



**00989/08/DE
WP150**

**Stellungnahme 2/2008 zur Überprüfung der Richtlinie 2002/58/EG über die
Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der
elektronischen Kommunikation (Datenschutzrichtlinie für elektronische
Kommunikation)**

Angenommen am 15. Mai 2008

Die Datenschutzgruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, Generaldirektion Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro Nr. LX-46 06/80.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

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

gestützt auf Artikel 255 des EG-Vertrags 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 FOLGENDES DOKUMENT ANGENOMMEN:

1. HINTERGRUND

Am 13. November 2007 nahm die Kommission den Vorschlag für eine Richtlinie zur Änderung u. a. der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation („den Vorschlag“) an.

Hauptanliegen des Vorschlags ist ein verbesserter Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen in der elektronischen Kommunikation, insbesondere durch strengere Sicherheitsbestimmungen und bessere Durchsetzungsmechanismen.

Die Artikel-29-Datenschutzgruppe gibt eine Stellungnahme zum Vorschlag ab und weist auf einige zusätzliche Aspekte hin.

2. SPEZIFISCHE ANMERKUNGEN

Meldung von Sicherheitsverletzungen

Artikel 4

Die Artikel-29-Datenschutzgruppe unterstützt die vorgeschlagene Stärkung von Artikel 4 „Betriebssicherheit“, indem die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet werden, Sicherheitsverletzungen zu melden, und weist auf die Bedeutung dessen hin, alle Betroffenen darüber zu informieren, wenn personenbezogene Daten preisgegeben wurden oder ein diesbezügliches Risiko besteht. Die Artikel-29-Datenschutzgruppe ist jedoch der Auffassung, dass in diesem Artikel einige Aspekte nicht ausreichend abgedeckt sind:

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

(a) Notwendigkeit, auch Dienste der Informationsgesellschaft zur Meldung von Sicherheitsverletzungen zu verpflichten

Die Artikel-29-Datenschutzgruppe schließt sich der Stellungnahme des Europäischen Datenschutzbeauftragten² vollumfänglich an, die festhält, dass die Einführung eines Systems zur Meldung von Sicherheitsverletzungen, wie in Artikel 4 Absatz 3 und Absatz 4 beschrieben, auch auf Dienste der Informationsgesellschaft wie Online-Banken, Online-Unternehmen, Online-Anbieter von Gesundheitsdienstleistungen usw. ausgedehnt werden sollte.

Den Geltungsbereich auf Dienste der Informationsgesellschaft im Allgemeinen auszuweiten, würde zur einer stärkeren Übernahme von Verantwortung durch diese Dienste und zur Bewusstseinsbildung in der Öffentlichkeit beitragen. Dadurch würde zweifellos ein Beitrag zur Verringerung der Sicherheitsrisiken geleistet.

(b) Empfänger der Meldungen von Sicherheitsverletzungen

Die Datenschutzgruppe ist der Auffassung, dass der Empfängerkreis der Meldungen von Sicherheitsverletzungen weiter gefasst werden sollte, sodass darin alle Betroffenen enthalten sind, nicht nur die „Teilnehmer“, indem das Wort „Teilnehmer“ in Artikel 4 durch „Betroffene“ ersetzt wird.

Die Formulierung „Betroffene“ würde alle Personen beinhalten, deren Daten durch die Sicherheitsverletzung tatsächlich preisgegeben wurden (d. h. Teilnehmer, aber auch ehemalige Teilnehmer und bestimmte Dritte).

Dies kann beispielsweise besonders dann relevant sein, wenn ein Teilnehmer einen Dienst kürzlich abbestellt hat, also nicht mehr „Teilnehmer“ ist, seine Daten jedoch noch beim für die Datenverarbeitung Verantwortlichen (d. h. dem Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes) gespeichert sind. Eine andere hypothetische Situation, die dafür spricht, den Empfängerkreis der Meldungen von Sicherheitsverletzungen weiter zu fassen, ist, wenn Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste Informationen über eine Person A speichern, die sich gar nicht für den Dienst angemeldet hat. Dies kann der Fall sein, wenn die Informationen von einem Teilnehmer des Dienstes übermittelt wurden, der A dazu aufgefordert hat, sich für den Dienst anzumelden. Wenn aufgrund einer Sicherheitsverletzung Informationen über A preisgegeben werden, sollte A daher über diesen Umstand in Kenntnis gesetzt werden.

