ARTIKEL-29-DATENSCHUTZGRUPPE

00350/09/DE
WP 159

Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation)

Angenommen am 10. Februar 2009

Inhalt

1. Einführung 3
2. Meldung von Verletzungen des Schutzes personenbezogner Daten 4
2.1. Bemerkungen 4
2.2. Ausnahmen von der Meldung 7
3. Verkehrsdaten 7
3.1. Verarbeitung von Verkehrsdaten zu Sicherheitszwecken 7
4. IP-Adressen 8
5. Information der Datenschutzbehörden 9
6. Unerbetene Nachrichten 10
7. Browser-Einstellungen 10
8. Klagen natürlicher und juristischer Personen 11
9. Sonstige Punkte 11
10. Schlussfolgerung 12

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

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

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

gestützt auf Artikel 255 EG-Vertrag und Verordnung (EG) Nr. 1044/2001 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. EINFÜHRUNG

Am 13 November 2007 verabschiedete die Kommission einen Vorschlag für eine Richtlinie (der Vorschlag) zur Änderung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Richtlinie 2002/21/EG (Rahmenrichtlinie).

In erster Lesung verabschiedete das Europäische Parlament am 24. September 2008 Abänderungen zu diesem Vorschlag (Abänderungen des Parlaments), die am 6. November 2008 in KOM(2008) 723 endgültig von der Europäischen Kommission kommentiert wurden (Anmerkungen der Kommission).

Am 27. November 2008 erzielte der Rat der Europäischen Union eine politische Einigung (Zustimmung des Rates).

Die Artikel-29-Datenschutzgruppe möchte Stellung nehmen zu den Abänderungen des Parlaments, den Anmerkungen der Kommission und der Zustimmung des Rates.

Die Datenschutzgruppe erinnert daran, dass sie bereits zwei Stellungnahmen zu den Vorschlägen zur Überprüfung des Rechtsrahmens der EU für elektronische Kommunikationsnetze und -dienste abgegeben hat (Stellungnahme 8/2006, angenommen am 26 September 2006[2] und Stellungnahme 2/2008, angenommen am 15. Mai 2008[3]).

Obwohl die Datenschutzgruppe mit Genugtuung feststellt, dass einige ihrer früheren Empfehlungen berücksichtigt wurden, möchte sie auf erhebliche Bedenken im Zusammenhang mit den nach der ersten Lesung im Parlament und im Rat aufgeworfenen Fragen hinweisen. Die Datenschutzgruppe geht nicht auf alle Punkte ihrer früheren Stellungnahmen ein. Diese bleiben jedoch weiterhin gültig.

---

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

2 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_de.pdf

3 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_de.pdf

2. MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

2.1. Bemerkungen

Die Datenschutzgruppe unterstützt die vorgeschlagene Verschärfung von Artikel 4 der Datenschutzrichtlinie, wonach die Anbieter öffentlich zugänglicher Kommunikationsdienste Sicherheitsverletzungen zu melden haben. Derartige Meldungen können zu einem wichtigen Instrument der Datenschutzbehörden werden, um die Verpflichtung der Diensteanbieter, geeignete Sicherheitsmaßnahmen zu ergreifen, besser und wirksamer durchzusetzen.

Im Allgemeinen empfiehlt die Datenschutzgruppe das folgende Vorgehen im Zusammenhang mit der Meldung von Verletzungen des Schutzes personenbezogener Daten:

- Die zuständige nationale Regulierungsbehörde wird unterrichtet, sobald die Gefahr nachteiliger Auswirkungen[4] auf den Schutz der Privatsphäre und den Datenschutz besteht;

- betroffene Teilnehmer müssen unverzüglich in den Fällen von den Dienstleistern informiert werden, in denen die Sicherheitsverletzung wahrscheinlich negative Auswirkungen[5] auf die Privatsphäre und den individuellen Datenschutz haben, ungeachtet der Möglichkeit, dass die zuständigen nationalen Regulierungsbehörden Informationen über die Sicherheitsverletzung veröffentlichen und den Dienstleister zur Offenlegung von Informationen über die Sicherheitsverletzung zwingen;

- jeder Dienstleistungsanbieter hat Aufzeichnungen[6] aller Verletzungen des Schutzes personenbezogener Daten zu führen.

