssystemen und -netzen innerhalb einer Organisation[2], oder soweit es sonst durch das anwendbare Recht erlaubt oder gefordert wird.

Die Arbeitsgruppe insbesondere besorgt, dass jegliche zusätzliche Anwendung von DPI durch Internet-Zugangsdiensteanbieter und andere Internetdiensteanbieter in einer weiteren Erosion des Fernmeldegeheimnisses münden wird. Sie wird auch die Vertrauensbeziehung zwischen diesen Anbietern und ihren Kunden beschädigen.

Die Anwendung von DPI bei Internet-Zugangsdiensteanbietern kann in der Informationsgesellschaft auf das Äquivalent des Abhörens von Telefongesprächen hinauslaufen. Die Gruppe unterstreicht ihre Position, die bereits in früheren Veröffentlichungen niedergelegt ist, dass Netzwerk- und Diensteanbieter (einschließlich Internet-Zugangsdiensteanbieter) prinzipiell jegliche Inhalte einer Kommunikation nicht abhören oder stören dürfen, außer wo dies durch das anwendbare Recht ausdrücklich erlaubt oder gefordert wird[3] (informationelle Gewaltenteilung). Dies wird heutzutage auch unter der Überschrift „Netzneutralität" diskutiert.

Empfehlungen

Im Lichte des oben gesagten fordert die Arbeitsgruppe Internet-Zugangsdiensteanbieter auf, insbesondere die Nutzung von DPI-Technologie für zielgerichtete beziehungsweise verhaltensbasierte Werbung zu unterlassen.

Zusätzlich fordert die Arbeitsgruppe die vermehrte Anwendung sicherer Ende-zu-Ende-Verschlüsslungsmechanismen. Das (optionale) Angebot solcher Technologien sollte gesetzlich vorgeschrieben werden wo dies nicht bereits der Fall ist, wenigstens für Anbieter, deren Dienste die Verarbeitung besonders sensitiver Daten beinhalten (z. B. Online-Banking, Nutzungen, die Kreditkarteninformationen beinhalten, Gesundheitsdaten, usw.) wie auch für Anbieter von Kommunikationsdiensten (wie E-Mail, Chat, Internettelefonie – VoIP, usw.)[4].

---

[2] Vergleiche Arbeitspapier zu Intrusion Detection–Systemen (IDS) (Berlin, 02./03.09.2003); http://www.datenschutz-berlin.de/attachments/229/enum_de.pdf

[3] Vergleiche gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz – zehn Gebote zum Schutz der Privatheit im Internet (Berlin, 13./14.09.2000); http://www.datenschutz-berlin.de/attachments/215/tc_de.pdf

[4] Vgl. Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet (Budapest-Berlin Memorandum) (Berlin, 19.11.1996), Punkt 7 auf Seite 2; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf

Arbeitspapier „Mobile Verarbeitung personenbezogener Daten und Datensicherheit“

Hintergrund

Im April 2004 hat die Arbeitsgruppe ein Arbeitspapier über potenzielle Risiken für die Privatsphäre in Verbindung mit drahtlosen Computernetzwerken *(engl. wireless networks)* angenommen.[1]

Seither wird durch die stark steigende Verbreitung und Vielfalt von mobilen Geräten, wie zum Beispiel Mobiltelefonen, Smartphones, Laptops und PDA's, einhergehend mit der ständigen Verfügbarkeit von öffentlichen Kommunikationsnetzen eine Verarbeitung jeglicher Art von vertraulichen und persönlichen Daten auf potenziell unsicheren Geräten in potenziell unsicheren öffentlichen Umgebungen immer einfacher.

Der Einsatz mobiler Geräte ist nicht ausschließlich auf die Pflege von Kontaktdaten und die Bearbeitung von Kalendereinträgen beschränkt. Vielmehr ist ein Zugriff auf vertrauliche und persönliche Informationen in Unternehmens-Datenbeständen oder die Nutzung von Cloud-Computing-Diensten bequem möglich.

Die stetig steigenden Speicherkapazitäten der mobilen Geräte und die immer schneller werdenden drahtlosen Netzwerke erlauben eine mobile Datenverarbeitung in einer Art und Weise, die in der Vergangenheit nur in festen und sichereren Umgebungen möglich war. Die verstärkte Integration mobiler Anwendungen in herkömmliche betriebliche IT-Infrastrukturen und Prozesse hat zur Folge, dass zunehmend vertrauliche, persönliche sowie geschäftskritische Daten nicht nur in zentralen Systemen abgespeichert sind, sondern auf den mobilen Geräten bearbeitet werden. Dies kann sich unmittelbar auf die Integrität, Vertraulichkeit und Sicherheit der Daten auswirken.

Zudem werden mobile Geräte vermehrt zur Archivierung und temporären Speicherung von Daten genutzt, was die Risiken von Datenverlust oder Veröffentlichung mit sich bringt.

Datenschutz und Datensicherheitsrisiken

Naturgemäß besitzen mobile Geräte eine kleine Bauform und ein geringes Gewicht. Die größten Gefahren für die Datensicherheit liegen in der Manipulation, dem Verlust und dem Diebstahl der Daten. Zur Erkennung einer Datenmanipula-

[1] http://www.datenschutz-berlin.de/attachments/196/1_de.pdf?1215693415

tion existieren geeignete Mechanismen zur Sicherung der Datenintegrität. Während der Verlust von Daten sofort erkennbar ist, wird ein Datendiebstahl oftmals erst dann bemerkt, wenn die Daten selbst oder das Ergebnis einer Bearbeitung an einem anderen Ort wieder auftauchen.

Es ergeben sich durch den Einsatz mobiler Geräte eine Reihe von spezifischen Risiken:

- Verbindungen zu öffentlichen Netzwerkzugängen (z. B. offene Internetzugänge in Restaurants, Hotels, Internetcafes usw.), ungeachtet der Anschlussart (z. B. Verbindung mit Netzwerkkabel oder Wireless LAN), alleinig mit einem nicht vertrauenswürdigen Netzwerk. Zumindest die Verbindungsdaten oder unter Umständen sogar die Inhaltsdaten können abgehört und mitgelesen werden. Das Abhören vertraulicher Informationen in der Kommunikation ist nicht nur für den Betreiber des Netzwerks, sondern, bei nicht ausreichenden Sicherheitsvorkehrungen im entsprechenden Netzwerksegment, von jedem Netzwerkanschluss aus möglich.

- Bei der Verwendung offener unverschlüsselter drahtloser Netzwerkzugänge, sogar bei sonst sicherer Netzwerkverbindung, kann die Nutzerkommunikation unbemerkt ausspioniert werden.

- Durch die laufende unbemerkte Auswertung von Standortdaten eines mobilen Geräts, z. B. durch im Hintergrund laufender standortbezogener Dienste (*Location Based Services – LBS*), kann ein Bewegungsprofil des Nutzers erstellt werden.[2]

- Angriffe auf die Verfügbarkeit von mobilen Geräten sind unter Umständen leichter durchführbar (z. B. Störsignale auf den entsprechenden Frequenzbändern) als vergleichbare Attacken auf Arbeitsplatzrechner.

- Durch die Nutzung von Kurzstreckenfunkverbindungen wie z. B. Bluetooth, die es einem Angreifer unter Umständen ermöglichen, die Kontrolle eines ungeschützten Geräts zu übernehmen.