Dies wäre auch der Fall, wenn die Meldung über eine Sicherheitsverletzung Dienste der Informationsgesellschaft betrifft. Tatsächlich können Nutzer mit verschiedenen Diensten der Informationsgesellschaft interagieren, ohne Teilnehmer zu sein.

(c) Veröffentlichung

Die Datenschutzgruppe schlägt vor, die nationalen Regulierungsbehörden im öffentlichen Interesse unter bestimmten Umständen zu ermächtigen, die Öffentlichkeit über eine Sicherheitsverletzung in Kenntnis zu setzen oder die betroffenen Unternehmen

2

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf

dazu zu verpflichten, dies zu tun. Die nationale Regulierungsbehörde sollte abschätzen, ob ein Fall der Veröffentlichung bedarf, und dabei die Interessen der Betreiber gegen jene der Betroffenen abwägen.

Artikel 4 Absatz 4

Gemäß Artikel 4 Absatz 4 kann die Kommission nach Absprache mit der Europäischen Behörde für die Märkte der elektronischen Kommunikation und dem Europäischen Datenschutzbeauftragten gegebenenfalls technische Durchführungsmaßnahmen in Bezug auf Umstände, Format und Verfahren im Zusammenhang mit den in Artikel 4 vorgesehenen Informations- und Meldungspflichten treffen.

(a) Wahl des Ausschussverfahrens

Die Artikel-29-Datenschutzgruppe begrüßt den Ansatz des Vorschlags, eine Vielzahl wichtiger Fragen betreffend die Weitergabe von Informationen an natürliche Personen und Datenschutzbehörden durch Ausführungsbestimmungen anstatt im Kontext der Datenschutzrichtlinie für elektronische Kommunikation anzugehen.

(b) Notwendigkeit der Konsultation der Artikel-29-Datenschutzgruppe

Zusätzlich zur Europäischen Behörde für die Märkte der elektronischen Kommunikation und zum Europäischen Datenschutzbeauftragten sollte auch die Artikel-29-Datenschutzgruppe konsultiert werden, da sich alle eingeführten Maßnahmen unmittelbar auf die Informationen auswirken, die den Betroffenen mitgeteilt werden müssen.

Konzept der „personenbezogenen Daten“

Die Datenschutzgruppe begrüßt den Umstand, dass Definition und Umfang des Begriffs „*personenbezogene Daten*“ im Vorschlag mit der entsprechenden Definition in der Datenschutzrichtlinie vereinbar sind und betont, dass eine Einschränkung des Umfangs der Definition des Begriffs „*personenbezogenen Daten*“ in der Datenschutzrichtlinie für elektronische Kommunikation eine Lücke beim Schutz natürlicher Personen in einem Kernbereich der elektronischen Kommunikation – und in der Folge auch bei Diensten der Informationsgesellschaft und eGovernment-Diensten, die auf elektronischen Diensten basieren – verursachen würde und daher aus der Sicht des Datenschutzes inakzeptabel wäre.

Konzept des „öffentlichen Kommunikationsnetzes“ und der „elektronischen Kommunikationsdienste“

Die Datenschutzrichtlinie für elektronische Kommunikation gilt für die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen. In der Praxis erweisen sich die Konzepte „*öffentliches Kommunikationsnetz*“ und „*elektronische Kommunikationsdienste*“ jedoch sehr oft als unklar. Die Dienste verwandeln sich zunehmend in eine Mischung privater und öffentlicher Elemente. Häufig ist es für Regulierungsgremien und Interessengruppen gleichermaßen schwierig, festzustellen, ob die Datenschutzrichtlinie für elektronische Kommunikation in einer bestimmten Situation anwendbar ist. Ist beispielsweise die Bereitstellung eines Internetzugangs für 30.000 Studierende ein öffentliches elektronisches Kommunikationssystem oder ein privates? Was, wenn ein multinationales

Unternehmen seinen 300.000 Mitarbeitern Internetzugang bietet? Und wie sieht es bei einem Internetcafé aus?