Die Datenschutzgruppe stellt ebenfalls fest, dass die drei Vorschläge (des Parlaments, der Kommission und des Rates) die Frage der Verletzung der Sicherheit und des Schutzes personenbezogener Daten äußerst unterschiedlich behandeln, insbesondere im Hinblick auf

- den Umfang der Verpflichtung (der bei den Abänderungen des Parlaments die Dienste der Informationsgesellschaft umfasst und beim Rat und der Kommission auf die öffentlich zugänglichen elektronischen Kommunikationsdienste beschränkt ist); die Datenschutzgruppe befürwortet mit Nachdruck eine Ausweitung des Umfangs der Verpflichtung auf die Dienste der Informationsgesellschaft;

- die Instanz, die über die Information von Einzelpersonen entscheidet (im Falle des Parlaments und der Kommission ist dies die zuständige Behörde, während es beim Rat der Dienstleister ist);

---

[4] Bei der Bewertung der Gefahr nachteiliger Auswirkungen sollten Elemente berücksichtigt werden wie der Umfang der von der Verletzung betroffenen Daten, ihre Art, die Auswirkungen der Sicherheitsverletzung für eine Person, beispielsweise Identitätsdiebstahl, finanzielle Verluste, Verlust von Geschäfts- oder Beschäftigungsmöglichkeiten oder eine Kombination davon sowie andere ähnliche Folgen. Die qualitativen und quantitativen Kriterien zur Beurteilung der Folgen der negativen Auswirkungen müssen im Rahmen des Komitologieverfahrens genau definiert werden, wobei zu berücksichtigen ist, dass die Behörden nicht mit geringfügigen Fällen überlastet und Einzelpersonen unnötig beunruhigt werden dürfen.

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_de.pdf

[6] Das Format dieser Aufzeichnungen sollte standardisiert werden, damit die Aufzeichnungen von den zuständigen nationalen Regulierungsbehörden überprüft werden können.

- die Art der zu meldenden Sicherheitsverletzungen (im Vorschlag des Parlaments und in den Anmerkungen der Kommission handelt es sich hierbei um alle Sicherheitsverletzungen, während es sich bei der Zustimmung des Rates nur um ernsthafte Sicherheitsverletzungen handelt);

- sowie die Personen, die benachrichtigt werden (Teilnehmer oder Einzelpersonen beim Parlament und bei der Kommission, aber nur Teilnehmer beim Rat).

Umfang der Meldung: Dienste der Informationsgesellschaft

Die Datenschutzgruppe unterstützt vehement die Abänderungsvorschläge 187/rev und 184 des Parlaments. **Eine Ausweitung der Meldung von Verletzungen des Schutzes personenbezogener Daten auf Dienste der Informationsgesellschaft ist notwendig, da diese Dienste eine immer wichtigere Rolle im täglichen Leben der europäischen Bürger spielen** und immer größere Mengen an personenbezogenen Daten verarbeiten. Online-Transaktionen mit Zugang zu elektronischen Bankdiensten, private Krankenakten und Online-Shopping sind einige Beispiele für Dienste, bei denen es zu Verletzungen des Schutzes personenbezogener Daten kommen kann, die zu erheblichen Gefahren für einen Großteil der europäischen Bürger führen können. Die Begrenzung des Umfangs dieser Verpflichtungen auf öffentlich zugängliche Kommunikationsdienste würde nur eine äußerst begrenzte Zahl der Akteure betreffen und somit die Wirkung der Meldung von Verletzungen des Schutzes personenbezogener Daten als Mittel zum Schutz der Bürger vor Gefahren wie Identitätsdiebstahl, finanziellen Verlusten, Verlust von Geschäfts- oder Beschäftigungsmöglichkeiten und physischen Schäden erheblich verringern.