Zudem ergeben sich Risiken im Zusammenhang mit der Speicherung und der direkten Datenverarbeitung auf mobilen Geräten:

- Mobile Geräte werden oft vom Anbieter mit zahlreichen zusätzlichen Anwendungen zur Datenverarbeitung ausgeliefert. Von einem seriösen Anbieter ist zu erwarten, dass dieser entdeckte Mängel und Verwundbarkeiten vor der Veröf-

[2] Gemeinsamer Standpunkt der IWGDPT zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, http://www.datenschutz-berlin.de/attachments/192/local_neu-de.pdf

fentlichung der Software behebt. Allerdings können andere Firmen und Privatpersonen durch teilweise offene und dokumentierte Programmierschnittstellen und Entwicklungsumgebungen Software (so genannte „Apps“) für mobile Geräte entwickeln und über das Internet einfach und kostengünstig verbreiten. Durch die Installation solcher Fremdanwendungen von Dritt-Anbietern steigt das Risiko der Infektion durch Schadsoftware bzw. der Datenbeschädigung durch unsichere Applikationen. Die Stabilität des gesamten Systems kann durch die nachträgliche Installation von nicht beglaubigter (zertifizierter) Drittsoftware beeinträchtigt werden.[3]

- Durch die Entwicklung einheitlicher Betriebssysteme und Standards für mobile Geräte wird zwar die Softwareentwicklung vereinfacht. Diese Standardisierung kann aber bei Verwundbarkeiten zu einem erhöhten Risiko der Verbreitung von Schadsoftware führen, wie es bereits in der Welt des „personal computing“ sichtbar ist. Allerdings ermöglichen einheitliche Betriebssysteme die Implementierung einheitlicher Sicherheitsmaßnahmen.

- „Push-Dienst“ oder „Server-Push-Dienst“ beschreibt eine meist internetbasierte Methode der Inhaltsverbreitung. Dabei werden Informationen von einem zentralen Server direkt an das mobile Geräte exportiert und dort unmittelbar verarbeitet. Durch eine ungeprüfte Verarbeitung der eingehenden Nachrichten entstehen Risiken, die heute aus dem Bereich der Email-Verarbeitung auf Arbeitsplatzrechnern bereits bekannt sind (z. B. Schadsoftware in Anhängen, Ausnutzung von Schwachstellen in der Verarbeitungssoftware, usw.).

Die Erfahrung zeigt, dass eine Balance zwischen der Implementierung von zu restriktiven und möglicherweise von den Nutzern daher nicht akzeptierten Sicherheitsvorgaben im Umgang mit mobilen Datenträgern sowie Geräten einerseits und der Bereitstellung eines sicheren Umfelds mit ausreichendem Schutz der Daten andererseits gefunden werden muss.

Die bloße Verschlüsselung der Daten und sensitiver Informationen *ohne* die Anwendung begleitender Maßnahmen und von Verhaltensstandards ist *kein* effektiver Weg, um jeglichen Risiken und Sicherheitsbedenken zu begegnen.

Empfehlungen

Basierend auf den oben angeführten Risiken richtet die Arbeitsgruppe folgende (vorläufige) Empfehlungen an Anbieter und Nutzer mobiler Endgeräte.

[3] Im gegenständlichen Arbeitspapier bleiben sämtliche Aspekte der Privatsphäre im Zusammenhang mit Drittanbieter-Software unberücksichtigt.

Anbieter

Die grundlegenden Sicherheitseinstellungen des mobilen Geräts sollten bei der Auslieferung das höchste Maß an Sicherheit berücksichtigen und im Einklang mit dem Zweck stehen, für den das Gerät vermarktet wird.

Ein oder mehrere Nutzerprofile mit konfigurierbar eingeschränkten Rechten sollte existieren, zusammen mit einem „Super-User", der den Zugriff auf die Sicherheitseinstellungen für diese Nutzerprofile kontrollieren und einschränken kann.

Der Nutzer sollte in einfacher Weise über jegliche Änderung an den Sicherheitseinstellungen informiert werden. Dies könnte zum Beispiel bei der Aktualisierung von Systemsoftware (z. B. Firmware- oder Betriebssystem-Update) oder durch die Installation von zusätzlichen Anwendungen der Fall sein.

Das Handbuch sollte jedenfalls ein eigenes Kapitel zum Thema „Sicherheit" und den „Sicherheitseinstellungen" enthalten. Dabei sollte auf die Risiken der Benutzung mobiler Geräte eingegangen und dem Nutzer ein übersichtlicher und verständlicher Leitfaden zur sicheren Handhabung gegeben werden.

Eingebaute Hardwarekomponenten und Schnittstellen, die zur Erhebung und Übermittlung von Daten dienen (z. B. Kamera, GPS, Mikrofon, IrDA, Bluetooth, WLAN, usw.), sollten werksseitig deaktiviert sein; diese Schnittstellen sollte, abhängig von den Rechten des entsprechenden Nutzerprofils, für den Nutzer verfügbar sein, und bei Bedarf aktiviert werden können.

Bei Mobiltelefonen kann der unbefugte Zugriff auf die SIM-Karte durch eine PIN geschützt werden. Über eine entsprechende Sicherheitseinstellung sollte dieser Zugriffsschutz auf den Telefonspeicher ausgeweitet werden können. Ein Nutzer sollte eine Zeitspanne bestimmen können, nach der das Gerät bei Inaktivität das Display/Tastatur sperrt und erst wieder nach erneuter Eingabe der PIN oder eines frei wählbaren Passworts freigibt.

Zur Kommunikation

Ein Nutzer sollte gewarnt werden, wenn möglicherweise unsichere Kommunikationskanäle für die Datenübertragung genutzt werden.

Wenn ein mobiles Gerät den Kontakt zu einer sicheren WLAN-Verbindung verliert und sich anschließend automatisch mit einem unsicheren WLAN Netzwerk verbindet, sollte eine Warnung an den Nutzer ausgegeben werden.

Es sollte für einen Nutzer einfach erkennbar sein, ob externe Kommunikationskanäle und Schnittstellen aktiv oder inaktiv sind. Zusätzliche Dienste, wie z. B.

Schnittstellen für die Kommunikation, sollten auf einem mobilen Gerät durch den Nutzer einfach ein- und ausgeschaltet werden können.

Zur Speicherung und Datenverarbeitung

Bei der nachträglichen Installation oder dem Herunterladen von nicht beglaubigter (zertifizierter) Software eines Drittanbieters sollte ein entsprechender Warnhinweis an den Nutzer ausgegeben werden.

Ein Nutzer sollte vor dem Herunterladen und vor der Installation von Applikationen die Möglichkeit haben, insbesondere den Namen und die elektronische Signatur des Anbieters, die Nutzungsbedingungen, die zur Ausführung erforderlichen Zugriffsrechte auf Gerätehardware sowie bereits installierter Software, Hinweise zur Deinstallation als auch weitere sicherheitsrelevante Informationen und Warnhinweise in einfacher Weise und in einer selbst gewählten Sprache einzusehen.

Ein Nutzer sollte die Möglichkeit haben, den Zugriff jeder installierten Applikation auf die verfügbare Gerätehardware (z. B. Netzwerkkarte, Kamera, usw.) sowie auch auf gespeicherte Daten (z. B. auf den Kalender oder das Adressbuch) einzuschränken.

Es sollte für den Nutzer einfach nachvollziehbar sein, welche Daten im mobilen Gerät verschlüsselt und welche unverschlüsselt abgespeichert werden.

Nutzer

Die Bewusstseinsbildung ist ein erster wichtiger Schritt zur Vorbeugung von Missbrauch, Datenverlust und Diebstahl. Die Nutzer sollten auf ihre Eigenverantwortung im Zusammenhang mit der Datensicherheit und Integrität hingewiesen werden. Unterstützend dazu folgende Empfehlungen:

Der Nutzer sollte nach einer Aktualisierung der Systemsoftware (z. B. Firmware-Update) die lokalen Sicherheitseinstellungen des mobilen Geräts überprüfen und wenn erforderlich auf die eigenen Bedürfnisse anpassen.

Bei Verwendung eines mobiles Geräts in einem öffentlichen Bereich, sollte der Nutzer alle Anstrengungen unternehmen, um sicherzustellen, dass der Bildschirm und die Tastatur durch Passanten oder Überwachungskameras eingesehen werden kann.

Bei der Nutzung mobiler Geräte eines Unternehmens, sind die durch die Fachabteilung erarbeiteten organisatorischen Maßnahmen unbedingt einzuhalten. Technische Manipulationen und Änderungen an den Systemeinstellungen sollten unterlassen werden.

Zur Kommunikation

Öffentliche Internetzugänge sollten mit Vorsicht verwendet werden. Vertrauliche Informationen und Daten sollten nicht über unsichere Netzwerkverbindungen verarbeitet werden, wenn die Übertragung nicht ausreichend durch zusätzliche Sicherheitsmaßnahmen, wie z. B. einen virtual private network (VPN)-Tunnel, geschützt ist.