Die Artikel-29-Datenschutzgruppe verweist auf ihre früheren Stellungnahmen (WP 36³ und WP 126⁴) und spricht sich erneut für die Klärung der Definition der Begriffe „elektronische Kommunikationsdienste“ und „öffentliche Kommunikationsnetze“ aus, da die Entwicklung hybrider öffentlicher/privater Netze berücksichtigt werden muss.

Die Artikel-29-Datenschutzgruppe lädt die Kommission ein, sie zu diesem Thema im Rahmen einer Mitteilung der Kommission oder eines anderen geeigneten Instruments zu konsultieren.

Nationale Regulierungsbehörden

Einige Verweise auf die nationale Regulierungsbehörde (NRB) im Vorschlag scheinen sich auf die nationale Telekom-Regulierungsbehörde zu beziehen, während andere anscheinend auf die Datenschutzbehörde verweisen.

Die Artikel-29-Datenschutzgruppe schlägt eine Formulierung analog zu Artikel 3 Absatz 5 der Rahmenrichtlinie 2002/21/EG vor, damit sichergestellt ist, dass nationale Regulierungsbehörden und nationale Datenschutzbehörden effektiv zusammenarbeiten.

Außerdem sieht der vorgeschlagene Artikel 15 Buchstabe a Ziffer 4 „*Umsetzung und Durchsetzung*“ gegebenenfalls eine Konsultation der Europäischen Behörde für die Märkte der elektronischen Kommunikation vor. Die Artikel-29-Datenschutzgruppe spricht sich energisch dafür aus, ebenfalls konsultiert zu werden. Zu diesem Zweck sollte ein ausdrücklicher Verweis auf einen obligatorischen Konsultationsprozess in den Wortlaut aufgenommen werden.

Schließlich hält es die Artikel-29-Datenschutzgruppe für erforderlich, sicherzustellen, dass der vorgeschlagene Harmonisierungsmechanismus die Mitgliedstaaten nicht davon abhält, zusätzliche Sicherheitsanforderungen zu stellen, um die Ziele der Datenschutzrichtlinie für elektronische Kommunikation zu erreichen.

Artikel 3

Die Artikel-29-Datenschutzgruppe schließt sich der oben erwähnten Stellungnahme des Europäischen Datenschutzbeauftragten an und erachtet diese Bestimmung als positiv, da dadurch klargestellt wird, dass einige RFID-Anwendungen in den Geltungsbereich der Datenschutzrichtlinie für elektronische Kommunikation fallen.

Artikel 13: Unerbetene Werbung

Die Artikel-29-Datenschutzgruppe nimmt in der Kommunikationstechnologie Entwicklungstendenzen wahr, die vom traditionellen Teilnehmer-Modell⁵ abweichen und schlägt daher vor, im gesamten Artikel 13 den Begriff „*Teilnehmer*“ durch den Begriff

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36de.pdf

⁴ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_de.pdf

⁵ Z. B. durch die zunehmende Nutzung von Technologien wie Bluetooth, die eine Form von Werbung ermöglichen, die ebenso aufdringlich geworden ist wie Spam, obwohl die technologische Grundlage unterschiedlich ist.

„Nutzer“ zu ersetzen und den Wortlaut des Dokuments um einen neuen Erwägungsgrund zu ergänzen, in dem die Rollen von Teilnehmern und Nutzern und ihre Beziehungen zueinander erläutert werden.

Die Datenschutzrichtlinie für elektronische Kommunikation in der neuen Fassung sollte Nutzer von kabellosen Medien mit geringer Reichweite gegen unerbetene Werbung im Sinne von Artikel 13 schützen. Eine detailliertere Klärung könnte in Form eines zusätzlichen Erwägungsgrundes erfolgen.

Artikel 13 Absatz 1

Zur Abdeckung der laufenden Entwicklung und Veränderung der Technologien sollte sich Absatz 1 nicht auf „*automatische Anrufsysteme*“ sondern auf „*automatische Anruf- und Kommunikationsysteme*“ beziehen, damit unter Berücksichtigung laufender technischer Fortschritte ein technologieneutraler Ansatz gewahrt bleibt.

Artikel 13 Absatz 6

Im neuen Artikel 13 Absatz 6 schlägt die Kommission vor, die Rechte natürlicher und juristischer Personen zu bekräftigen, damit bei Verstößen gegen nationale Vorschriften, die aufgrund von Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation erlassen wurden, rechtlich vorgegangen werden kann. Die Datenschutzgruppe empfiehlt, dieses Recht auf Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation auszudehnen, sodass auch bei Verstößen gegen nationale Vorschriften zum Verbot von Spähprogrammen rechtliche Schritte unternommen werden können.

3. SONSTIGE ZU BERÜCKSICHTIGENDE ASPEKTE

(a) Standardmäßiger Datenschutz

Die Artikel-29-Datenschutzgruppe spricht sich für eine Anwendung des Prinzips der Datenvermeidung und den Einsatz datenschutzfreundlicher Technologien⁶ durch die für die Datenverarbeitung Verantwortlichen aus.

Die Datenschutzgruppe fordert den europäischen Gesetzgeber auf, dieses Prinzip stärker hervorzuheben, indem die Erwägungsgründe 9 und 30 der Datenschutzrichtlinie für elektronische Kommunikation in einem neuen Absatz in Artikel 1 dieser Richtlinie wiederholt werden.

(b) IP-Adressen

Die Artikel-29-Datenschutzgruppe stellt fest, dass im Zusammenhang mit der Erörterung der Datenschutzrichtlinie für elektronische Kommunikation die Frage aufgeworfen wurde, ob es sich bei IP-Adressen um personenbezogene Daten handelt. Die Datenschutzgruppe erinnert daran, dass in den meisten Fällen – auch bei dynamischer IP-Adressen-Zuweisung – die erforderlichen Daten zur Identifikation des Nutzers/der Nutzer der IP-Adresse vorhanden sind.

⁶ KOM(2007) 228 endg.

In ihrem WP 136⁷ hielt die Datenschutzgruppe fest: „*Wenn der Internet-Diensteanbieter [...] nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmbar Benutzern gehören, muss er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln.*“ Diese Erwägungen sind auch auf die Betreiber von Suchmaschinen anzuwenden (WP 148⁸).

(c) Artikel 5 Absatz 1

Die Artikel-29-Datenschutzgruppe erinnert daran, dass dieser Artikel eine Verpflichtung zur Sicherstellung der Vertraulichkeit der Nachrichten unabhängig von der Art des Netzes und davon, ob eine grenzüberschreitende Kommunikation mit Nicht-EU-Mitgliedstaaten erfolgt, vorsieht.

Betreiber elektronischer Kommunikationsdienste sollten verstärkt Maßnahmen treffen, um einen besseren Schutz aller natürlichen Personen zu erreichen, die auf elektronischem Weg mit Parteien kommunizieren, die sich in Nicht-EU-Staaten befinden. Die Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation ist das geeignete Forum zur Bekräftigung der Bürgerrechte in diesem Zusammenhang und insbesondere zur Gewährleistung von Transparenz hinsichtlich der Mechanismen zur Weiterleitung von Nachrichten.

4. ABSCHLIESSENDE BEMERKUNGEN, SCHLUSSFOLGERUNG

Die Artikel-29-Datenschutzgruppe ersucht den europäischen Gesetzgeber um Berücksichtigung der in der vorliegenden Stellungnahme erläuterten Aspekte.

Geschehen zu Brüssel, am 15. Mai 2008
Für die Datenschutzgruppe
Der Vorsitzende
Alex Türk

⁷ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf

⁸ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_de.pdf