Daher bedauert die Datenschutzgruppe zutiefst, dass dieser Vorschlag von Kommission und Rat nicht unterstützt wurde. Sie erinnert daran, dass einige Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation bereits über den eigentlichen Rahmen der elektronischen Kommunikationsdienste hinaus gelten[7].

Verantwortlichkeit und Kriterien für die Meldung

Die entsprechenden Diensteanbieter sollten für die Bewertung der Risiken, die durch Verletzungen des Schutzes personenbezogener Daten entstehen, verantwortlich sein. Sie sind am besten in der Lage, anhand der behördlichen Bewertungsvorschriften unverzüglich zu bestimmen, ob die betroffenen Personen benachrichtigt werden sollen. **Ungeachtet ihrer Verpflichtung, die zuständigen nationalen Regulierungsbehörden über alle Sicherheitsverletzungen zu informieren, sofern negative Folgen drohen, sollten die Diensteanbieter bestimmen, ob eine Benachrichtigung von Teilnehmern oder Einzelpersonen notwendig ist. Um sicherzustellen, dass zutreffende und einschlägige Informationen der Öffentlichkeit bereitgestellt werden, können die zuständigen nationalen Regulierungsbehörden beschließen, die Sicherheitsverletzung öffentlich zu**

---

[7] Einige Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation wie Artikel 5 Absatz 3 (Cookies und Spyware) sowie Artikel 13 (unerbetene Nachrichten) sind bereits allgemeine Bestimmungen, die nicht nur für die elektronische Kommunikation gelten.
Diese mögliche Ausweitung über den eigentlichen Rahmen öffentlich zugänglicher elektronischer Kommunikationsdienste hinaus, ist auch in anderen Fällen vorgesehen, weil die Kommission vorgeschlagen hat, den Anwendungsbereich von Artikel 5 Absatz 3 auf Fälle auszudehnen, in denen Cookies und Spyware durch Medien wie CD-ROM oder USB-Sticks verbreitet werden, die nicht zu den öffentlich zugänglichen elektronischen Kommunikationsdiensten gehören.

machen, wenn dies für notwendig erachtet wird, und den Diensteanbieter veranlassen, Informationen über die Sicherheitsverletzung zu veröffentlichen.

Da die Meldung durch den Diensteanbieter erfolgt, **muss die Richtlinie Garantien enthalten, um zu gewährleisten, dass Sicherheitsverletzungen nicht verschwiegen wurden,** die Bewertung der Sicherheitsverletzung korrekt durchgeführt wurde und Einzelpersonen, wann immer notwendig, informiert wurden.

Die Behörden werden in einer größeren Zahl von Fällen informiert, so dass sie in der Lage sind, die Information der Privatpersonen durch die Dienstleister zu überwachen. Das Format der Meldung sollte auf europäischer Ebene harmonisiert werden und objektive und eindeutige Kriterien enthalten, die die Abschätzung der Folgen der durch die Sicherheitsverletzung verursachten negativen Auswirkungen erleichtert. Ferner sollte die zuständige nationale Regulierungsbehörde prüfen, ob die Bewertung der Sicherheitsverletzung vom Diensteanbieter ordnungsgemäß durchgeführt wurde und ob nach der Verletzung des Schutzes personenbezogener Daten geeignete Maßnahmen ergriffen wurden. Um schließlich zu **verhindern, dass Sicherheitsverletzungen verschwiegen werden, muss die Richtlinie die zuständige nationale Regulierungsbehörde ermächtigen, finanzielle Sanktionen (Strafzahlungen)[8] in Fällen zu verhängen, in denen ein Diensteanbieter Einzelpersonen oder die nationale Regulierungsbehörde nicht oder unzutreffend über die Verletzung des Schutzes personenbezogener Daten informiert**.