Vor dem Austausch von *vertraulichen* Informationen sollte die Identität des Kommunikationspartners geprüft werden. Jede unbekannte Meldung oder Unregelmäßigkeit im Betrieb sollte hinterfragt und im Zweifel ein Experte oder in einem Firmenumfeld die verantwortliche Stelle Informiert bzw. zu Rate gezogen werden.

Für den unmittelbaren Betrieb nicht benötigte Schnittstellen sollten über die Einstellungen des mobilen Geräts deaktiviert werden (z. B. Einrichtungen zur Datenübertragung mit Bluetooth, Infrarotsignalen (IrDA), drahtlosen Netzwerken (WLAN), usw.). Speziell standortbezogene Dienste (*Location Based Services – LBS*) sollten deaktiviert sein, wenn sie nicht unmittelbar genutzt werden.

Zur Speicherung und Datenverarbeitung

Vor der Installation von Fremdapplikationen sollte die Quelle genau geprüft werden. Signaturen und Herstellerangaben können das Risiko einer Infektion minimieren. Im Zweifel sollte von einer Installation abgesehen werden.

Der Zugriff der installierten Fremdapplikationen sollte auf die für den ordnungsgemäßen Betrieb erforderlichen Daten eingeschränkt werden. So benötigt zum Beispiel nicht jede Anwendung den Zugriff auf das Adressbuch oder den Kalender des mobilen Geräts.

B. Dokumente zur Informationsfreiheit

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließung der 20. Konferenz am 24. Juni 2010 in Berlin

Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten

Die Informationsfreiheit erfasst grundsätzlich alle Formen und Bereiche öffentlich-rechtlichen Handelns. Ihr Ziel ist es, Verwaltungsvorgänge transparenter zu gestalten und den Menschen die politische Mitgestaltung zu erleichtern. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland weist deshalb darauf hin, dass das Recht auf Informationszugang auch gegenüber den öffentlich-rechtlichen Rundfunkanstalten als Trägern mittelbarer Staatsverwaltung gilt, sofern nicht deren grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit berührt ist.

Die Rundfunkfreiheit garantiert den Schutz vor staatlicher Kontrolle und Beeinflussung. Eine Öffnung aller Sendeanstalten außerhalb dieses geschützten Kernbereichs für die Informationsbelange der Bürgerinnen und Bürger gefährdet diese Freiheit nicht. Offenheit und Transparenz sind keine Bedrohungen, sondern schaffen Vertrauen in der Bevölkerung. Die Geltung der Informationsfreiheitsgesetze wird die Rundfunkanstalten daher in ihrem demokratischen Auftrag und Selbstverständnis nachhaltig stärken.

Die derzeitige Rechtslage ist aufgrund unterschiedlicher Landesgesetze uneinheitlich. Während in einigen Bundesländern die Anwendbarkeit des Informationsfreiheitsgesetzes ausdrücklich festgeschrieben oder ausgeschlossen ist, ergibt sie sich in anderen Bundesländern nur aus allgemeinen Regeln. Einige Sendeanstalten der ARD sind zudem in Ländern ansässig, in denen noch immer kein Informationsfreiheitsgesetz gilt.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb die Schaffung ausdrücklicher Rechtsvorschriften, sofern nicht schon vorhanden, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind.

2. Stellungnahme der Konferenz der Informationsfreiheitsbeauftragten zur Evaluation des Verbraucherinformationsgesetzes (VIG) vom 2. September 2010

Der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) gehören folgende Mitglieder an: der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Berliner Beauftragte für Datenschutz und Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der Landesbeauftragte für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, die Landesbeauftragte für Datenschutz und Informationsfreiheit Saarland, der Landesbeauftragte für den Datenschutz Sachsen-Anhalt, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt, dass die Bundesregierung die Evaluation des VIG auf eine wissenschaftliche Grundlage gestellt hat, in dem sie Gutachten bei drei unabhängigen Forschungseinrichtungen in Auftrag gegeben hat. Durch die Ergebnisse der nunmehr veröffentlichten Studien sehen sich die Informationsfreiheitsbeauftragten in Deutschland in vielen Punkten bestätigt, die sie bereits als Verbesserungsvorschläge gegenüber dem ersten Entwurf eines VIG geltend gemacht hatten (vgl. Entschließung der 12. Sitzung der Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland vom 26. Juni 2006: „Verbraucherinformationsgesetz nachbessern“). Die nachfolgende Stellungnahme orientiert sich an dem Fragenkatalog, den die Bundesregierung in ihrem Bericht über die Ergebnisse der Evaluation des VIG aufgestellt hat (BT-Drs. 17/1800, S. 9 ff.).

1. Nichtlegislative Optionen

Frage: Wie können Hemmschwellen bei den Verbrauchern für die Stellung von Informationsanträgen nach dem VIG abgebaut werden (z. B. ***durch zentral vorgehaltene und im Internet veröffentlichte Informationen*** *zum Verwaltungsverfahren bzw. -organisation sowie zu den Gebührenordnungen der einzelnen Bundesländer)?*

Die Konferenz der Informationsfreiheitsbeauftragten hält die dem VIG zugrundeliegende Ausgangsposition, dass der mündige Verbraucher im Hinblick auf die Lebensmittelsicherheit und die Transparenz des Marktes ein gesteigertes Informationsinteresse besitzt, für zutreffend (BT-Drs. 16/5404, S. 7). Ebenso hält sie die Grundannahme des Gesetzgebers, dass strukturelle Informationsasymme-

trien zu Lasten des Verbrauchers bestehen, da sein Informationsbedarf über die Selbstregulierungskräfte des Marktes nicht effektiv gedeckt werden kann, für richtig (BT-Drs. 16/5404, a. a. O.). Dass das VIG bisher überwiegend von Verbraucherorganisationen und weniger von den Verbraucherinnen und Verbrauchern in Anspruch genommen wird, dürfte daher nicht auf ein fehlendes Informationsinteresse zurückzuführen sein, sondern auf anderen, mithin auch gesetzesimmanenten Ursachen beruhen:

Ein Grund für die verhaltene Nutzung des Gesetzes dürfte zunächst darin liegen, dass die Informationsfreiheitsrechte und damit auch das VIG in der Bevölkerung noch nicht ausreichend verankert sind. Viele Menschen wissen überhaupt nicht, dass sie entsprechende Rechte besitzen. Daher sollte das VIG und die nach ihm bestehenden Transparenzrechte der Verbraucherinnen und Verbraucher in der Öffentlichkeit insgesamt bekannter gemacht werden.

Zentral veröffentlichte Informationen insbesondere zum Antragsverfahren und den Gebühren tragen dazu bei, Hemmschwellen für die Stellung von VIG-Anträgen abzubauen, und wären daher ausdrücklich zu begrüßen. Hilfreich wäre auch, wenn sich die Verbraucherinnen und Verbraucher im Internet genauer darüber informieren könnten, welche Art von Informationen bei welchen Behörden vorhanden ist. Die Behörden sollten außerdem auf die Möglichkeit der Erstellung eines Kostenvoranschlags hinweisen.

*Frage: Wäre es sinnvoll, alle **proaktiven Informationsmaßnahmen** der Behörden in einer zentralen Website **zu verlinken**?*

Grundsätzlich ist eine Verbesserung und Ausweitung proaktiver Informationsmaßnahmen der vom Anwendungsbereich des VIG erfassten Behörden zu begrüßen. Dabei wäre es sicherlich sinnvoll, wenn zunächst die jeweils betroffene Behörde diejenigen Informationen, für die sie ein Öffentlichkeitsinteresse bejaht, auf ihrer Homepage zum Abruf zur Verfügung stellen würde.

Eine bundes- bzw. landesweite Verlinkung der Informationsmaßnahmen aller Behörden in einer zentralen Webseite wäre sicherlich zu befürworten. Die Realisierbarkeit dieses ehrgeizigen Projekts sollte daher ernsthaft geprüft werden. Dabei wären durch die Gestaltung der Webseite die Übersichtlichkeit und Verständlichkeit der Informationen für die Verbraucherinnen und Verbraucher zu gewährleisten. Auch müsste die Webseite regelmäßig gepflegt und stets auf dem aktuellen Stand gehalten werden.

2. Abstimmung und Systematisierung des Informationszugangsrechts

Frage: Welche Argumente sprechen für bzw. gegen die nachfolgend (siehe BT-Drs. 17/1800, S. 9 f.) skizzierten politischen Optionen (Option 1: „große Lö-

sung"; Option 2: „Modellgesetz"; Option 3: „Ausweitung des Anwendungsbereichs des VIG"; Option 4: „sektorspezifischer Ansatz"; Option 5: „kombinierter Ansatz")?

Die Informationsfreiheitsbeauftragten des Bundes und der Länder haben bereits mehrfach – zuletzt in einer Entschließung der 19. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 16. Dezember 2009 – gefordert, die Regelungen zum Informationszugang der Bürgerinnen und Bürger zu vereinheitlichen. Gegenwärtig existiert eine Vielzahl von Informationszugangsregelungen (IFG, UIG, VIG, spezialgesetzliche und landesrechtliche Regelungen), deren Abgrenzung und Verhältnis zueinander oft unklar oder widersprüchlich ist. Vergleichbare Sachverhalte werden oft unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Ausnahmeregelungen, die Fristen zur Beantwortung von Anfragen, die Gebühren und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Rechte der Bürgerinnen und Bürger und trägt zu Unsicherheiten bei der Rechtsanwendung der Behörden bei.

Um hier Abhilfe zu schaffen und den Gedanken von Informationsfreiheit und Transparenz insgesamt zu stärken, sollten – entsprechend Option 2 – die Vorschriften des IFG, des UIG und des VIG horizontal auf Bundesebene in einem einheitlichen Gesetz zusammengeführt werden, welches dann als Vorbild für die Ländergesetzgebung dienen kann. Für eine solche Lösung haben sich auch die Regierungsparteien in ihrem Koalitionsvertrag ausgesprochen.

Die Vorschriften des einheitlichen Bundesgesetzes sollten so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Es sollte eine möglichst umfassende, materielle Vereinheitlichung erfolgen, um die bestehenden unterschiedlichen Regelungen vergleichbarer Sachverhalte durch eine einzige zu ersetzen. Eine lediglich formale Zusammenführung unter Beibehaltung unter Beibehaltung der Unterschiede – beispielsweise in Form eines Artikelgesetzes – sowie eine Vereinheitlichung auf dem kleinsten gemeinsamen Nenner sind auf jedem Fall zu vermeiden.

Sollte entgegen der hier befürworteten Lösung keine Zusammenführung von IFG, UIG und VIG erfolgen, bedarf es dringend einer Ausweitung des Anwendungsbereichs des VIG (Option 3). Eine Ausweitung des Anwendungsbereichs empfiehlt sich dabei aus mehreren Gründen: Ein Informationsbedürfnis der Bürgerinnen und Bürger besteht nicht nur im Hinblick auf Lebens- und Futtermittel, sondern gleichermaßen auch hinsichtlich sonstiger Produkte und Dienstleistungen. Insbesondere im Bereich der Information über Sicherheitslücken in informationstechnischen Produkten und Dienstleistungen und über Schadprogramme, der Arzneimittelaufsicht, der Finanzdienstleistungsaufsicht sowie in den Bereichen der Energieinformations- und Telekommunikationsnetze bedarf es einer

größeren Transparenz für die Verbraucherinnen und Verbraucher. Nach der bisher geltenden Rechtslage kommen hier Informationszugangsansprüche aus Spezialgesetzen (z. B. dem Arzneimittelgesetz), aus dem UIG und dem IFG in Betracht, wobei auch hier wieder die dargestellten Konkurrenzprobleme bestehen. Eine Einbeziehung dieser Bereiche in den Anwendungsbereich des VIG würde für Rechtssicherheit sorgen, da damit klargestellt wäre, dass die Verbraucherinnen und Verbraucher einen Informationszugangsanspruch nach dem VIG besitzen. Eine Einbeziehung dieser Gebiete in das VIG ist auch sinnvoll, da dieses schon jetzt Regelungen besitzt, die im Vergleich zu den anderen Gesetzen für die Verbraucherinnen und Verbraucher vorteilhafter sind. So ist z. B. das VIG das einzige Gesetz, das eine Pflicht zur Aufbereitung der Informationen kennt (§ 5 Abs. 1 S. 3 VIG).

3. Zugang zu Unternehmensinformationen

Frage: Welche – bislang nicht vorgetragenen – Argumente sprechen für, welche gegen dieEinführung eines ***allgemeinen Unternehmensauskunftsanspruches****? Wurden in den wissenschaftlichen Studien eventuell bestimmte Aspekte bzw. Argumente übersehen oder nicht richtig gewichtet?*

Die Studien lehnen die Schaffung eines direkten Informationsanspruchs gegenüber Unternehmen im Wesentlichen mit dem Argument ab, dass ein solcher Anspruch der deutschen Rechtsordnung fremd sei. Dabei wird jedoch übersehen, dass das UIG bereits direkte Informationsansprüche gegen Unternehmen kennt (vgl. § 2 Abs. 1 Nr. 2 UIG). Auch wird außer Acht gelassen, dass die Verbraucherinnen und Verbraucher schon jetzt nach den Informationszugangsgesetzen (VIG, IFG, UIG) Informationen über Unternehmen erhalten, die bei den Behörden vorhanden sind. Es ist daher nicht nachvollziehbar, dass sie bezüglich derselben Informationen keinen direkten Auskunftsanspruch gegenüber dem Unternehmen besitzen (vgl. im Übrigen auch § 40 Abs. 2 LFGB). Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat sich daher schon im Jahre 2006 für die Einführung eines unmittelbaren Rechtsanspruchs auf Informationszugang gegenüber Unternehmen ausgesprochen (Entschließung der 12. Konferenz der Informationsfreiheitsbeauftragten vom 26. Juni 2006: „Verbraucherinformationsgesetz nachbessern“).

Um als Verbraucherin oder Verbraucher verantwortungsvoll entscheiden zu können, sind Informationen erforderlich, die sich auf die Zusammensetzung eines Produkts und die Herkunft seiner Zutaten bzw. Inhaltsstoffe, aber auch auf Produktionsort und -verfahren, soziale Standards bei der Herstellung, Arbeitsbedingungen etc. beziehen können. Diese Informationen sind weniger bei den Behörden, sondern primär bei den Unternehmen selbst vorhanden. Ein Höchstmaß an Transparenz in diesen Bereichen würde nicht nur im Verbraucherinteresse liegen, sondern auch im wohlverstandenen Interesse all der Unternehmen, die sich ge-

wissen Standards verpflichtet fühlen und ihren Marktvorteil nicht in einem Verhalten suchen, das ihre Erzeugnisse diskreditieren würde, wenn die Verbraucherin oder der Verbraucher davon Kenntnis hätte. Die Transparenzrechte der Bürgerinnen und Bürger sollten daher auch durch Auskunftsansprüche gegenüber Privatunternehmen gesetzlich verankert werden.

Für die Einbeziehung auch rein privater Institutionen in das Informationszugangsrecht spricht auch ein Seitenblick zum Datenschutz. Dort wird inzwischen nicht mehr bezweifelt, dass die Datenmacht in der Privatwirtschaft eine mindestens ebenso große Gefahr für das Recht auf informationelle Selbstbestimmung darstellt wie die staatliche Datenverarbeitung, weshalb sich die datenschutzrechtlichen Anforderungen in beiden Bereichen auch immer stärker angleichen. Entsprechende Parallelen lassen sich auch mit Blick auf die Transparenzinteressen der Bürgerinnen und Bürger ziehen. Wie die Finanzkrise gezeigt hat, verfügen z. B. Unternehmen in der Finanzdienstleistungsbranche über einen enormen gesellschaftlichen Einfluss. Ihr Handeln am Markt ist jedoch bislang für den einzelnen Anleger oder Sparer kaum zu bewerten, obwohl es für diesen häufig von existenzieller Bedeutung ist. Der Einzelne sollte daher die Möglichkeit haben, auch unmittelbar von Unternehmen Informationen zu erhalten.

Frage: Inwieweit würde die Problematik des Zugangs zu Unternehmensinformationen durch die Einführung der von der Europäischen Kommission vorgeschlagenen ***allgemeinen Verpflichtung des Unternehmers zur vorvertraglichen Verbraucherinformation*** *(z. B. über die „wesentlichen Merkmale" des Produktes) gemäß Art. 5 des Vorschlags für eine Richtlinie über Rechte der Verbraucher (KOM [2008] 614 endg.) entschärft?*

Zum einen ist bereits fraglich, inwieweit die in Art. 5 des Richtlinienvorschlags vorgesehenen „allgemeinen Informationspflichten", die sich im Wesentlichen auf Angaben zur Produktbeschaffenheit und zu den Vertragsbedingungen beschränken und zudem ein vorvertragliches Verhältnis voraussetzen, überhaupt über bereits bestehende Pflichten hinausgehen. Jedenfalls bliebe der in Art. 5 der Richtlinie vorgesehene Informationsanspruch weit hinter einem grundsätzlich umfassenden Informationsanspruch des VIG zurück. Bedenken bestehen zum anderen vor allem wegen des in Art. 4 des Richtlinienvorschlags vorgesehenen Grundsatzes der Vollharmonisierung, der es den Mitgliedstaaten verbieten würde, einen weitergehenden Auskunftsanspruch gegenüber Unternehmen auf nationaler Ebene zu schaffen. Der Richtlinienvorschlag könnte daher u. U. sogar zu einer Senkung des nationalen Verbraucherschutzniveaus führen.

Frage: Welche ***freiwilligen Initiativen*** *zur Verbesserung des Informationszugangs der Verbraucher sollten seitens der Bundesregierung gefördert bzw. angestoßen werden?*

Initiativen, die freiwillige Transparenz fördern, sind generell zu begrüßen und sollten grundsätzlich unterstützt werden. Sie können aber Informationszugangsansprüche nur ergänzen und nicht ersetzen. Insbesondere bei Gütesiegeln u. ä. sind aber auch Instrumente wichtig, die einem Missbrauch vorbeugen und somit mögliche Verbrauchertäuschungen vermeiden.

Frage: Wird die Einführung eines ***In-camera-Verfahrens im Zivilprozess*** *für sinnvoll erachtet?*

Beweiserleichterungen oder die Einführung eines In-camera-Verfahrens können zwar die Position der Verbraucherinnen und Verbraucher im Zivilprozess verbessern, einen materiellen unmittelbaren Auskunftsanspruch gegenüber Unternehmen aber nicht ersetzen.

4. Optimierungsmöglichkeiten bezüglich des VIG

Frage: Im Rahmen der wissenschaftlichen Studien wurde festgestellt, dass die Zahl der Anfragen „normaler" Verbraucher im Vergleich zu denjenigen „institutioneller" Fragesteller wie Verbraucherorganisationen und Journalisten vergleichsweise gering ist. Daher ist die Bundesregierung an der Entwicklung von Handlungsoptionen interessiert, um mehr ***„normale" Verbraucher*** *dazu zu ermutigen, aktiv von ihren Informationsrechten Gebrauch zu machen (z. B. Antragstellung per einfacher Mail; Einführung einer Verpflichtung zur Weiterleitung von Anfragen an die zuständige Behörde bei Unzuständigkeit etc.). Welche sonstigen Möglichkeiten bestehen, um einen rechtlich sicheren, möglichst niedrigschwelligen und bürgerfreundlichen Informationszugang zu ermöglichen?*

Dass das VIG bisher überproportional von Verbraucherverbänden genutzt wird, dürfte im Wesentlichen darauf zurückzuführen sein, dass Informationen über Lebensmittel und Bedarfsgegenstände, zu denen das Gesetz Zugang gewährt, von den Verbraucherinnen und Verbrauchern im Rahmen einer Kaufentscheidung eher kurzfristig benötigt werden, da die entsprechenden Anschaffungen nur bedingt aufgeschoben werden können. Viele Verbraucherinnen und Verbraucher dürften wegen des Verfahrensaufwandes (Schriftform/ Drittbeteiligung), der Dauer der Informationszugangsgewährung sowie der zu erwartenden Kosten auf eine eigene Antragstellung verzichten.

Das Verfahren sollte daher insgesamt, d. h. von der Antragstellung bis zum Informationszugang, einfacher und verbraucherfreundlicher ausgestaltet werden. Das VIG weicht, ohne dass eine sachliche Rechtfertigung erkennbar ist, von dem Grundsatz der Formlosigkeit des Verwaltungsverfahrens ab. Zukünftig sollten Anträge auf Informationszugang formlos – insbesondere also auch per E-Mail – gestellt werden können, wie dies bei den Informationsfreiheitsgesetzen des Bundes und der Länder möglich ist. Außerdem sollte die Regelung zu den

Bearbeitungsfristen in § 4 Abs. 2 Satz 1 VIG insofern an § 7 Abs. 5 Satz 1 IFG angepasst werden, als die Informationen grundsätzlich unverzüglich zugänglich zu machen sind. Informationen werden – insbesondere auch im verbraucherschutzrelevanten Bereich – durch Zeitablauf schnell wertlos. Ein wirksames Zugangsrecht setzt daher eine möglichst rasche Information voraus. Außerdem sollte die Gebührenregelung bürgerfreundlicher gestaltet werden (s. u.). Hilfreich könnte z. B. auch eine an die Anforderungen des VIG angepasste Aktenführung sein, in deren Rahmen die Behörden geeignete organisatorische Vorkehrungen treffen, damit Informationen, die nach dem VIG preiszugeben sind, ohne unverhältnismäßigen Aufwand von den geheimhaltungsbedürftigen Informationen getrennt, zumindest aber gekennzeichnet werden können (vgl. zur Aktenführung auch § 14 HmbIFG). In diesem Zusammenhang sollten Unternehmen gebeten werden, die Behörden schon bei der Übermittlung von Informationen unter Darlegung des berechtigten wirtschaftlichen Geheimhaltungsinteresses auf das (potentielle) Vorliegen von Betriebs- und Geschäftsgeheimnissen hinzuweisen.

Neben den Verfahrensvorschriften dürften aber auch materielle Regelungen ein Grund für die geringe Zahl der Anfragen „normaler" Verbraucherinnen und Verbraucher gewesen sein. Das VIG stand von Anfang an wegen seines engen Anwendungsbereichs und der weit gehenden Ausnahmetatbestände in der – berechtigten – Kritik. Wer annimmt, dass sein Informationsanspruch auf Grund dieser Regelungen im Ergebnis gar nicht oder nur eingeschränkt zum Tragen kommt, wird möglicherweise von vornherein auf die Antragstellung verzichten.

Ein weiterer Grund für eine verhaltene Nutzung des VIG dürfte auch das Fehlen eines unabhängigen Ansprechpartners sein, der die Verbraucherinnen und Verbraucher bei der Antragstellung bzw. während des Verfahrens beraten und bei Streitfällen zwischen ihnen und den Behörden vermitteln kann. Während sich ein Antragsteller nach den Informationsfreiheitsgesetzen des Bundes und der Länder an den Bundes- bzw. die Landesbeauftragten für die Informationsfreiheit wenden kann, wenn er sich in seinem Recht auf Informationszugang als verletzt ansieht, und so außerhalb von aufwändigen Gerichtsverfahren in Konfliktfällen unbürokratisch und kostengünstig eine Einigung versuchen kann, fehlt im VIG eine entsprechende Anrufungsmöglichkeit. Dies wurde sowohl im Gutachten der Universität Marburg (S. 296) als auch im Gutachten der Ruprecht Karls Universität Heidelberg (S. 358) ausdrücklich kritisiert. Die Einrichtung einer entsprechenden Ombudsstelle durch § 12 IFG sowie die meisten Informationsfreiheitsgesetze der Länder hat sich – worauf auch die Studie der Universität Marburg ausdrücklich hinweist – in der Praxis bewährt.

Frage: Empfiehlt sich die ***Übernahme ausländischer Kostenregelungen*** *(d. h. Kostenfreistellung einfacher Anfragen bei gleichzeitiger voller Kostenpflichtigkeit besonders aufwändiger Anfragen)? Sollen Anfragen von Verbraucherorgani-*

sationen und/oder Journalisten von der Kostenerhebung ganz oder teilweise freigestellt werden? Wenn ja, unter welchen Voraussetzungen?

Die Gebührenregelung des § 6 Abs. 1 VIG, nach der – sofern sich die begehrten Informationen nicht auf Rechtsverstöße beziehen – kostendeckende Gebühren und Auslagen erhoben werden, gewährleistet nicht hinreichend, dass die Gebühren im Einzelfall nicht abschreckend wirken. Entsprechend den Regelungen in § 12 UIG und § 10 IFG sollte daher zumindest festgelegt werden, dass die Gebühren eine wirksame Inanspruchnahme des Informationszuganges nicht behindern dürfen (betr. Umweltinformationen siehe bereits EuGH, Urteil vom 9. September 1999, Rs. C 217/97) und einfache Auskünfte gebührenfrei sind.

Darüber hinaus könnte insbesondere die britische Kostenregelung als Vorbild dienen. Durch eine grundsätzliche Kostenfreiheit des Informationszugangs bei gleichzeitiger voller Kostenpflichtigkeit besonders aufwändiger Anfragen könnten mehr „normale", d. h. nichtinstitutionelle Verbraucherinnen und Verbraucher zur Nutzung ihrer Informationsrechte ermutigt werden. In jedem Fall ist jedoch zu beachten, dass die Voraussetzungslosigkeit des Zugangsanspruchs, d. h. das Nichtbestehen einer Begründungspflicht des Antragstellers, gewahrt bleiben muss. Aus diesem Grund sollten Sonderregelungen beispielsweise für eine kommerzielle Nutzung nicht erwogen werden. Im Übrigen besteht ohnehin die Möglichkeit der Gebührenerhebung für die kommerzielle Weiterverwendung von Informationen auf der Grundlage des Informationsweiterverwendungsgesetzes (IWG). Das Ziel einer Vereinheitlichung der Zugangsregelungen (VIG, IFG, UIG, siehe oben) beinhaltet auch eine Vereinheitlichung der entsprechenden Kostenvorschriften. Soweit eine separate Kostenverordnung nur für die Verbraucherinformationen beibehalten wird, sollten darin abweichende Kostentatbestände im Sinne der Verwaltungsvereinfachung und Bürgerfreundlichkeit möglichst vermieden werden. Eine Privilegierung institutioneller Antragsteller gegenüber den „normalen" Verbraucherinnen und Verbrauchern erscheint nicht zuletzt vor dem Hintergrund des Interesses der Bundesregierung, letztere zu einer verstärkten Antragstellung zu ermutigen, nicht sachgerecht.

*Frage: Welche **Begrifflichkeiten** (z. B. Betriebs- und Geschäftsgeheimnisse, Rechtsverstoß) sollen **legal definiert** werden? Welche Definitionen werden hierfür vorgeschlagen? Soll eine Präzisierung des Begriffs des „Rechtsverstoßes" dahingehend erfolgen, dass hiermit nur rechtskräftig festgestellte Verstöße gemeint sind? Oder sollen sog. „Beanstandungen" der chemischen Untersuchungsämter genügen?*

Betriebs- und Geschäftsgeheimnisse zählen nicht nur im VIG, sondern auch im UIG und IFG zu den wichtigsten Gründen für den Ausschluss des Informationszugangs. Das Bundesverwaltungsgericht hat in seiner Entscheidung vom 28. Mai 2009 (Az. 7 C 18/08) für den Begriff des Betriebs- und Geschäftsgeheimnisses

im Rahmen von IFG und UIG klargestellt, dass neben dem Mangel an Offenkundigkeit der unternehmensbezogenen Information ein berechtigtes Interesse des Unternehmens an deren Nichtverbreitung erforderlich ist, welches besteht, wenn die Offenlegung geeignet ist, exklusives technisches oder kaufmännisches Wissen den Marktkonkurrenten zugänglich zu machen und so die Wettbewerbsposition des Unternehmen nachteilig zu beeinflussen. Angesichts dieser höchstrichterlichen Rechtsprechung erscheint die Aufnahme einer (positiven) Legaldefinition des Begriffs in das VIG zwar nicht zwingend erforderlich. Wegen der erheblichen Bedeutung des Merkmals für die Informationsfreiheitsgesetze insgesamt würde eine Legaldefinition jedoch erheblich zur Rechtssicherheit beitragen. In jedem Fall sollte in Form eines Negativkataloges klargestellt werden, welche Unternehmensinformationen keine Betriebs- und Geschäftsgeheimnisse darstellen. Dies gilt im Rahmen des VIG – neben den durch § 2 Satz 3 i. V. m. § 1 Abs. 1 Satz 1 Nr. 1 VIG bereits ausgenommenen Informationen über Rechtsverstöße gegen bestimmte verbraucherschutzrelevante Regelungen – insbesondere für amtliche Mess-, Analyse- und Kontrollergebnisse.

Hinsichtlich des Begriffs des Rechtsverstoßes in § 1 Abs. 1 Satz 1 Nr. 1 VIG sollte klargestellt werden, dass unter einem Verstoß jedes Verhalten zu verstehen ist, das einem Gebot oder Verbot zuwiderläuft, so dass neben Bußgeld- oder Straftatbeständen auch z. B. Beanstandungen von Grenzwertüberschreitungen von dem Informationszugangsanspruch erfasst werden. Ferner sollte der Informationszugangsanspruch nicht an die rechtskräftige Feststellung des Rechtsverstoßes, sondern an die auf Tatsachen beruhende Überzeugung der zuständigen Behörde vom Vorliegen eines Rechtsverstoßes anknüpfen (vgl. VG Stuttgart, Urteil vom 26. November 2009, Az.: 4 K 2331/09; Schoch, Neuere Entwicklungen im Verbraucherinformationsrecht, in: NJW 2010, 2241, 2244). Könnten Informationen über Verstöße bis zu einer rechtskräftigen Entscheidung zurückgehalten werden, würden diese für die Verbraucherin bzw. den Verbraucher durch den Zeitablauf häufig wertlos. Gerade bei lebensmittelrechtlichen Verstößen besteht ein besonderes Interesse an schneller und aktueller Informationsgewährung. Außerdem sieht das VIG in § 2 Satz 1 Nr. 1 Buchstabe b selbst die Möglichkeit vor, auch während laufender Verwaltungsverfahren Zugang zu Informationen über Rechtsverstöße zu erhalten.

Frage: Soll der Ausschlusstatbestand der ***„sonstigen wettbewerbsrelevanten Informationen“*** *gestrichen werden? Kommt ihm angesichts der vom Bundesverfassungsgericht verwendeten Begriffsbestimmung für „Betriebs- und Geschäftsgeheimnisse“ überhaupt eigenständige Bedeutung zu?*

Der Ausnahmetatbestand der „sonstigen wettbewerbsrelevanten Informationen, die in ihrer Bedeutung für den Betrieb einem Betriebs- oder Geschäftsgeheimnis vergleichbar sind“ (§ 2 Satz 1 Nr. 2 Buchstabe c VIG) sollte im Interesse der Rechtsklarheit und praktischen Handhabbarkeit der Norm ersatzlos gestrichen

werden. Zum einen bestehen Zweifel an seiner Bestimmtheit, zum anderen ist kein eigenständiger Anwendungsbereich neben dem Schutz von Betriebs- und Geschäftsgeheimnissen erkennbar.

*Frage: Wäre die Einführung einer **allgemeinen Abwägungsklausel** sinnvoll, wonach Ausschlusstatbestände wie z. B. Betriebs- und Geschäftsgeheimnisse stets mit dem Informationsinteresse abzuwägen sind? Bei welchen „absoluten" Ausschlussgründen (z. B. öffentliche Sicherheit) soll auf eine Abwägung verzichtet werden?*

Insbesondere für den Ausnahmetatbestand „Betriebs- und Geschäftsgeheimnisse" ist eine Abwägungsklausel dringend geboten. Die Erfahrungen mit der vergleichbaren Vorschrift des § 6 Satz 2 IFG haben gezeigt, dass ein absoluter Schutz von Betriebs- und Geschäftsgeheimnissen einen wirksamen Informationszugang unverhältnismäßig beschränkt. Es gibt durchaus Betriebs- und Geschäftsgeheimnisse, bei denen das öffentliche Interesse an der Offenbarung den Schutzbedarf überwiegt.

Aber auch im Hinblick auf die sonstigen Ausnahmetatbestände wäre die Schaffung einer (allgemeinen) Abwägungsklausel nachdrücklich zu befürworten, damit im Einzelfall bestehenden überwiegenden Informationsinteressen Rechnung getragen werden kann. Als Vorbild könnte der in anderen Rechtsordnungen enthaltene sog. „public interest test" dienen. So können beispielsweise im Rahmen des britischen Freedom of Information Act die meisten Ausnahmetatbestände durch ein – stets zu prüfendes – überwiegendes öffentliches Interesse an der Offenlegung der Information überwunden werden. Im Übrigen zeigen die Regelungen § 8 Abs. 1 und 2 sowie § 9 Abs. 1 UIG, dass eine regelmäßige Abwägung zwischen dem öffentliche Informationsinteresse einerseits und dem Schutz von Betriebs- und Geschäftsgeheimnissen, Persönlichkeitsrechten, Urheberrecht und öffentlichen Geheimhaltungsgründen andererseits dem deutschen Informationszugangsrecht nicht fremd ist.

*Frage: Welche Möglichkeiten bestehen zur **Optimierung des Drittbeteiligungsverfahrens** bei der Abfrage großer Datenbestände? Wäre eine Streichung des Anhörungserfordernisses des jetzigen § 4 Absatz 1 VIG mit der Folge einer Anwendung der allgemeinen Vorschrift des § 28 VwVfG auch im Anwendungsbereich des VIG sinnvoll? In welchen Fällen könnte auf eine Anhörung betroffener Unternehmen verzichtet werden? Wäre eine Verpflichtung zur Einstufung übermittelter Informationen als Betriebs- und Geschäftsgeheimnis bereits zum Zeitpunkt der Übermittlung der Information sinnvoll?*

Die Anhörungs- bzw. Beteiligungspflichten der Behörde dienen maßgeblich dem Grundrechtsschutz durch Verfahren. Dem Dritten soll Gelegenheit gegeben werden, sich zu den entscheidungserheblichen Tatsachen zu äußern bzw. zu Fragen einer gesetzlich notwendigen Einwilligung Stellung nehmen. Eine gänzliche Streichung

des Drittbeteiligungsverfahrens nach § 4 Abs. 1 VIG kann daher – insbesondere für den Bereich personenbezogener Daten Dritter – nicht befürwortet werden. Für den Bereich der Betriebs- und Geschäftsgeheimnisse sollte jedoch klargestellt werden, dass eine Anhörung des betroffenen Unternehmens nur erfolgt, wenn die Behörde nach einer entsprechenden Prüfung tatsächliche Anhaltspunkte dafür hat, dass ein – nach o.g. Interessenabwägung schützenswertes – Betriebs- oder Geschäftsgeheimnis vorliegt. Die bloße Kennzeichnung der begehrten Information durch das Unternehmen als Betriebs- oder Geschäftsgeheimnis ohne nähere Begründung reicht hierfür nicht aus. Betreffen die begehrten Informationen bereits festgestellte Rechtsverstöße oder amtliche Untersuchungsergebnisse, sollte auf eine Anhörung der Unternehmen generell verzichtet werden.

Entsprechend der baden-württembergischen Regelung des § 3 AGVIG sollte außerdem auf eine Beteiligung Dritter ausnahmsweise verzichtet werden, wenn eine solche bereits im Rahmen eines gleichartigen Antrags auf Informationszugang innerhalb des letzten Jahres durchgeführt wurde. In diesem Fall ist der Dritte nicht schutzwürdig, weil er zu einem gleichgelagerten Sachverhalt bereits gehört wurde. Eine erneute Anhörung wäre im Regelfall daher eine bloße Förmlichkeit.

Frage: Sollen positive Bescheide über eine Informationserteilung kraft Gesetzes ***sofort vollziehbar*** *sein? Binnen welcher Frist sollten betroffene Dritte ggf. zur Einlegung von Rechtsbehelfen verpflichtet werden?*

Eine generelle sofortige Vollziehbarkeit des stattgebenden Bescheids kraft Gesetzes erscheint insofern bedenklich, als eine einmal erfolgte Informationsgewährung nicht mehr rückgängig zu machen ist. Insbesondere Dritte, die hierdurch in ihren Datenschutzrechten verletzt werden könnten, müssen die Möglichkeit haben, die Rechtmäßigkeit des Bescheids vor dessen Vollziehung überprüfen zu lassen. Zu beachten ist außerdem, dass § 4 Abs. 3 Satz 3 und 4 VIG bereits jetzt die Möglichkeit einer Anordnung der sofortigen Vollziehung im Einzelfall vorsieht, hiervon aber in der Praxis offenbar kaum Gebrauch gemacht wird. Die Behörden sollten daher in geeigneter Weise auf diese Möglichkeit hingewiesen werden. Hilfreich könnte auch die Einführung eines beschleunigten Gerichtsverfahrens für Informationszugangsprozesse sein.

5. Proaktive Information der Öffentlichkeit

Frage: Welche Ergebnisse der Lebensmittelkontrolle sollen von den Behörden ***proaktiv veröffentlicht*** *werden (z. B. sämtliche Kontrollergebnisse, alle Rechtsverstöße, nur Straftaten oder auch Ordnungswidrigkeiten, nur wiederholte und/oder besonders schwerwiegende und/oder rechtskräftig festgestellte Verstöße)? Soll eine Differenzierung zwischen gesundheitsrelevanten und sonstigen Verstößen erfolgen?*

Ergebnisse der Lebensmittelkontrolle sind für die Verbraucherinnen und Verbraucher von ganz wesentlicher Bedeutung. Die Behörden sollten daher möglichst sämtliche Kontrollergebnisse von sich aus veröffentlichen, um die notwendige Transparenz zu schaffen und zugleich die Notwendigkeit individueller Anfragen zu reduzieren. Da amtliche Mess-, Analyse- und Kontrollergebnisse nicht unter die gesetzliche Definition der Betriebs- und Geschäftsgeheimnisse im Sinne des VIG gefasst werden sollten (s. o.), wären insofern auch keine Bedenken hinsichtlich entgegenstehender Rechte der Unternehmen erkennbar.

Im Übrigen zeigt die Erfahrung des Berliner Bezirks Pankow mit dem sog. Smiley-Projekt, dass die Veröffentlichung positiver Kontrollergebnisse – im Gegensatz zur Beschränkung auf Verstöße – die Akzeptanz der betroffenen Unternehmen stärkt, da sie die eigene Regeltreue zu Werbungszwecken nutzen können.

Veröffentlichte Informationen sollten stets in verständlicher Weise aufbereitet werden – auch, wenn es darum geht, dass die Verbraucherinnen und Verbraucher erkennen können, ob es sich um gesundheitsrelevante oder sonstige Verstöße handelt. Verständlichkeit ist eine wesentliche Voraussetzung, um das Recht auf Informationszugang effektiv wahrzunehmen.

*Frage: **Welcher Grad an Ermessen** soll den vor Ort zuständigen Behörden zugestanden werden („Kann"-, „Soll"-, „Muss"-Bestimmung)? Reichen die bestehenden Regelungen des § 5 Absatz 1 Satz 2 VIG, § 40 LFGB mit Blick auf die notwendige Flexibilität für die handelnden Behörden zur Berücksichtigung von Einzelfallbesonderheiten als gesetzliche Ermächtigungen aus? Sind ggf. unter-gesetzliche Maßnahmen angezeigt und wenn ja, welche? Welche Regelungsdichte ist zur Sicherstellung einer angemessenen Rechtssicherheit für die handelnden Behörden nötig?*

§ 5 Abs. 1 Satz 2 VIG-E sieht vor, dass die zuständige Stelle Informationen, zu denen Zugang zu gewähren ist, auch unabhängig von einem Antrag über das Internet oder in sonstiger Weise öffentlich zugänglich machen kann. Die Ausgestaltung dieser Regelung als Kann-Vorschrift greift zu kurz. Ein aktives Informationsverhalten der Behörden ist ein wesentlicher Faktor für mehr Transparenz. Es erleichtert den Verbraucherinnen und Verbrauchern den Informationszugang und reduziert zugleich den Verwaltungsaufwand der Behörden bei der Bearbeitung von Einzelanträgen. Daher sollte entsprechen § 11 Abs. 3 IFG geregelt werden, dass geeignete Informationen allgemein zugänglich gemacht werden sollen.

Die gegenwärtige Soll-Regelung des § 40 LFBG zur aktiven Information durch die Behörden über Gesundheitsgefahren, Rechtsverstöße, Funde von ekelerregenden Lebensmitteln u. Ä. sollte in eine Muss-Bestimmung umgewandelt werden. Es hat sich gezeigt, dass in diesen Fällen noch viel zu selten „Ross und Reiter" genannt werden.

*Frage: In welchen Fallgestaltungen sollte eine **Anhörung betroffener Dritter** ggf. zur Gewährleistung einer zeitnahen Information der Öffentlichkeit unterbleiben? Welche sonstigen Maßnahmen im Spannungsfeld einer möglichst zeitnahen, Aktualität gewährleistenden Veröffentlichungspraxis und der angemessenen Wahrung verfassungsmäßiger Rechte betroffener Dritter sind zur Verfahrensbeschleunigung möglich?*

Nach der gesetzlichen Systematik ist die Information der Öffentlichkeit durch die Behörde die ultima ratio, da zuvor andere ebenso wirksame Maßnahmen, insbesondere die Information der Öffentlichkeit durch den Unternehmer selbst nicht rechtzeitig möglich gewesen sein müssen (vgl. § 40 Abs. 2 LFGB). Auf eine Anhörung kann daher grundsätzlich nicht verzichtet werden, da die Behörde klären muss, ob der Unternehmer zur rechtzeitigen Information der Öffentlichkeit in der Lage ist. § 40 Abs. 3 LFBG sieht daher gegenwärtig vor, dass die Behörde, bevor sie die Öffentlichkeit informiert, den Hersteller oder Inverkehrbringer anzuhören hat, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Eine Anhörung sollte aus hiesiger Sicht vor allem dann unterbleiben, wenn sie die Information über bestehende Gesundheitsgefahren verzögern würde.

Um die Information der Öffentlichkeit zu beschleunigen, sollte die Behörde verpflichtet werden, die Anhörung unverzüglich durchzuführen. Ferner sollte die Anhörung der betroffenen Unternehmen zeitlich limitiert werden, d. h. sowohl für die Mitteilung der Behörde an das Unternehmen als auch für die Reaktion des Unternehmens jeweils eine – möglichst kurze – Frist vorgesehen werden.

Frage: Sollten die Ergebnisse positiv beschiedener Informationsanträge allgemein zugänglich im Internet veröffentlicht werden?

Nach dem US-amerikanischen Freedom of Information Act sind alle Akten, die Gegenstand einer positiv beschiedenen Informationsanfrage waren, zu veröffentlichen, wenn diese Gegenstand häufiger Anfragen sind oder dies zu erwarten ist. Die Schaffung einer ähnlichen Regelung – ggf. als Soll-Vorschrift – wäre durchaus zu befürworten, da dadurch nicht nur mehr Transparenz für die Bürgerinnen und Bürger geschaffen, sondern auch der Verwaltungsaufwand der Behörden für die Beantwortung gleichartiger Anfragen verringert würde. Solche würden entweder gar nicht erst gestellt oder könnten durch Verweis auf die Veröffentlichung leichter beantwortet werden.

gez. Dagmar Hartge

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg und Vorsitzende der Konferenz der Informationsfreiheitsbeauftragten in Deutschland im zweiten Halbjahr 2010

3. Entschließungen der 21. Konferenz am 13. Dezember 2010 in Kleinmachnow

Open Data: Mehr statt weniger Transparenz!

Die WikiLeaks-Debatte zeigt beispielhaft sowohl ein wachsendes Bedürfnis der internationalen Öffentlichkeit nach verbesserter Information und mehr Transparenz staatlichen Handelns als auch nach einem wirksamen rechtsstaatlichen Rahmen für den Zugang zu öffentlichen Informationen. Auch in Deutschland muss die Transparenz des politischen Handelns einen deutlich höheren Stellenwert bekommen, indem die rechtlichen und tatsächlichen Möglichkeiten zum Zugang zu staatlichen Informationen verbessert werden.

Die Informationsfreiheitsbeauftragten haben bereits vor vier Jahren die Verwaltungen aufgefordert, Informationen nicht erst auf Anfrage zu gewähren, sondern auch aus eigener Initiative im Internet zu veröffentlichen. Den Bürgerinnen und Bürgern soll damit der Zugang erleichtert und gleichzeitig der Aufwand für die öffentlichen Stellen mit der Bearbeitung von individuellen Anträgen auf Informationszugang reduziert werden.

Inzwischen ist einiges geschehen: Immer mehr Informationen, zum Beispiel über die Umwelt, Gerichtsentscheidungen, Parlamentsdokumente, amtliche Statistiken oder Vorlagen kommunaler Vertretungen, sind im Internet frei zugänglich. Aber immer noch fehlt ein Wegweiser durch die meist dezentral veröffentlichten Informationen ebenso wie ein einheitlicher technischer Standard, der die Weiterverwendung der Informationen erleichtern würde.

Beispiele aus dem In- und Ausland zeigen bereits heute, dass es möglich ist, eine Vielzahl von Informationen übersichtlich und über eine einheitliche Plattform zur Verfügung zu stellen. So kann Transparenz gleichermaßen einen Beitrag zur Stärkung der Demokratie und auch zur effizienten Aufgabenwahrnehmung der Verwaltung leisten.

Verträge zwischen Staat und Unternehmen offen legen!

Öffentliche Stellen des Bundes, der Länder und der Kommunen bedienen sich bei der Wahrnehmung ihrer Aufgaben vielfach privater Unternehmen: von großen Firmen, die öffentliche Infrastrukturprojekte verwirklichen, bis hin zu kleinen Betrieben, die für eine Gemeinde das Dorffest arrangieren. Dabei nimmt der Umfang des Outsourcing ständig zu und umfasst auch zentrale Felder der staatlichen Daseinsvorsorge. Die wesentlichen Inhalte und Konditionen werden dabei vertraglich fixiert.

Das Interesse der Öffentlichkeit an den Inhalten solcher Verträge ist groß, die Bereitschaft der Vertragspartner, sie offen zu legen, meist gering. Bisweilen wird privaten Geschäftspartnern sogar die Vertraulichkeit der Vertragsbestimmungen ausdrücklich zugesichert, um deren Offenbarung zu vermeiden.

Von besonderem öffentlichem Interesse sind aussagekräftige Informationen über öffentliche Gelder, die für bestimmte Leistungen bezahlt wurden, ob die Leistungen mit den zuvor ausgeschriebenen Anforderungen übereinstimmen und in welcher Höhe Steuermittel dafür aufgewendet werden. Diese Angaben dienen der Haushaltstransparenz und der Verhinderung von Korruption. Transparenz bei derartigen Verträgen ist auch deshalb besonders wichtig, weil hier nicht selten langfristige Weichenstellungen getroffen werden, die auch Parlamente späterer Legislaturperioden nicht mehr ändern können. Angaben hierüber dürfen der politischen Diskussion nicht vorenthalten werden.

Die Informationsfreiheitsbeauftragten fordern deshalb, die Verträge zwischen Staat und Unternehmen grundsätzlich offen zu legen. Die pauschale Zurückweisung von auf solche Verträge gerichteten Auskunftsbegehren unter Hinweis auf Vertraulichkeitsabreden und Betriebs- und Geschäftsgeheimnisse ist nicht länger hinnehmbar. Die Konferenz hält es deshalb für zwingend geboten, den Zugang zu entsprechenden Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies jüngst im Berliner Informationsfreiheitsgesetz (GVBl. Berlin 2010, Seite 358) geschehen ist.