<u>Arten der Einzelpersonen mitzuteilenden Sicherheitsverletzungen: Der Begriff der negativen Folgen</u>

Die Datenschutzgruppe begrüßt die Einführung einer Neudefinition des Begriffs "Verletzung des Schutzes personenbezogener Daten" in Artikel 2[9], wie in den Anmerkungen der Kommission vorgeschlagen[10].

Allerdings stellt die Arbeitsgruppe fest, dass die drei Vorschläge mit unterschiedlichem Wortlaut festlegen, wann Sicherheitsverletzungen den Betroffenen mitgeteilt werden sollten. Daher **empfiehlt die Datenschutzgruppe, dass Sicherheitsverletzungen den Betroffenen mitgeteilt werden sollten, wenn diese negative Auswirkungen auf die Privatsphäre und den Datenschutz haben könnten.** In dieser Hinsicht finden sich in der Zustimmung des Rates nützliche Beispiele unter Erwägung 29.

<u>Personen, die benachrichtigt werden sollten</u>

Die Datenschutzgruppe begrüßt die Hinweise auf "Teilnehmer oder Personen", auf "geschädigte Nutzer" sowie "die zuständige nationale Behörde" in Erwägung 29 der Abänderungen des Parlaments.[11] In der Zustimmung des Rates werden Meldungen auf "Teilnehmer" beschränkt und somit werden einige Verletzungen des Schutzes personenbezogener Daten, die in Stellungnahme 2/2008 beschrieben wurden, den Geschädigten nicht mitgeteilt.

---

8 Die Datenschutzgruppe stellt fest, dass entsprechende Bestimmungen vom Parlament, der Kommission und dem Rat in einem neuen Artikel 15 a Absatz 1 vorgeschlagen wurden.

9 Siehe Anmerkungen der Kommission zu den Abänderungen 187/rev und 184 des Parlaments.

10 Gleichwohl ist dieser Begriff der "Verletzung des Schutzes personenbezogener Daten" allgemeiner Natur und sollte nicht auf Daten beschränkt sein, die im Zusammenhang mit der Bereitstellung öffentlich verfügbarer elektronischer Kommunikationsdienste verarbeitet werden. Er sollte auch zumindest Dienste der Informationsgesellschaft umfassen.

11 Siehe Abänderung 183.

2.2. Ausnahmen von der Meldung

Die Datenschutzgruppe stellt fest, dass die Meldung von Sicherheitsverletzungen Informationen über die Umstände der Sicherheitsverletzung beinhalten soll, wozu auch gehört, ob die personenbezogenen Daten durch Verschlüsselung geschützt wurden. Diese Information ist für die zuständige nationale Regulierungsbehörde im Falle einer Sicherheitsverletzung entscheidend, um geeignete Maßnahmen festzulegen, die gegebenenfalls vom Diensteanbieter zu ergreifen sind.

Allerdings ist die Datenschutzgruppe gegen die Einführung von Ausnahmen hinsichtlich der Meldeverpflichtung[12], wenn Diensteanbieter "geeignete technische Schutzmaßnahmen für die betroffenen Daten" ergriffen haben. Diese Bestimmung würde die Qualität und Nützlichkeit der Informationen für die Betroffenen wesentlich beeinträchtigen. Betroffene können nur dann geeignete Maßnahmen zur Begrenzung der Gefahren, denen sie ausgesetzt sind, ergreifen, wenn sie ausreichend informiert sind. Daher verweist die Datenschutzgruppe auf die Bedeutung des Meldeformats und der Risikobewertung, um festzustellen, ob Einzelpersonen unabhängig von den technischen Maßnahmen, die tatsächlich zum Schutz ihrer Daten ergriffen wurden, informiert werden sollten.

3. VERKEHRSDATEN

3.1. Verarbeitung von Verkehrsdaten zu Sicherheitszwecken

In einem neuen Artikel 6.6 a wollen Parlament, Rat und Kommission eine neue Ausnahme in der Datenschutzrichtlinie für elektronische Kommunikation schaffen, um die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken zu erlauben.

Der Datenschutzgruppe ist bewusst, dass "Betreiber von Sicherheitsdiensten" Sicherheits-Software[13] verwenden (wie Anti-Viren- und Anti-Spam-Software, Firewalls oder Intrusionsmeldesysteme), die die Verarbeitung von Verkehrsdaten zum Schutz personenbezogener Daten der Nutzer und zum Schutz des Dienstes selbst erfordern. Gleichwohl besteht die Sorge, dass der aktuelle Wortlaut einen umfassenden Einsatz tiefgreifender Paketanalysen[14] sowohl im Netz als auch in Nutzergeräten wie ADSL-Boxen legitimiert, obwohl der derzeitige Rechtsrahmen bereits im Einzelnen die Fälle aufführt, in denen die Verkehrsdaten zu Sicherheitszwecken verarbeitet werden dürfen.

Die Rechtsgrundlagen für die Erlaubnis zur Verarbeitung von Verkehrsdaten durch öffentlich zugängliche elektronische Kommunikationsdienste und zur Verarbeitung personenbezogener Daten durch die für die Verarbeitung Verantwortlichen sind in Artikel 6 der Datenschutzrichtlinie für die elektronische Kommunikation sowie Artikel 7 und 17 der Datenschutzrichtlinie niedergelegt. Inwieweit die Verarbeitung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird, erforderlich ist, wird in Artikel 7 Absatz f der Datenschutzrichtlinie festgelegt. Die Grundrechte und Grundfreiheiten der betroffenen Personen dürfen hierdurch nicht beeinträchtigt werden. Artikel 17 der Datenschutzrichtlinie sieht ferner vor, dass der für die Verarbeitung Verantwortliche "*die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige*

---

[12] Siehe Erwägung 29 der Abänderungen des Parlaments (Abänderung 122) und Erwägungen 29 und 32 der Zustimmung des Rates.

[13] Entweder im Endgerät des Nutzers oder im Netz.

[14] Diese tiefgreifende Paketanalyse erlaubt eine äußerst intensive Feststellung und Verfolgung des Benutzerverhaltens.

Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind". Diese Maßnahmen müssen auch den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen sein.

Die Datenschutzgruppe betont ferner, dass der Umfang von Abänderungsvorschlag 180 des Parlaments in den Anmerkungen der Kommission präzisiert wurde. **Die Datenschutzgruppe nimmt zur Kenntnis, dass der von der Kommission vorgeschlagene Wortlaut ohne jeden Zweifel feststellt, dass die Verarbeitung von Verkehrsdaten in den Anwendungsbereich der Datenschutzrichtlinie fällt.** Daher haben Anbieter von Sicherheitsdienstleistungen den nationalen Datenschutzbehörden, wann immer erforderlich, Meldung zu machen und zu gewährleisten, dass die Rechte der Betroffenen wahrgenommen werden können.

Schließlich weist die Datenschutzgruppe darauf hin, dass die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken bereits in Mitgliedstaaten erfolgt, in denen Sondermaßnahmen gemäß Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation verabschiedet wurden, wonach Mitgliedstaaten Rechtsvorschriften erlassen können, um auf den Grundsatz der Anonymisierung oder Löschung von Verkehrsdaten[15] zu verzichten, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, um die unbefugte Nutzung der elektronischen Kommunikationssysteme zu verhindern.

Aus den oben genannten Gründen ist **der Vorschlag eines neuen Artikels 6 Absatz 6 a nicht erforderlich.**

4. IP-ADRESSEN

Das Parlament und die Kommission schlagen die Einführung einer neuen Erwägung 27 a über IP-Adressen vor[16].

Die Datenschutzgruppe begrüßt den in der Stellungnahme der Kommission vorgeschlagenen Wortlaut in Bezug auf seine Arbeit. Allerdings ist die Datenschutzgruppe dagegen, in einer Richtlinie explizit auf diese Frage einzugehen.

In diesem Zusammenhang **verweist sie erneut auf ihre frühere Stellungnahme[17], wonach der Internet-Diensteanbieter,** *wenn er nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmbaren Benutzern gehören, sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln muss.*

IP-Adressen beziehen sich in den meisten Fällen auf bestimmbare Personen. Bestimmbarkeit bedeutet bestimmbar durch den Zugangsprovider oder auf andere Weise mit Hilfe zusätzlicher Kennungen wie Cookies oder in Interaktionen mit Internetdiensten, wodurch die betroffene Person explizit oder implizit bestimmt wird.

In Erwägung 26 der Datenschutzrichtlinie wird eindeutig festgelegt, dass um festzustellen, ob eine Person bestimmbar ist, *alle Mittel zu berücksichtigen sind, die von dem für die Verarbeitung Verantwortlichen oder von jeder anderen Person nach vernünftiger Einschätzung zur Identifizierung der betreffenden Person genutzt werden können*.

---

15 Gemäß Artikel 6 Absatz 1.

16 Abänderung 185 des Parlaments.

17 Stellungnahme 4/2007 zum Begriff der personenbezogenen Daten und Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen.

Der Begriff der personenbezogenen Daten in der Datenschutzrichtlinie bezieht sich auf Daten, die auf eine Person bezogen sind, und IP-Adressen werden in der Regel verwendet, um zwischen Nutzern zu unterscheiden, die beispielsweise im Rahmen gezielter Werbung oder der Profilerstellung unterschiedlich behandelt werden sollen.

Die Datenschutzgruppe ist zwar bereit, die Kommission bei der Durchführung der vom Parlament[18] vorgeschlagenen Arbeiten zum Thema IP-Adressen zu unterstützen, stimmt aber mit der Kommission darin überein, dass eine materiellrechtliche Vorschrift in einer Richtlinie keine geeignete Herangehensweise an dieses Thema ist, und dass eine Berichtspflicht, die sich auf Zwecke bezieht, die nicht unter diese Richtlinie fallen, nicht angemessen ist.

5. INFORMATION DER DATENSCHUTZBEHÖRDEN

In erster Lesung hat das Parlament die Abänderung 136 zu Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation angenommen, die dann durch die Anmerkungen der Kommission abgeändert wurde. Dieser Vorschlag hätte alle Anbieter von Telekommunikationsdiensten und -netzen sowie alle Anbieter von Diensten der Informationsgesellschaft verpflichtet, der zuständigen Datenschutzbehörde alle gemäß Absatz 1 eingegangenen Anträge[19] zu melden, und diese Behörde verpflichtet, jeden Antrag zu untersuchen und an die zuständigen Justizbehörden rückzuüberweisen, wenn sie der Auffassung ist, dass die einschlägigen Bestimmungen des nationalen Rechts nicht beachtet worden sind.

Die vorgeschlagene Meldepflicht ist eine sinnvolle Ergänzung im Interesse von mehr Transparenz und größerer Kontrolle durch die Regulierungsbehörden. Obwohl diese Bestimmung zu einer erheblichen Verbesserung der Überwachung und Durchsetzungsmöglichkeiten der Datenschutzbehörde führen und somit zu einer besseren Anwendung des rechtmäßigen Zugriffs auf die Informationen bieten würde, entstünde aber auch mehr Bürokratie sowohl für die beteiligten Unternehmen als auch für die Datenschutzbehörden. In diesem Zusammenhang betrachtet die Datenschutzgruppe mit Sorge die Notwendigkeit, die zunehmende Zahl der Anträge der Justizbehörden[20] zu überwachen und wegen der neuen Verantwortung der Datenschutzbehörden jede einzelne Ermittlung der Justiz zu kontrollieren, was eine erhebliche Aufstockung der finanziellen und personellen Ressourcen dieser Behörden erfordert.

Daher **schlägt die Datenschutzgruppe vor, dass eine derartige Meldung nur einmal im Jahr erfolgen sollte. Hierbei könnten gegebenenfalls Angaben über die internen Verfahren zur Beantwortung der Anträge auf Zugang zu personenbezogenen Daten der Nutzer, die Zahl der eingegangenen Anträge, die herangezogene Rechtsgrundlage und eventuelle Probleme gemacht werden.** Wichtig ist auch, dass diese Berichtspflicht auf EU-Ebene harmonisiert und im Einzelnen ausgeführt.

---

[18] In Abänderungen 139 und 186/rev.

[19] Dort sind die in der Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) festgelegten Verpflichtungen zur Vorratsspeicherung von Daten beschrieben.

[20] Viele Betreiber von Telekommunikationsdiensten erhalten mehrere hundert Anträge pro Tag.

6. UNERBETENE NACHRICHTEN

Die Abänderung stellt klar, dass MMS und ähnliche Technologien unter die Begriffsbestimmung für „elektronische Post“ in Artikel 2 Buchstabe h fallen.

Erstens stellt die Datenschutzgruppe fest, dass in Erwägung 40 der Datenschutzrichtlinie für elektronische Kommunikation bereits klargestellt ist, dass SMS unter den Begriff „elektronische Post“ fallen.[21]

Zweitens muss Artikel 13 Absatz 1 entsprechend dem Grundsatz in Erwägung 4[22] an die technische Entwicklung angepasst werden. Der jetzige Wortlaut von Artikel 13 Absatz 1 geht von der Annahme aus, dass die betroffene Person bereits mit dem Netzwerk verbunden ist, das für die Kommunikation (beispielsweise ein Anruf oder eine elektronische Post) verwendet wird. Er betrifft nicht Fälle, in denen ein Nutzer per Werbung gebeten wird, eine Verbindung zu einem Netz herzustellen, das ausschließlich Werbezwecken dient. Dies kann bei Bluetooth-Marketinganwendungen die Regel sein.

Daher begrüßt die Datenschutzgruppe, dass die in der Stellungnahme der Kommission zum Geltungsbereich von Artikel 13 enthaltenen Klarstellungen im Wesentlichen die Verwendung des Wortes Kommunikation betreffen, und sich der neue Erwägungsgrund auf “ähnliche Technologien" bezieht. Dies gewährleistet, dass bei Bluetooth-Marketinganwendungen eine vorherige Zustimmung erforderlich ist, wodurch den Anmerkungen der Datenschutzgruppe in ihrer Stellungnahme 2/2008 Rechnung getragen wird, wonach Nutzer von kabellosen Medien mit geringer Reichweite gegen unerbetene Werbung im Sinne von Artikel 13 geschützt werden müssen. Ein ausdrücklicher Hinweis auf Bluetooth könnte auch in Erwägung 40 aufgenommen werden.

Drittens verweist die Datenschutzgruppe erneut auf ihre Anmerkungen in Stellungnahme 2/2008 über die Verwendung des Begriffs "Teilnehmer" in Artikel 13 und nimmt mit Befriedigung den in der Zustimmung des Rates vorgeschlagenen Wortlaut zur Kenntnis.

Schließlich ist der Vorschlag des Rates zur Abänderung von Artikel 13 Absatz 2 durch das Hinzufügen der Worte "zum Zeitpunkt der Erhebung der elektronischen Kontaktinformationen" ebenfalls äußerst nützlich, da er eindeutig den Zeitpunkt benennt, wann Nutzer die Nutzung ihrer elektronischen Kontaktinformationen für Zwecke der Direktwerbung ablehnen können.

7. BROWSER-EINSTELLUNGEN

Die Datenschutzgruppe ist eindeutig gegen die vom Parlament verabschiedete Abänderung 128, in der es heißt, dass die Browser-Einstellung eine vorherige Einwilligung darstellt. Auch wenn diese Änderung Teil der Anmerkungen der Kommission und der Zustimmung des Rates war, möchte die Arbeitsgruppe diese Abänderung kommentieren.

---

[21] Definiert in Artikel 2 Absatz h der Datenschutzrichtlinie für elektronische Kommunikation.

[22] Worin es heißt, dass die Richtlinie an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden muss, 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.

Abgesehen von dem formalen Problem, eine derart fachspezifische Sprache in der Richtlinie zu verwenden, ist die Datenschutzgruppe besorgt über die Aushöhlung des Begriffs Einwilligung und die sich daraus ergebende fehlende Transparenz.

Die meisten Browser verwenden Standardeinstellungen, die es nicht erlauben, dass Nutzer über die vorläufige Speicherung oder den Zugang zu ihren Endgeräten informiert werden. Daher sollten Standard-Browser-Einstellungen "datenschutzfreundlich sein", dürfen jedoch kein Mittel sein, um - wie in Artikel 2 Absatz h der Datenschutzrichtlinie vorgeschrieben - eine Einwilligung der betroffenen Person ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage zu erzielen.

Im Hinblick auf Cookies ist die Datenschutzgruppe der Auffassung, dass der für die Verarbeitung der Cookies Verantwortliche die Nutzer in der Datenschutzerklärung informieren und sich nicht auf die (Standard-)Browser-Einstellungen stützen sollte. Außerdem beschränkt sich der gewählte Wortlaut nicht nur auf das aktuelle Thema der Cookies, sondern impliziert andere neue Techniken, die zur Ermittlung des Verhaltens der Nutzer mit Hilfe ihres Browsers verwendet werden könnten.

8. KLAGEN NATÜRLICHER UND JURISTISCHER PERSONEN

Die Datenschutzgruppe unterstützt den Vorschlag des Parlaments[23], in Artikel 13 Absatz 6 die Möglichkeit aufzunehmen, dass natürliche und juristische Personen, die von Verstößen gegen einzelstaatliche Vorschriften zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation betroffen sind, gegen solche Verstöße gerichtlich vorgehen können.

Diese Bestimmung stärkt zweifellos die Nutzerrechte und trägt zur Entwicklung besserer Sicherheitsmaßnahmen auf Seiten der Industrie bei.

9. SONSTIGE PUNKTE

Abschließend stellt die Datenschutzgruppe mit Befriedigung fest

- dass der Gesetzgeber beabsichtigt, Phishing-Praktiken zu bestrafen[24];
- dass Kommission und Rat die Bitte der Datenschutzgruppe berücksichtigt hat[25], während des in Artikel 4 Absatz 4 genannten Komitologieverfahrens angehört zu werden;
- dass sie in den in Artikel 15 a Absatz 4 genannten Anhörungsprozess einbezogen wird;
- dass sie bei der Vorbereitung des Berichts über die Anwendung der geänderten Datenschutzrichtlinie für elektronische Kommunikation angehört wird[26];
- dass Kommission, Rat und Parlament klarstellen wollen, dass die Datenschutzrichtlinie für elektronische Kommunikation auch für neue Technologien wie RFID[27] und NFC, die kontaktlose Identifikationsgeräte mit Funkfrequenzen nutzen, gilt.

---

23 In Abänderung 133.
24 Siehe Abänderung 132 des Parlaments.
25 In ihrer Anmerkung zur Abänderung 127 des Parlaments.
26 Siehe Abänderung 139 und 186/rev des Parlaments.
27 In Artikel 3 und Erwägung 28.

10. SCHLUSSFOLGERUNG

Die Artikel 29-Datenschutzgruppe fordert den europäische Gesetzgeber auf, von allen in dieser Stellungnahme genannten Fragen vor allem der Ausweitung des Anwendungsbereichs der Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten auf Dienste der Informationsgesellschaft Priorität einzuräumen, da dies wesentliche Auswirkungen auf den Schutz der personenbezogenen Daten aller europäischen Bürger hat.

Brüssel, den 10.2.2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK