Zweite Stellungnahme des Europäischen Datenschutzbeauftragten 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)

(2009/C 128/04)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

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,

gestützt auf die 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,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

Hintergrund

1. Die Kommission hat am 13. November 2007 einen Vorschlag zur Änderung unter anderem der Richtlinie 2002/58/EG über den Schutz der Privatsphäre und elektronische Kommunikation – üblicherweise als Datenschutzrichtlinie für elektronische Kommunikation ([1]) bezeichnet – (nachstehend „Vorschlag" oder „Kommissionsvorschlag" genannt) unterbreitet. Der Europäische Datenschutzbeauftragte (EDSB) hat am 10. April 2008 eine Stellungnahme zu dem Kommissionsvorschlag („erste Stellungnahme des EDSB") ([2]) angenommen, in der er Empfehlungen für die Verbesserung des Vorschlags gibt, um so dazu beizutragen, dass mit den vorgeschlagenen Änderungen der bestmögliche Schutz der Privatsphäre und der personenbezogenen Daten der Bürger erreicht wird.

2. Der EDSB hat die von der Kommission vorgeschlagene Einrichtung eines obligatorischen Systems zur Benachrichtigung bei Sicherheitsverletzungen begrüßt, in dessen Rahmen die Unternehmen verpflichtet wären, die Bürger im Falle einer Kompromittierung ihrer personenbezogenen Daten zu benachrichtigen. Außerdem würdigte er die neue Bestimmung, die juristischen Personen (z. B. Verbraucherverbänden und Internet-Diensteanbietern) rechtliche Schritte gegen die Versender unerbetener Werbung (Spam) ermöglicht, als weitere Ergänzung der bestehenden Instrumente zur Bekämpfung von Spam.

3. Während der parlamentarischen Aussprachen im Vorfeld der ersten Lesung des Europäischen Parlaments hat der EDSB weitere Beratung in Form von Kommentaren zu ausgewählten Fragen erteilt, die sich aus den Berichten der für die Prüfung der Universaldienstrichtlinie ([3]) und der Datenschutzrichtlinie für elektronische Kommunikation zuständigen Ausschüsse des Europäischen Parlaments ergeben hatten („Kommentare") ([4]). In den Kommentaren wurden in erster Linie Fragen der Verarbeitung von Verkehrsdaten und des Schutzes der Rechte des geistigen Eigentums behandelt.

4. Am 24. September 2008 hat das Europäische Parlament („EP") eine legislative Entschließung zu der Datenschutzrichtlinie für elektronische Kommunikation angenommen („erste Lesung") ([5]). Der EDSB hat mehrere der Abänderungen, die das EP ausgehend von den obengenannten Stellungnahmen und Kommentaren angenommenen hatte, positiv bewertet. Zu den bedeutendsten Änderungen zählt, dass die Meldepflicht bei Sicherheitsverletzungen auf die

([1]) Die Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation ist Teil eines umfassenderen Überprüfungsprozesses, der auf die Errichtung einer EU-Behörde für Telekommunikation und die Überprüfung der Richtlinien 2002/21/EG, 2002/19/EG, 2002/20/EG, 2002/22/EG und 2002/58/EG sowie der Verordnung (EG) Nr. 2006/2004 (insgesamt nachstehend „Überprüfung des Telekommunikationspakets" genannt) abstellt.

([2]) Stellungnahme vom 10. April 2008 zum Vorschlag für eine Richtlinie zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation), ABl. C 181 vom 18.7.2008, S.1.

([3]) Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), ABl. L 108 vom 24.4.2002, S.51.

([4]) Kommentare des EDSB zu ausgewählten Fragen, die sich aus dem Bericht des IMCO (Ausschuss für Binnenmarkt und Verbraucherschutz) zur Prüfung der Richtlinien 2002/22/EG (Universaldienste) und der Richtlinie 2002/58/EG (Datenschutz und elektronische Kommunikation) ergeben, 2. September 2008. Verfügbar auf: www.edps.europa.eu.

([5]) Legislative Entschließung des Europäischen Parlaments vom 24. September 2008 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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 (KOM(2007) 0698 – C6-0420/2007 – 2007/0248 (COD)).

Betreiber von Diensten der Informationsgesellschaft (d.h. Unternehmen, die Internetdienste anbieten) ausgedehnt wurde. Der EDSB hat auch die Abänderung begrüßt, die es juristischen und natürlichen Personen ermöglicht, gegen Verstöße gegen gleich welche Bestimmung der Datenschutzrichtlinie für elektronische Kommunikation gerichtlich vorzugehen (und nicht nur gegen Verstöße gegen die Spam-Bestimmungen, wie es ursprünglich im Kommissionsvorschlag vorgesehen war). Im Anschluss an die erste Lesung im Parlament hat die Kommission einen geänderten Vorschlag zu der Datenschutzrichtlinie für elektronische Kommunikation (nachstehend „geänderter Vorschlag" genannt) ([6]) angenommen.

5. Am 27. November 2008 hat der Rat eine politische Einigung über die Überprüfung der Vorschriften des Telekommunikationspakets einschließlich der Datenschutzrichtlinie für elektronische Kommunikation erzielt, die im Gemeinsamen Standpunkt des Rates („Gemeinsamer Standpunkt") ([7]) Ausdruck findet. Der Gemeinsame Standpunkt wird dem EP nach Artikel 251 Absatz 2 des Vertrags zur Gründung der Europäischen Gemeinschaft übermittelt, woraufhin das EP Abänderungen vorschlagen kann.

Allgemeine Bewertung des Standpunkts des Rates

6. Der Rat hat den Text des Vorschlags in wesentlichen Teilen geändert und viele der vom EP angenommenen Abänderungen nicht akzeptiert. Wenngleich der Gemeinsame Standpunkt sicherlich positive Elemente enthält, ist der EDSB insgesamt besorgt über dessen Inhalt, vor allem weil in dem Gemeinsamen Standpunkt einige der positiven Abänderungen fehlen, die vom EP und in dem geänderten Vorschlag oder in den über die Datenschutzgruppe „Artikel 29" veröffentlichten Stellungnahmen des EDSB und der Europäischen Datenschutzbehörden ([8]) vorgeschlagen worden waren.

7. Im Gegenteil wurden in nicht wenigen Fällen die in dem geänderten Vorschlag oder in den Abänderungen des EP enthaltenen Bestimmungen, die den Bürgern Garantien boten, gestrichen oder deutlich abgeschwächt. Im Ergebnis bietet der Gemeinsame Standpunkt ein deutlich geringeres Schutzniveau für die Bürger. Daher gibt der EDSB nunmehr eine zweite Stellungnahme ab in der Hoffnung, dass im weiteren Verlauf des Gesetzgebungsverfahrens für die Datenschutzrichtlinie für elektronische Kommunikation neue Änderungen angenommen werden, durch die die Datenschutzgarantien wiederhergestellt werden.

8. Der EDSB konzentriert sich in dieser zweiten Stellungnahme auf einige wesentliche Bedenken und greift nicht alle Punkte erneut auf, die in seiner ersten Stellungnahme oder in den Kommentaren behandelt wurden; diese behalten alle ihre Gültigkeit. In der vorliegenden Stellungnahme werden insbesondere die folgenden Punkte behandelt:

— die Bestimmungen zur Meldepflicht für Sicherheitsverletzungen;

— der Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation in Bezug auf private und öffentlich zugängliche private Netze;

— die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken;

— das Recht juristischer Personen, gegen Verstöße gegen die Datenschutzrichtlinie für elektronische Kommunikation gerichtlich vorzugehen.

9. Zur Klärung der obengenannten Punkte wird in dieser Stellungnahme der Gemeinsame Standpunkt des Rates analysiert und mit den Ergebnissen der ersten Lesung des EP sowie mit dem geänderten Kommissionsvorschlag verglichen. Die Stellungnahme enthält Empfehlungen, um die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation zu straffen und dafür zu sorgen, dass die Richtlinie weiterhin einen angemessenen Schutz der Privatsphäre und der personenbezogenen Daten natürlicher Personen gewährleistet.

II. BESTIMMUNGEN ÜBER DIE MELDEPFLICHT BEI SICHERHEITSVERLETZUNGEN

10. Der EDSB unterstützt die Annahme einer Regelung zur Benachrichtigung bei Sicherheitsverletzungen, in deren Rahmen die Behörden und die betreffenden Personen benachrichtigt werden, wenn personenbezogene Daten kompromittiert ([9]) wurden. Die Benachrichtigung über Sicherheitsverletzungen kann den Bürgern helfen, die notwendigen Schritte zu unternehmen, um etwaigen Schaden infolge dieser Kompromittierung zu mindern. Außerdem wird die Verpflichtung zur Benachrichtigung bei Sicherheitsverletzungen die Unternehmen veranlassen, die Datensicherheit zu verbessern, und ihre Verantwortlichkeit für die ihnen anvertrauten personenbezogenen Daten verstärken.

11. Der geänderte Kommissionsvorschlag, die erste Lesung des Parlaments und der Gemeinsame Standpunkt des Rates verkörpern drei unterschiedliche Konzepte für die Benachrichtigung bei Sicherheitsverletzungen, die derzeit geprüft werden. Jedes der drei Konzepte weist positive Aspekte auf. Nach Auffassung des EDSB bieten aber alle Konzepte Raum für Verbesserungen; er rät daher, bei der Prüfung der abschließenden Schritte vor der Annahme einer Regelung für die Benachrichtigung bei Sicherheitsverletzungen die nachstehenden Empfehlungen zu berücksichtigen.

([6]) Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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, Brüssel, 6.11.2008, KOM(2008) 723 endg.

([7]) Verfügbar auf der öffentlichen Website des Rates.

([8]) 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), verfügbar auf der Website der Datenschutzgruppe „Artikel 29".

([9]) In dieser Stellungnahme wird das Wort „kompromittiert" verwendet für jegliche Verletzung personenbezogener Daten als Folge der zufälligen oder unrechtmäßigen Zerstörung sowie des Verlusts, der Änderung, der unberechtigten Weitergabe dieser Daten oder des unberechtigten Zugangs zu ihnen im Zusammenhang mit ihrer Übermittlung, Speicherung oder sonstigen Verarbeitung.

12. Bei der Analyse der drei Regelungen für die Benachrichtigung bei Sicherheitsverletzungen sind fünf wesentliche Punkte zu berücksichtigen; (i) die Definition von Sicherheitsverletzungen; (*ii*) die Einrichtungen, die der Meldepflicht unterliegen („betroffene Einrichtungen"); (*iii*) der Standard, der die Meldepflicht auslöst; (*iv*) die Bestimmung der Stelle, die zu entscheiden hat, ob eine Sicherheitsverletzung dem Standard entspricht oder nicht; (v) die Empfänger der Benachrichtigung.

Überblick über die Konzepte von Kommission, Rat und EP

13. Das Europäische Parlament, die Kommission und der Rat haben jeweils unterschiedliche Konzepte für die Benachrichtigung bei Sicherheitsverletzungen angenommen. Das EP hat in erster Lesung die im Kommissionsvorschlag enthaltene ursprüngliche Regelung für die Benachrichtigung bei Sicherheitsverletzungen geändert ([10]). Nach dem Konzept des EP gilt die Meldepflicht nicht nur für die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, sondern auch für die Betreiber von Diensten der Informationsgesellschaft. Außerdem wären nach diesem Konzept alle Verletzungen personenbezogener Daten an die nationale Regulierungsbehörde oder die zuständigen Behörden (insgesamt nachstehend „Behörden" genannt) zu melden. Sollten die Behörden entscheiden, dass es sich um eine *schwerwiegende* Sicherheitsverletzung handelt, so würden sie von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern von Diensten der Informationsgesellschaft verlangen, unverzüglich die betroffene Person zu benachrichtigen. Falls die Verletzungen eine unmittelbare Gefahr darstellen, müssten die Anbieter und Betreiber die betroffenen Personen benachrichtigen, bevor sie die Behörden unterrichten, ohne eine regulatorische Entscheidung abzuwarten. Eine Ausnahme von der Pflicht, die Verbraucher zu benachrichtigen, gilt für Einrichtungen, die den Behörden glaubhaft machen können, dass „*geeignete technische Schutzmaßnahmen ergriffen wurden*", um die Daten für alle unbefugten Personen zu verschlüsseln.

14. Nach dem Konzept des Rates sind ebenfalls die Teilnehmer und die Behörden zu benachrichtigen, jedoch nur in Fällen, in denen die *betroffene Einrichtung* die Verletzung als eine *ernsthafte Bedrohung* der Privatsphäre des Teilnehmers (d.h. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschädigung) betrachtet.

15. In dem geänderten Kommissionsvorschlag wird die vom EP eingebrachte Verpflichtung, den Behörden alle Sicherheitsverletzungen zu melden, beibehalten. Im Gegensatz zum Konzept des EP sieht der geänderte Vorschlag jedoch eine Ausnahme von der Pflicht zur Benachrichtigung der Bürger vor, wenn der Anbieter öffentlicher elektronischer Kommunikationsdienste den zuständigen Behörden glaubhaft macht, dass infolge der Verletzung (i) mit *großer Wahrscheinlichkeit* nicht mit einem Schaden (z. B. wirtschaftlichen Einbußen, sozialen Nachteilen oder Identitätsdiebstahl) zu rechnen ist oder (*ii*) „*geeignete technische Schutzmaßnahmen*" für die von der Sicherheitsverletzung betroffenen Daten ergriffen wurden. Das Konzept der Kommission umfasst also eine Schadensanalyse in Verbindung mit individuellen Benachrichtigungen.

16. Es sei darauf hingewiesen, dass nach dem Konzept des EP ([11]) und dem der Kommission letztlich *die Behörden* zu entscheiden haben, ob die Sicherheitsverletzung schwerwiegend ist oder mit großer Wahrscheinlichkeit Schaden verursachen wird. Im Gegensatz dazu wird nach dem Konzept des Rates diese Entscheidung den *betroffenen Einrichtungen* überlassen.

17. Die Konzepte sowohl des Rates als auch der Kommission gelten nur für die Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten und nicht – wie beim Konzept des EP – für die Betreiber von Diensten der Informationsgesellschaft.

Definition der Sicherheitsverletzung

18. Der EDSB begrüßt, dass die drei Gesetzgebungsvorschläge die gleiche Definition für die Meldepflicht für Sicherheitsverletzungen enthalten, die beschrieben werden als „*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 [...] verarbeitet werden*" ([12]).

19. Wie nachstehend weiter ausgeführt wird, ist diese Definition insofern begrüßenswert, als sie genügend weit gefasst ist, um die meisten einschlägigen Situationen abzudecken, in denen eine Benachrichtigung über Sicherheitsverletzungen gerechtfertigt sein könnte.

20. Erstens enthält die Definition Beispiele für den *unberechtigten Zugang* von Dritten zu personenbezogenen Daten, wie z. B. das Hacken eines Servers, auf dem personenbezogene Daten gespeichert sind, und die Abfrage solcher Daten.

21. Zweitens würde diese Definition auch Situationen einschließen, in denen es zum Verlust oder zur Offenlegung personenbezogener Daten gekommen ist, ein unberechtigter Zugang aber noch nachgewiesen werden muss. Hierzu würden Situationen zählen, in denen personenbezogene Daten verloren gegangen sind (z. B. CD-ROM, USB-Speicherstifte oder andere portable Datenträger) oder sie durch reguläre Nutzer öffentlich zugänglich gemacht wurden (Mitarbeiterdatei, die versehentlich und vorübergehend in einen öffentlich zugänglichen Teil des Internets eingestellt wurde). Da häufig nicht nachzuweisen ist, ob zu einem bestimmten Zeitpunkt ein Zugriff oder eine Nutzung durch unbefugte Dritte erfolgt ist oder nicht, erscheint es sinnvoll, diese Beispiele in den Geltungsbereich der Definition aufzunehmen. Der EDSB empfiehlt daher, diese Definition beizubehalten. Er empfiehlt ferner, die Definition der Sicherheitsverletzung in Artikel 2 der Datenschutzrichtlinie für elektronische Kommunikation aufzunehmen, da dies besser der Gesamtstruktur der Richtlinie entspräche und für mehr Klarheit sorgen würde.

([10]) Diese Problematik wird insbesondere in den EP-Abänderungen 187, 124 bis 127 sowie 27, 21, und 32 behandelt.

([11]) Ausgenommen in Fällen unmittelbarer Gefahr, in denen die betroffenen Einrichtungen zuerst die Verbraucher zu benachrichtigen haben.

([12]) Artikel 2 Buchstabe h der Richtlinie (Gemeinsamer Standpunkt) bzw. Artikel 2 Buchstabe i (geänderter Vorschlag) und Artikel 4 Absatz 3 (erste Lesung des EP).

Einrichtungen, die der Meldepflicht unterliegen sollten

22. Die Meldepflicht gilt nach dem Konzept des EP sowohl für Anbieter elektronischer Kommunikationsdienste als auch für Betreiber von Diensten der Informationsgesellschaft. Nach den Plänen des Rates und der Kommission sollen jedoch nur Anbieter elektronischer Kommunikationsdienste wie beispielsweise Telekommunikationsunternehmen und Internet-Diensteanbieter verpflichtet werden, die Bürger über Sicherheitsverletzungen, durch die ihre personenbezogenen Daten kompromittiert wurden, zu benachrichtigen. Für andere Tätigkeitsbereiche, wie z. B. Online-Banken, Online-Händler, Anbieter von Online-Gesundheitsdiensten, besteht diese Verpflichtung nicht. Aus den im Folgenden dargelegten Gründen ist der EDSB der Ansicht, dass unter dem Blickwinkel der öffentlichen Ordnung unbedingt gewährleistet sein muss, dass Dienste der Informationsgesellschaft, die Online-Unternehmen, Online-Banken, Online-Anbieter von Gesundheitsdiensten usw. umfassen, ebenso der Meldepflicht unterliegen.

23. Der ESDB stellt erstens fest, dass Telekommunikationsunternehmen zwar sicherlich Ziel von Sicherheitsverletzungen sind, die eine Meldepflicht rechtfertigen, dass dies aber auch für andere Arten von Unternehmen/Anbietern gilt. Online-Händler, Online-Banken und Online-Apotheken haben wahrscheinlich in gleichem, wenn nicht in höherem Maße als Telekommunikationsunternehmen unter Sicherheitsverletzungen zu leiden. Daher sprechen Risikoerwägungen nicht für eine Beschränkung der Meldepflicht bei Sicherheitsverletzungen auf Anbieter öffentlicher elektronischer Kommunikationsdienste. Die Notwendigkeit eines weiter gefassten Ansatzes wird durch die Erfahrungen anderer Länder veranschaulicht. So haben in den Vereinigten Staaten fast alle Bundesstaaten (derzeit mehr als 40) Gesetze zur Meldepflicht bei Sicherheitsverletzungen mit einem breiter angelegten Anwendungsbereich erlassen, der nämlich nicht nur Anbieter öffentlicher elektronischer Kommunikationsdienste erfasst, sondern alle Einrichtungen, die die erforderlichen personenbezogenen Daten aufbewahren.

24. Zweitens, wenn eine Verletzung der Arten personenbezogener Daten, die von Anbietern öffentlicher elektronischer Kommunikationsdienste regelmäßig verarbeitet werden, eindeutig Auswirkungen auf die Privatsphäre der Bürger haben kann, so gilt dies mindestens in gleichem Maße für die Arten personenbezogener Daten, die von Betreibern von Diensten der Informationsgesellschaft verarbeitet werden. Mit Sicherheit können sich Banken und andere Finanzinstitute hochvertrauliche Informationen (z. B. Kontendaten) besitzen, deren Offenlegung Identitätsdiebstahl begünstigen kann. Ebenso kann die Offenlegung hochsensibler Gesundheitsdaten durch Online-Anbieter von Gesundheitsdiensten besonders schädlich für die Bürger sein. Daher erfordern die Arten personenbezogener Daten, die kompromittiert werden könnten, ebenfalls eine breiter angelegte Anwendung der Meldepflicht bei Sicherheitsverletzungen, die sich zumindest auf die Betreiber von Diensten der Informationsgesellschaft erstrecken müsste.

25. Es wurden einige rechtliche Argumente gegen eine Erweiterung des Anwendungsbereichs dieses Artikels, d.h. bezüglich der von dieser Anforderung betroffenen Einrichtungen, vorgebracht. Insbesondere wurde die Tatsache, dass der allgemeine Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation nur Anbieter öffentlicher elektronischer Kommunikationsdienste betrifft, als Hindernis für die Anwendung der Meldepflicht auch auf Betreiber von Diensten der Informationsgesellschaft angeführt.

26. In diesem Zusammenhang möchte der EDSB auf Folgendes hinweisen: *(i)* Es gibt keinerlei rechtliche Hindernisse, andere Akteure als Anbieter öffentlicher elektronischer Kommunikationsdienste in den Geltungsbereich einiger Bestimmungen der Richtlinie aufzunehmen. Der Gemeinschaftsgesetzgeber hat in dieser Hinsicht völlige Ermessensfreiheit. *(ii)* In der bestehenden Datenschutzrichtlinie für elektronische Kommunikation sind weitere Beispiele für die Anwendung auf andere Einrichtungen als Anbieter öffentlicher elektronischer Kommunikationsdienste zu finden.

27. So gilt beispielsweise Artikel 13 nicht nur für Anbieter öffentlicher elektronischer Kommunikationsdienste, sondern für jedes Unternehmen, das unerbetene Nachrichten versendet, indem eine ausdrückliche vorherige Einwilligung hierfür gefordert wird. Darüber hinaus ist Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, der unter anderem die Speicherung von Informationen wie Cookies in den Endgeräten der Nutzer untersagt, nicht nur für Anbieter öffentlicher elektronischer Kommunikationsdienste bindend, sondern für jeden, der versucht, Informationen in den Endgeräten der Bürger zu speichern oder auf dort gespeicherte Informationen zuzugreifen. Zudem hat die Kommission in dem laufenden Gesetzgebungsverfahren sogar vorgeschlagen, den Anwendungsbereich von Artikel 5 Absatz 3 zu erweitern, sobald derartige Technologien (Cookies/Spähsoftware) nicht nur über elektronische Kommunikationssysteme, sondern durch jedes mögliche andere Verfahren (Verbreitung durch Herunterladen aus dem Internet oder über externe Datenspeichermedien wie CD-ROM, USB-Speicherstifte, Flash-Laufwerke usw.) übertragen werden. Alle diese Elemente sind begrüßenswert und sollten beibehalten werden, sie sollten aber auch relevante Präzedenzfälle für die gegenwärtige Diskussion über den Anwendungsbereich schaffen.

28. Außerdem haben im laufenden Gesetzgebungsverfahren die Kommission, das EP und wohl auch der Rat einen neuen Artikel 6 Absatz 6a vorgeschlagen, der für andere Einrichtungen als Anbieter öffentlicher elektronischer Kommunikationsdienste gelten soll; dieser wird im Weiteren noch behandelt.

29. Berücksichtigt man die zahlreichen positiven Aspekte der Meldepflicht bei Sicherheitsverletzungen, so werden die Bürger diesen Nutzen sehr wahrscheinlich nicht nur dann erwarten, wenn ihre personenbezogenen Daten durch Anbieter öffentlicher elektronischer Kommunikationsdienste kompromittiert werden, sondern auch dann, wenn dies durch Betreiber von Diensten der Informationsgesellschaft geschieht. Diesen Erwartungen der Bürger wird man nicht gerecht, wenn ein Bürger beispielsweise nicht benachrichtigt wird, wenn eine Online-Bank seine Kontendaten verloren hat.

30. Insgesamt ist der EDSB überzeugt, dass der volle Nutzen der Meldepflicht bei Sicherheitsverletzungen besser erreicht wird, wenn sowohl die Anbieter öffentlicher elektronischer Kommunikationsdienste als auch die Betreiber von Diensten der Informationsgesellschaft in die Kategorie der betroffenen Einrichtungen fallen.

Standard, der die Meldepflicht auslöst

31. Was den Auslöser für die Meldepflicht betrifft, so ist der EDSB – wie im Folgenden erläutert – der Ansicht, dass der Standard in dem geänderten Vorschlag *„reasonably likely to harm"* (verursacht mit großer Wahrscheinlichkeit Schaden) der am besten geeignete der drei vorgeschlagenen Standards ist. Jedoch muss sichergestellt werden, dass „Schaden verursachen" genügend weit gefasst wird, um alle einschlägigen Beispiele für negative Auswirkungen auf die Privatsphäre oder andere legitime Interessen der Bürger abzudecken. Andernfalls wäre es besser, einen neuen Standard einzuführen, wonach die Benachrichtigung obligatorisch wäre, *„wenn die Sicherheitsverletzung mit großer Wahrscheinlichkeit nachteilige Folgen für die betreffenden Personen hat"*.

32. Wie in dem vorherigen Abschnitt bereits ausgeführt wurde, unterscheiden sich die Voraussetzungen, unter denen eine Benachrichtigung der betreffenden Personen zu erfolgen hat (als „Auslöser" oder „Standard" bezeichnet), in den Konzepten des EP, der Kommission und des Rates. Natürlich wird es in großem Maße von dem für die Benachrichtigung festgelegten Auslöser oder Standard abhängen, in welchem Umfang die Bürger benachrichtigt werden.

33. Nach den Plänen des Rates und der Kommission hat eine Benachrichtigung zu erfolgen, wenn die Verletzung *„eine ernsthafte Bedrohung der Privatsphäre des Teilnehmers"* darstellt (Rat) oder wenn *„infolge der Verletzung"* [mit großer Wahrscheinlichkeit] *„mit einer Gefährdung der Interessen der Verbraucher zu rechnen ist"* (Kommission). Nach dem Plan des EP ist der Auslöser für die Benachrichtigung der Bürger die *„Schwere der Verletzung"* (d.h. eine Benachrichtigung der betreffenden Personen ist erforderlich, wenn die Verletzung als *„schwerwiegend"* gilt). Unterhalb dieser Schwelle ist eine Benachrichtigung nicht erforderlich ([13]).

34. Der EDSB versteht, dass im Falle einer Kompromittierung personenbezogener Daten argumentiert werden könnte, dass die betreffenden Personen Anspruch darauf haben, unter allen Umständen Kenntnis von einem solchen Vorfall zu haben. Es ist jedoch nur recht und billig abzuwägen, ob dies angesichts anderer Interessen und Überlegungen eine geeignete Lösung darstellt.

35. Es wurde angedeutet, dass die Verpflichtung, bei einer Kompromittierung personenbezogener Daten in jedem Fall – d. h. ohne Einschränkungen – eine Benachrichtigung zu versenden, zu einer Überbenachrichtigung oder „Benachrichtigungsmüdigkeit" führen könnte, in deren Ergebnis es zu einer Desensibilisierung kommen könnte. Wie nachstehend ausführlicher dargelegt wird, ist der EDSB offen für dieses Argument, er möchte aber gleichzeitig seine Bedenken dagegen zum Ausdruck bringen, dass eine Überbenachrichtigung ein möglicher Indikator für ein weit verbreitetes Scheitern der Verfahren im Bereich der Informationssicherheit sein soll.

36. Wie bereits gesagt, sieht der EDBS die möglichen negativen Folgen einer Überbenachrichtigung und möchte mit dafür sorgen, dass der Rechtsrahmen für die Meldung von Sicherheitsverletzungen nicht zu diesem Ergebnis führt. Wenn die Bürger häufig Benachrichtigungen über Verletzungen erhalten, selbst wenn es keine nachteiligen Folgen, keinen Schaden und keine Notlage gibt, dann wird letztlich eines der zentralen Ziele der Benachrichtigung unterlaufen, denn die Bürger könnten paradoxerweise die Benachrichtigung genau dann ignorieren, wenn sie eigentlich Schritte zu ihrem eigenen Schutz unternehmen müssten. Es ist also wichtig, durch sinnvolle Benachrichtigungen das richtige Gleichgewicht zu erreichen, denn wenn die Bürger nicht auf die empfangenen Benachrichtigungen reagieren, wird die Wirksamkeit der Meldevorschriften erheblich verringert.

37. Damit ein geeigneter Standard angenommen wird, der nicht zu einer Überbenachrichtigung führt, müssen neben dem Auslöser der Meldepflicht auch andere Faktoren, insbesondere die Definition der Sicherheitsverletzung und die der Meldepflicht unterliegenden Daten, berücksichtigt werden. Hierzu stellt der EDSB fest, dass bei allen drei vorgeschlagenen Konzepten die Menge der Benachrichtigungen angesichts der oben erörterten weit gefassten Definition der Sicherheitsverletzung recht hoch sein kann. Die Besorgnis über eine Überbenachrichtigung wird ferner dadurch verstärkt, dass die Definition der Sicherheitsverletzung alle Arten personenbezogener Daten erfasst. Wenngleich der EDSB dies für den richtigen Ansatz hält (nämlich keine Einschränkung der meldepflichtigen personenbezogenen Daten) – im Gegensatz zu anderen Ansätzen wie den US-amerikanischen Gesetzen, in denen die Anforderungen auf die Empfindlichkeit der Daten ausgerichtet sind –, muss dieser Faktor dennoch berücksichtigt werden.

38. Vor dem Hintergrund dieser Ausführungen und unter Berücksichtigung aller verschiedenen Variablen hält es der EDSB für sinnvoll, einen Schwellenwert oder Standard aufzunehmen, unterhalb dessen keine Meldepflicht besteht.

39. Beide vorgeschlagenen Standards – d.h. die Sicherheitsverletzung stellt eine *„ernsthafte Bedrohung der Privatsphäre"* dar oder *„verursacht mit großer Wahrscheinlichkeit Schaden"* – scheinen beispielsweise soziale Nachteile, Rufschädigung und wirtschaftliche Schäden einzuschließen. So würden diese Standards Fälle möglichen Identitätsdiebstahls durch die Freigabe nicht öffentlicher Erkennungszeichen wie Passnummern sowie Fälle möglicher Informationen über das Privatleben der Bürger abdecken. Der EDSB begrüßt diesen Ansatz. Seiner Überzeugung nach kann der Nutzen der Meldepflicht bei Sicherheitsverletzungen nicht in vollem Umfang zum Tragen kommen, wenn das Meldesystem nur Verletzungen erfasst, die zu wirtschaftlichen Schäden führen.

([13]) Hinsichtlich der Ausnahme von dieser Regel siehe Fußnote 11.

40. Von den beiden vorgeschlagenen Standards bevorzugt der EDSB den Standard der Kommission *„verursacht mit großer Wahrscheinlichkeit Schaden“*, da er ein besseres Schutzniveau für die Bürger bieten würde. Sicherheitsverletzungen werden viel eher eine Benachrichtigung erfordern, wenn sie *„mit großer Wahrscheinlichkeit Schaden“* für die Privatsphäre der Bürger *„verursachen“*, als wenn sie eine *„ernsthafte Bedrohung“* hinsichtlich eines solchen Schadens darstellen. Werden nur Sicherheitsverletzungen erfasst, die eine ernsthafte Bedrohung der Privatsphäre der Bürger darstellen, so würde dies die Zahl der meldepflichtigen Verletzungen erheblich einschränken. Nur derartige Sicherheitsverletzungen zu erfassen, würde den Anbietern öffentlicher elektronischer Kommunikationsdienste und den Betreibern von Diensten der Informationsgesellschaft einen übergroßen Ermessensspielraum hinsichtlich der Notwendigkeit einer Benachrichtigung lassen, da es für sie viel einfacher wäre, die Schlussfolgerung, dass keine *ernsthafte Bedrohung* hinsichtlich eines Schadens besteht, als die Schlussfolgerung zu rechtfertigen, dass *mit großer Wahrscheinlichkeit kein Schaden verursacht wird*. Wenngleich eine Überbenachrichtigung sicherlich zu vermeiden ist, muss im Zweifelsfall für die Interessen des Schutzes der Privatsphäre entschieden werden, und die Bürger sollten zumindest dann geschützt sein, wenn eine Sicherheitsverletzung ihnen mit großer Wahrscheinlichkeit Schaden verursacht. Außerdem wird die Formulierung *„mit großer Wahrscheinlichkeit“* in der Praxis sowohl für die betroffenen Anbieter als auch für die zuständigen Behörden wirkungsvoller sein, da sie eine objektive Beurteilung des Falls in seinem jeweiligen Kontext erfordert.

41. Außerdem können Verletzungen der Sicherheit personenbezogener Daten Schäden verursachen, die schwer bezifferbar sind und sich unterscheiden können. Tatsächlich kann die Offenlegung der gleichen Art von Daten – in Abhängigkeit von den individuellen Umständen – einer Person erheblich mehr Schaden zufügen als einer anderen. Ein Standard, wonach der Schaden materiell, erheblich oder schwerwiegend sein müsste, wäre nicht geeignet. So würde das Konzept des Rates, dem zufolge durch die Sicherheitsverletzung die Privatsphäre einer Person *schwerwiegend* beeinträchtigt werden muss, insofern nur einen unzureichenden Schutz für Privatpersonen bieten, als nach einem solchen Standard die Auswirkungen auf die Privatsphäre „schwerwiegend“ sein müssen. Zudem bietet es Raum für eine subjektive Beurteilung.

42. Zwar scheint der obengenannte Standard *„verursacht mit großer Wahrscheinlichkeit Schaden“* für die Meldepflicht bei Sicherheitsverletzungen geeignet zu sein, doch hat der EDSB nach wie vor Bedenken, dass dieser Standard vielleicht nicht alle Situationen erfasst, in denen eine Benachrichtigung der Bürger gerechtfertigt ist, d.h. alle Situationen, in denen mit großer Wahrscheinlichkeit mit negativen Auswirkungen auf die Privatsphäre oder andere legitime Interessen von Personen zu rechnen ist. Aus diesem Grund könnte ein Standard erwogen werden, nach dem eine Benachrichtigung erforderlich wäre, *„wenn die Sicherheitsverletzung mit großer Wahrscheinlichkeit nachteilige Folgen für die Personen hat“*.

43. Dieser alternative Standard hätte außerdem den Vorteil, dass er im Einklang mit den Datenschutzvorschriften der EU stünde. Tatsächlich wird in der Datenschutzrichtlinie mehrfach auf die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen verwiesen. So erlauben beispielsweise Artikel 18 und Erwägungsgrund 49, in denen die Pflicht zur Registrierung von Datenverarbeitungsvorgängen bei den Datenschutzbehörden behandelt wird, eine Ausnahme von dieser Pflicht in Fällen, in denen *„eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist“*. Ein ähnlicher Wortlaut wird in Artikel 13 Absatz 6 des Gemeinsamen Standpunkts verwendet, um juristischen Personen ein gerichtliches Vorgehen gegen Spam-Versender zu ermöglichen.

44. Unter Berücksichtigung des oben Gesagten wäre außerdem zu erwarten, dass die betroffenen Einrichtungen und insbesondere die für die Durchsetzung der Datenschutzvorschriften zuständigen Behörden mit dem obengenannten Standard besser vertraut wären und somit leichter beurteilen könnten, ob eine bestimmte Sicherheitsverletzung dem geforderten Standard entspricht.

Stelle, die zu bestimmen hat, ob eine Sicherheitsverletzung dem Standard entspricht oder nicht

45. Nach dem Konzept des EP (außer in Fällen von unmittelbarer Gefahr) und dem geänderten Vorschlag der Kommission liegt es bei den Behörden der Mitgliedstaaten, zu bestimmen, ob eine Sicherheitsverletzung dem Standard entspricht, der die Pflicht zur Benachrichtigung der betreffenden Personen auslöst.

46. Der EDSB ist der Auffassung, dass die Einbeziehung einer Behörde insofern wichtig für die Entscheidung über die Erfüllung des Standards ist, als sie in gewisser Weise eine Garantie für die ordnungsgemäße Anwendung des Rechtsaktes bietet. Ein solches System kann verhindern, dass Unternehmen die Verletzung fälschlicherweise als nicht schädlich/schwerwiegend einschätzen und somit eine Benachrichtigung umgehen, obwohl diese eigentlich erforderlich wäre.

47. Andererseits befürchtet der EDSB, dass eine Regelung, nach der die Behörden eine Bewertung durchführen müssen, unpraktisch und schwer anwendbar sein könnte oder sich in der Praxis als kontraproduktiv erweisen könnte. Sie könnte sogar die Datenschutzgarantien für die Bürger abschwächen.

48. Tatsächlich würden die Datenschutzbehörden bei einem solchen Ansatz wahrscheinlich mit Meldungen von Sicherheitsverletzungen überhäuft und könnten ernsthafte Schwierigkeiten haben, die erforderlichen Bewertungen vorzunehmen. Es sei darauf hingewiesen, dass die Behörden für die Bewertung, ob eine Sicherheitsverletzung dem Standard entspricht, genügend interne Informationen – oft komplexer technischer Natur – benötigen, die sie sehr schnell verarbeiten müssen. Angesichts der Schwierigkeit der Bewertung und der Tatsache, dass einige Behörden nur über begrenzte Mittel verfügen, befürchtet der EDSB, dass es den Behörden äußerst schwerfallen würde, dieser Verpflichtung nachzukommen, und dass Mittel von anderen wichtigen Prioritäten abgezogen werden könnten. Außerdem könnte durch ein solches System unangemessener Druck auf die Behörden ausgeübt werden; tatsächlich könnten sie unter Umständen haftbar gemacht werden, falls sie entscheiden sollten, dass eine Verletzung nicht schwerwiegend ist, den betreffenden Personen aber dennoch Schaden entsteht.

49. Diese Schwierigkeit wird noch deutlicher, wenn man berücksichtigt, dass Zeit ein entscheidender Faktor für die Begrenzung der Risiken ist, die sich aus Sicherheitsverletzungen ergeben. Sofern die Behörden nicht in der Lage sind, die Bewertung in kürzester Zeit vorzunehmen, kann sich durch die zusätzliche Zeit, die sie für eine solche Bewertung benötigen, der Schaden für die betreffenden Personen noch vergrößern. Daher kann dieser zusätzliche Schritt, der den Bürgern mehr Schutz bieten soll, paradoxerweise dazu führen, dass er weniger Schutz bietet als Systeme, die auf einer direkten Benachrichtigung beruhen.

50. Aus diesen Gründen hält es der EDSB für besser, ein System einzuführen, in dem die betroffenen Einrichtungen bewerten sollten, ob eine Verletzung dem Standard entspricht oder nicht, so wie es im Konzept des Rates vorgesehen ist.

51. Um die Gefahren eines möglichen Missbrauchs zu vermeiden (z. B. durch Einrichtungen, die eine Benachrichtigung in Fällen ablehnen, in denen sie eindeutig erforderlich ist), ist es äußerst wichtig, einige der nachstehenden Datenschutzgarantien aufzunehmen.

52. Erstens muss die für die betroffenen Einrichtungen geltende Pflicht, über die Notwendigkeit einer Benachrichtigung zu entscheiden, natürlich mit der Verpflichtung einhergehen, dass den Behörden zwingend alle Sicherheitsverletzungen zu melden sind, die dem geforderten Standard entsprechen. Von den betroffenen Einrichtungen sollte in diesen Fällen verlangt werden, dass sie die Behörden über die Sicherheitsverletzung, über die Gründe für ihre Entscheidung hinsichtlich einer Benachrichtigung sowie über den Inhalt einer etwaigen Benachrichtigung informieren.

53. Zweitens muss den Behörden eine wirkliche Aufsichtsfunktion übertragen werden. Bei der Ausübung dieser Funktion müssen die Behörden die Möglichkeit haben, ohne dazu verpflichtet zu sein, Untersuchungen zu den Umständen der Sicherheitsverletzung anzustellen und gegebenenfalls geeignete Korrekturmaßnahmen zu fordern ([14]). Hierzu sollte nicht nur die Benachrichtigung der betreffenden Personen (sofern dies nicht bereits erfolgt ist) zählen, sondern auch die Möglichkeit, eine bestimmte Vorgehensweise vorzuschreiben, um künftige Sicherheitsverletzungen zu verhindern. Die Behörden sollten hierfür tatsächliche Befugnisse und Mittel erhalten, und sie müssen über den notwendigen Spielraum verfügen, um zu entscheiden, wann auf die Meldung einer Sicherheitsverletzung zu reagieren ist. Mit anderen Worten, dies würde den Behörden ermöglichen, gezielt vorzugehen und Untersuchungen einzuleiten (z. B. über umfangreiche, wirklich schädliche Sicherheitsverletzungen) und die Einhaltung der rechtlichen Anforderungen zu überprüfen und durchzusetzen.

54. Um das zu erreichen, empfiehlt der EDSB, neben den im Rahmen der Datenschutzrichtlinie für elektronische Kommunikation, insbesondere von Artikel 15a Absatz 3, und der Datenschutzrichtlinie anerkannten Befugnissen folgenden Text aufzunehmen: „*Falls der betreffende Teilnehmer oder die betreffende Person nicht bereits benachrichtigt wurde, kann die zuständige nationale Behörde, nachdem sie die Art der Sicherheitsverletzung geprüft hat, den Anbieter von öffentlichen elektronischen Kommunikationsdiensten oder den Betreiber von Diensten der Informationsgesellschaft auffordern, dies zu tun.*“

55. Außerdem empfiehlt der EDSB dem EP und dem Rat, die vom EP vorgeschlagene Verpflichtung der Einrichtungen, die Risiken ihrer Systeme und der personenbezogenen Daten, die sie verarbeiten wollen, zu bestimmen und zu beurteilen (Abänderung 122, Artikel 4 Absatz 1 Buchstabe a), zu bestätigen. Ausgehend von dieser Verpflichtung erstellen die Einrichtungen eine maßgeschneiderte und genaue Beschreibung der Sicherheitsmaßnahmen, die in ihrem Fall gilt und die den Behörden vorliegen sollte. Kommt es zu einer Sicherheitsverletzung, so wird diese Verpflichtung den betroffenen Einrichtungen – und letztlich auch den Behörden in ihrer Aufsichtsfunktion – bei der Entscheidung helfen, ob die Kompromittierung solcher Daten zu nachteiligen Folgen oder Schäden für die Bürger führen kann.

56. Drittens muss die Verpflichtung der betroffenen Einrichtungen, über die Notwendigkeit einer Benachrichtigung der Bürger zu entscheiden, mit der Verpflichtung einhergehen, ein detailliertes und umfassendes Protokoll der internen Prüfung zu führen, in dem alle aufgetretenen Sicherheitsverletzungen, alle diesbezüglichen Benachrichtigungen sowie alle Maßnahmen zur Verhinderung künftiger Sicherheitsverletzungen beschrieben werden. Dieses Protokoll der internen Prüfung muss den Behörden für ihre Überprüfung und ihre möglichen Untersuchungen zur Verfügung stehen. Auf diese Weise werden die Behörden ihre Aufsichtsfunktion ausüben können. Erreicht werden könnte das durch die Annahme eines Textes mit folgendem Wortlaut: „*Die Anbieter von öffentlichen elektronischen Kommunikationsdiensten und die Betreiber von Diensten der Informationsgesellschaft führen und bewahren umfassende Aufzeichnungen, in denen alle aufgetretenen Sicherheitsverletzungen, die diesbezüglichen relevanten technischen Informationen und die getroffenen Korrekturmaßnahmen ausführlich dargelegt sind. Die Aufzeichnungen müssen ferner einen Verweis auf alle Benachrichtigungen der betreffenden Teilnehmer oder der betreffenden Personen und der zuständigen nationalen Behörden, einschließlich ihres Datums und ihres Inhalts, enthalten. Diese Aufzeichnungen sind der zuständigen nationalen Behörde auf Anfrage vorzulegen.*“

57. Um eine kohärente Umsetzung dieses Standards sowie anderer relevanter Aspekte des Rahmens für die Regelung von Sicherheitsverletzungen (wie z. B. Gestaltung und Verfahren der Benachrichtigung) zu gewährleisten, sollte die Kommission nach Konsultation des EDSB, der Datenschutzgruppe „Artikel 29“ und der einschlägigen Interessenträger technische Durchführungsmaßnahmen erlassen.

([14]) In Artikel 15a Absatz 3 wird diese Aufsichtsbefugnis anerkannt: „*Die Mitgliedstaaten stellen sicher, dass die zuständigen nationalen Regulierungsbehörden und gegebenenfalls andere nationale Behörden über alle erforderlichen Untersuchungsbefugnisse und Mittel verfügen, einschließlich der Möglichkeit, sämtliche zweckdienliche Informationen zu erlangen, die sie benötigen, um die Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften zu überwachen und durchzusetzen.*“

Empfänger der Benachrichtigung

58. Was die Empfänger der Benachrichtigungen anbelangt, so gibt der EDSB der Begriffswahl des EP und der Kommission den Vorzug gegenüber jener des Rates. Tatsächlich hat das EP das Wort „Teilnehmer" durch „Nutzer" ersetzt. Die Kommission benutzt die Begriffe „Teilnehmer" und „betroffene Person". Die Formulierungen des EP wie auch der Kommission würden als Empfänger der Benachrichtigungen nicht nur die aktuellen Teilnehmer einschließen, sondern auch frühere Teilnehmer und Dritte, wie z. B. Nutzer, die mit einigen betroffenen Einrichtungen kommunizieren, ohne sich bei ihnen zu abonnieren. Der EDSB begrüßt diesen Ansatz und ersucht das EP und den Rat, ihn beizubehalten.

59. Der EDSB stellt jedoch eine Reihe von Widersprüchen bei der Begriffswahl der ersten Lesung des EP fest, die beseitigt werden sollten. So wurde beispielsweise das Wort „Teilnehmer" in den meisten Fällen durch „Nutzer" ersetzt, in einigen Fällen aber auch durch „Verbraucher". Dies sollte vereinheitlicht werden.

III. ANWENDUNGSBEREICH DER DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION: ÖFFENTLICHE UND PRIVATE NETZE

60. In Artikel 3 Absatz 1 der geltenden Datenschutzrichtlinie für elektronische Kommunikation sind die in erster Linie von dieser Richtlinie betroffenen Einrichtungen festgelegt, d.h. die Einrichtungen, die Daten *„in Verbindung mit"* der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen Netzen verarbeiten (vorstehend als „Anbieter öffentlicher elektronischer Kommunikationsdienste" bezeichnet) ([15]). Beispiele für Tätigkeiten von Anbietern elektronischer Kommunikationsdienste sind die Bereitstellung eines Internetzugangs, die Übertragung von Informationen über elektronische Netze, Mobiltelefon- und Telefonverbindungen usw.

61. Das EP hat Abänderung 121 zur Änderung von Artikel 3 des ursprünglichen Kommissionsvorschlags angenommen, die besagt, dass der Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation erweitert wurde, um *„die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen und privaten Kommunikationsnetzen und öffentlich zugänglichen privaten Netzen in der Gemeinschaft, […]"* aufzunehmen (Artikel 3 Absatz 1 der Richtlinie 2002/58/EG). Leider hatten der Rat und die Kommission Schwierigkeiten, diese Abänderung zu akzeptieren, weshalb dieses Konzept nicht in den Gemeinsamen Standpunkt und den geänderten Vorschlag übernommen wurde.

Anwendung der Datenschutzrichtlinie für elektronische Kommunikation auf öffentlich zugängliche private Netze

62. Aus den im Folgenden dargelegten Gründen und um einen Konsens zu begünstigen, rät der EDSB, Abänderung 121 im Wesentlichen zu bewahren. Außerdem empfiehlt er, eine Änderung aufzunehmen, die zur weiteren Präzisierung der in den erweiterten Anwendungsbereich fallenden Arten von Diensten beitragen würde.

63. Private Netze dienen oft dazu, elektronische Kommunikationsdienste wie einen Internetzugang für eine unbestimmte — potenziell hohe — Anzahl von Personen bereitzustellen. Das gilt zum Beispiel für den Internetzugang in Internet-Cafés sowie über Hot Spots in Hotels, Restaurants, Zügen, auf Flughäfen und in anderen öffentlich zugänglichen Einrichtungen, in denen derartige Dienste oft ergänzend zu anderen Dienstleistungen (Getränke, Unterbringung usw.) bereitgestellt werden.

64. Bei allen obengenannten Beispielen wird der Öffentlichkeit ein Kommunikationsdienst, d.h. der Internetzugang, nicht über ein öffentliches Netz zur Verfügung gestellt, sondern über eines, das eher als privat anzusehen ist, d.h. über ein privat betriebenes Netz. Wenngleich in den obengenannten Fällen der Kommunikationsdienst für die Öffentlichkeit bereitgestellt wird, ist die Bereitstellung dieser Dienste *wohl* durch die gesamte Datenschutzrichtlinie für elektronische Kommunikation oder zumindest durch einige ihrer Artikel nicht erfasst, da das benutzte Netz eher privater als öffentlicher Natur ist ([16]). Infolgedessen sind die durch die Datenschutzrichtlinie für elektronische Kommunikation garantierten Grundrechte der Bürger in diesen Fällen nicht geschützt und es ergibt sich eine ungleiche Rechtslage für Nutzer der gleichen Dienste des Internetzugangs je nachdem, ob sie über öffentliche Telekommunikationsunternehmen oder über private Anbieter darauf zugreifen. Dies gilt ungeachtet der Tatsache, dass die Gefährdung der Privatsphäre und der personenbezogenen Daten der Bürger in all diesen Fällen ebenso hoch ist wie in Fällen, in denen der Dienst über öffentliche Netze bereitgestellt wird. Kurz gesagt, es gibt keinen Grund dafür, im Rahmen dieser Richtlinie Kommunikationsdienste, die über ein privates Netz bereitgestellt werden, anders zu behandeln als Dienste, die über ein öffentliches Netz bereitgestellt werden.

65. Daher würde der EDSB eine Änderung wie Abänderung 121 des EP unterstützen, wonach die Datenschutzrichtlinie für elektronische Kommunikation auch für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in *privaten* Kommunikationsnetzen gelten würde.

66. Der EDSB räumt aber ein, dass diese Formulierung unvorhersehbare und möglicherweise unbeabsichtigte Folgen haben könnte. Tatsächlich könnte ein bloßer Bezug auf private Netze dahin gehend ausgelegt werden, dass Situationen erfasst werden, die eindeutig nicht unter diese

([15]) „Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen".

([16]) Andersherum könnte argumentiert werden, dass, weil der Kommunikationsdienst für die Öffentlichkeit bereitgestellt wird, die Bereitstellung solcher Dienste in den bestehenden Rechtsrahmen fällt, obwohl es sich um ein privates Netz handelt. Tatsächlich wurden beispielsweise in Frankreich Arbeitgeber, die ihren Arbeitnehmern einen Internetzugang gewährten, mit Internet-Providern, die einen Internetzugang auf kommerzieller Basis anbieten, gleichgesetzt. Diese Auslegung stößt nicht auf breite Zustimmung.

Richtlinie fallen sollen. So könnte beispielsweise behauptet werden, dass eine wörtliche oder strenge Auslegung dieser Formulierung dazu führen würde, dass die Eigentümer von Häusern mit WiFi-Ausstattung ([17]), über die jeder innerhalb ihrer Reichweite (in der Regel innerhalb des Hauses) eine Verbindung herstellen könnte, in den Anwendungsbereich der Richtlinie fallen, auch wenn dies mit Abänderung 121 nicht beabsichtigt wird. Um das zu vermeiden, empfiehlt der EDSB, Abänderung 121 umzuformulieren, indem in den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation *„die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen oder öffentlich zugänglichen privaten Kommunikationsnetzen in der Gemeinschaft, …“* aufgenommen wird.

67. Dadurch würde klargestellt, dass nur öffentlich zugängliche private Netze unter die Datenschutzrichtlinie für elektronische Kommunikation fallen würden. Indem die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation *lediglich* auf *öffentlich zugängliche private Netze* (und nicht auf alle privaten Netze) angewandt werden, wird eine Grenze gesetzt, so dass die Richtlinie nur die Kommunikationsdienste erfasst, die über absichtlich der Öffentlichkeit *zugänglich* gemachte private Netze bereitgestellt werden. Mit dieser Formulierung würde deutlicher herausgestellt, dass die *Verfügbarkeit* privater Netze *für Angehörige der breiten Öffentlichkeit* der Schlüsselfaktor für die Entscheidung ist, ob die Richtlinie greift (zusätzlich zu der Bereitstellung eines öffentlich zugänglichen Kommunikationsdienstes). Mit anderen Worten würde ein Netz/Dienst unter die Datenschutzrichtlinie für elektronische Kommunikation fallen, unabhängig davon, ob es sich um ein öffentliches oder privates Netz handelt, wenn das Netz absichtlich der Öffentlichkeit zugänglich gemacht wird, um einen öffentlichen Kommunikationsdienst, wie z. B. einen Internetzugang, bereitzustellen, selbst wenn dieser Dienst eine andere Dienstleistung (z. B. Hotelunterbringung) ergänzt.

68. Der EDSB stellt fest, dass der vorstehend befürwortete Ansatz, nach dem die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation für *öffentlich zugängliche private Netze* gelten sollen, im Einklang mit den Ansätzen mehrerer Mitgliedstaaten steht, wo die Behörden bereits erklärt haben, dass derartige Dienste ebenso wie Dienste in rein privaten Netzen in den Anwendungsbereich der nationalen Bestimmungen zur Durchführung der Datenschutzrichtlinie für elektronische Kommunikation fallen. ([18])

69. Um die Rechtssicherheit für die durch den neuen Anwendungsbereich erfassten Einrichtungen zu fördern, könnte es sinnvoll sein, in die Datenschutzrichtlinie für elektronische Kommunikation eine Änderung aufzunehmen, in der „öffentlich zugängliche private Netze“ definiert werden; diese Definition könnte wie folgt lauten: *„‚Öffentlich zugängliches privates Netz‘ bezeichnet ein privat betriebenes Netz, zu dem Angehörige der breiten Öffentlichkeit normalerweise unbeschränkten Zugang haben, ganz gleich ob entgeltlich oder unentgeltlich oder in Verbindung mit anderen Dienstleistungen oder Angeboten, sofern sie die geltenden Bedingungen akzeptieren.“*

70. In der Praxis würde dieser Ansatz bedeuten, dass private Netze in Hotels und anderen Einrichtungen, die der breiten Öffentlichkeit einen Internetzugang über ein privates Netz bieten, erfasst würden. Andersherum wäre die Bereitstellung von Kommunikationsdiensten in rein privaten Netzen, in denen die Dienstleistung auf eine begrenzte Gruppe identifizierbarer Personen beschränkt ist, nicht erfasst. Daher würden beispielsweise virtuelle private Netze und Privatwohnungen mit WiFi-Ausstattung nicht unter die Richtlinie fallen. Auch Dienstleistungen, die über rein unternehmensinterne Netze bereitgestellt werden, wären nicht erfasst.

Private Netzwerke im Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation

71. Die oben empfohlene Ausnahme privater Netze *per se* sollte als eine vorläufige Maßnahme betrachtet werden, die weiter erörtert werden sollte. In Anbetracht der Auswirkungen, die ein einfacher Ausschluss rein privater Netze auf die Privatsphäre haben könnte, und angesichts der Tatsache, dass dieser Beschluss eine Vielzahl von Personen betrifft, die normalerweise über Firmennetze auf das Internet zugreifen, müsste diese Frage in Zukunft eventuell überdacht werden. Aus diesem Grund und um die Diskussion über dieses Thema anzuregen, empfiehlt der EDSB die Aufnahme eines Erwägungsgrunds in die Datenschutzrichtlinie für elektronische Kommunikation, nach dem die Kommission eine öffentliche Konsultation zur Anwendung dieser Richtlinie auf alle privaten Netze mit Beiträgen des EDSB, der Datenschutzbehörden und anderer einschlägiger Interessenträger durchführen wird. Außerdem könnte in dem Erwägungsgrund präzisiert werden, dass die Kommission im Ergebnis der öffentlichen Konsultation geeignete Vorschläge unterbreiten sollte, um die Arten von Einrichtungen, die unter diese Richtlinie fallen, zu erweitern oder zu begrenzen.

72. Darüber hinaus sollten die verschiedenen Artikel der Datenschutzrichtlinie für elektronische Kommunikation entsprechend geändert werden, so dass sich alle Durchführungsbestimmungen ausdrücklich neben öffentlichen Netzen auf öffentlich zugängliche private Netze beziehen.

IV. **VERARBEITUNG VON VERKEHRSDATEN ZU SICHERHEITSZWECKEN**

73. Während des Gesetzgebungsverfahrens zur Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation haben Unternehmen, die Sicherheitsdienste bereitstellen, geltend gemacht, dass in die Richtlinie eine Bestimmung aufgenommen werden müsse, um die Sammlung von Verkehrsdaten zu legitimieren, damit eine wirksame Online-Sicherheit garantiert werden könne.

([17]) Normalerweise Funknetzwerke (Wireless Local Area Networks — WLANs).

([18]) Siehe Fußnote 16.

74. Daraufhin hat das EP Abänderung 181 aufgenommen, mit der ein neuer Artikel 6 Absatz 6a eingeführt wurde, der die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken ausdrücklich gestatten würde: „*Unbeschadet der Einhaltung der Vorschriften außer denjenigen des Artikels 7 der Richtlinie 95/46/EG und des Artikels 5 dieser Richtlinie können Verkehrsdaten im berechtigten Interesse des für die Verarbeitung Verantwortlichen verarbeitet werden, um technische Maßnahmen für die Netz- und Informationssicherheit gemäß der Definition in Artikel 4 Buchstabe c der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit durchzuführen in Bezug auf einen öffentlichen Dienst für elektronische Kommunikationsdienste und -netze, ein öffentliches oder privates Netz für elektronische Kommunikation, einen Dienst der Informationsgesellschaft oder damit zusammenhängende Endgeräte und Geräte für elektronische Kommunikation, sofern nicht das Interesse oder die geschützten Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Eine solche Verarbeitung muss auf das für derartige Sicherheitsvorkehrungen unbedingt erforderliche Maß beschränkt bleiben.*“

75. Im geänderten Vorschlag der Kommission wurde diese Abänderung im Grundsatz gebilligt, aber es wurde eine wichtige Klausel entfernt, die sicherstellen sollte, dass die übrigen Bestimmungen der Richtlinie eingehalten werden; in der entfernten Klausel heißt es: „*Unbeschadet […] dieser Richtlinie*“. Der Rat hat eine überarbeitete Version angenommen, die bei der Abschwächung der in Abänderung 181 vorgesehenen bedeutenden Schutzmaßnahmen und des Interessenausgleichs noch einen Schritt weiter geht; sie hat folgenden Wortlaut: „*Verkehrsdaten können im strikt notwendigen Ausmaß verarbeitet werden, um die Netz- und Informationssicherheit gemäß der Definition in Artikel 4 Buchstabe c der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit zu gewährleisten.*“

76. Wie nachstehend näher erläutert wird, ist Artikel 6 Absatz 6a unnötig und birgt ein Missbrauchsrisiko, insbesondere wenn er in einer Form angenommen wird, die nicht die wichtigen Garantien, die Klauseln zur Einhaltung anderer Bestimmungen der Richtlinie und den Interessenausgleich enthält. Daher empfiehlt der EDSB, diesen Artikel zu streichen oder aber zumindest sicherzustellen, dass ein etwaiger Artikel zu diesem Thema die Arten von Garantien enthält, die in der vom EP angenommenen Abänderung 181 enthalten sind.

Rechtsgründe für die Verarbeitung von Verkehrsdaten, die für elektronische Kommunikationsdienste und andere für die Datenverarbeitung Verantwortliche im Rahmen der geltenden Datenschutzvorschriften zutreffen

77. Der Umfang, in dem die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste Verkehrsdaten rechtmäßig verarbeiten dürfen, ist in Artikel 6 der Datenschutzrichtlinie für elektronische Kommunikation geregelt, in dem die Verarbeitung von Verkehrsdaten auf eine begrenzte Anzahl von Zwecken wie Gebührenabrechnung, Bezahlung von Zusammenschaltungen und Vermarktung beschränkt wird. Diese Verarbeitung kann nur unter bestimmten Bedingungen erfolgen; so ist beispielsweise für eine Vermarktung die Einwilligung der betreffenden Personen erforderlich. Zudem dürfen andere für die Datenverarbeitung Verantwortliche wie die Betreiber von Diensten der Informationsgesellschaft nach Artikel 7 der Datenschutzrichtlinie Verkehrsdaten verarbeiten; in diesem Artikel ist festgelegt, dass die für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeiten dürfen, wenn sie mindestens eine der aufgelisteten Rechtsgrundlagen, auch Rechtsgründe genannt, erfüllen.

78. Ein Beispiel für eine solche Rechtsgrundlage ist Artikel 7 Buchstabe a der Datenschutzrichtlinie, in dem die Einwilligung der betroffenen Person gefordert wird. Wenn beispielsweise ein Online-Einzelhändler Verkehrsdaten im Hinblick auf die Versendung von Werbe- oder Marketingmaterial verarbeiten will, so muss er die Einwilligung der betroffenen Person einholen. Eine weitere Rechtsgrundlage in Artikel 7 kann in bestimmten Fällen die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken erlauben, z.B. durch Sicherheitsfirmen, die Sicherheitsdienste anbieten. Basis hierfür ist Artikel 7 Buchstabe f, in dem festgelegt ist, dass die für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeiten können, wenn „*die Verarbeitung erforderlich [ist] zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen ...*“. Die Datenschutzrichtlinie enthält keine konkreten Beispiele, in denen die Verarbeitung personenbezogener Daten dieser Anforderung entsprechen würde. Stattdessen wird die Entscheidung von den für die Verarbeitung Verantwortlichen fallweise — oft mit der Zustimmung der nationalen Datenschutzbehörden oder anderer Behörden — getroffen.

79. Es sollte das Zusammenspiel zwischen Artikel 7 der Datenschutzrichtlinie und dem vorgeschlagenen Artikel 6 Absatz 6a der Datenschutzrichtlinie für elektronische Kommunikation geprüft werden. In dem vorgeschlagenen Artikel 6 Absatz 6a ist festgelegt, unter welchen Umständen die Anforderungen des Artikels 7 Buchstabe f erfüllt wären. Dadurch nämlich, dass Artikel 6 Absatz 6a die Verarbeitung von Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit erlaubt, ermöglicht er eine solche Verarbeitung im berechtigten Interesse des für die Verarbeitung Verantwortlichen.

80. Wie nachstehend erläutert wird, hält der EDSB den vorgeschlagenen Artikel 6 Absatz 6a weder für notwendig noch für sinnvoll. Tatsächlich muss aus rechtlicher Sicht im Grunde nicht festgelegt werden, ob eine bestimmte Art der Datenverarbeitungstätigkeit — in diesem Fall die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken — den Anforderungen von Artikel 7 Buchstabe f der Datenschutzrichtlinie entspricht oder nicht, was nach Artikel 7 Buchstabe a die Einwilligung der betroffenen Person erforderlich machen kann. Wie zuvor bereits festgestellt, erfolgt die Bewertung normalerweise durch die für die Verarbeitung Verantwortlichen, d.h. auf der Umsetzungsebene durch die Unternehmen in Konsultation mit den Datenschutzbehörden und bei Bedarf durch die Gerichte. Generell ist der EDSB der Auffassung, dass in bestimmten Fällen die rechtmäßige Verarbeitung von Verkehrsdaten zu Sicherheitszwecken, sofern sie die Grundrechte und Grundfreiheiten der betroffenen Personen nicht gefährdet, wahrscheinlich den Anforderungen von Artikel 7 Buchstabe f der Datenschutzrichtlinie entspricht und daher

durchgeführt werden kann. Außerdem gibt es in der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation kein weiteres Beispiel dafür, dass bestimmte Arten der Datenverarbeitungstätigkeit, die den Anforderungen von Artikel 7 Buchstabe f entsprechen würden, herausgegriffen oder besonders behandelt werden, und es hat keinen nachgewiesenen Bedarf für eine solche Ausnahmeregelung gegeben. Wie oben dargelegt, zeigt sich im Gegenteil, dass sich diese Art der Tätigkeit unter vielen Umständen bequem in den vorhandenen Text einpassen würde. Daher ist eine Rechtsvorschrift zur Bestätigung dieser Bewertung im Grunde unnötig.

Die Versionen des EP, des Rates und der Kommission für Artikel 6 Absatz 6a

81. Wenngleich sie — wie oben erklärt — unnötig ist, so ist doch hervorzuheben, dass die vom EP angenommene Abänderung 181 in gewissem Maße unter Berücksichtigung der in den Datenschutzvorschriften verankerten Grundsätze des Schutzes der Privatsphäre und des Datenschutzes verfasst wurde. In der Abänderung 181 des EP könnten die Interessen des Datenschutzes und des Schutzes der Privatsphäre noch weiter behandelt werden, z. B. indem der Passus „in bestimmten Fällen" aufgenommen wird, um eine selektive Anwendung dieses Artikels zu gewährleisten, oder indem ein spezieller Aufbewahrungszeitraum eingeführt wird.

82. Abänderung 181 enthält einige positive Elemente. In ihr wird bestätigt, dass die Verarbeitung im Einklang mit allen anderen für die Verarbeitung von personenbezogenen Daten geltenden Grundsätzen des Datenschutzes stehen sollte („*Unbeschadet der Einhaltung der Vorschriften […] der Richtlinie 95/46/EG und […] dieser Richtlinie*"). Außerdem erlaubt Abänderung 181 zwar die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken, doch findet sie einen Mittelweg zwischen den Interessen der Einrichtung, die Verkehrsdaten verarbeitet, und den Interessen der Personen, deren Daten verarbeitet werden, so dass eine solche Datenverarbeitung nur erfolgen kann, wenn die Interessen der Einrichtung, die die Daten verarbeitet, nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen („*sofern nicht das Interesse oder die geschützten Grundrechte und Grundfreiheiten der betroffenen Person überwiegen*"). Diese Anforderung ist insofern wesentlich, als sie die Verarbeitung von Verkehrsdaten in bestimmten Fällen zulassen kann; sie würde einer Einrichtung aber nicht die Verarbeitung von Verkehrsdaten *en bloc* ermöglichen.

83. Die vom Rat überarbeitete Fassung dieser Abänderung enthält lobenswerte Elemente wie die Beibehaltung der Formulierung „*strikt notwendig*", die den begrenzten Anwendungsbereich dieses Artikels verdeutlicht. In der Version des Rates sind jedoch die obengenannten Garantien für den Datenschutz und den Schutz der Privatsphäre gestrichen. Wenn auch im Prinzip die allgemeinen Datenschutzvorschriften gelten, ganz gleich, ob in jedem Fall eine spezielle Bezugnahme erfolgt, so kann die Ratsversion von Artikel 6 Absatz 6a doch so ausgelegt werden, dass uneingeschränkter Ermessensspielraum für die Verarbeitung von Verkehrsdaten gewährt wird, ohne dass Garantien für den Datenschutz oder den Schutz der Privatsphäre gegeben werden, wie sie bei der Verarbeitung von Verkehrsdaten stets gelten. Daher könnte argumentiert werden, dass Verkehrsdaten gesammelt, gespeichert und anderweitig genutzt werden könnten, ohne dass sie den Grundsätzen des Datenschutzes und den besonderen Verpflichtungen unterliegen, die ansonsten für die Verantwortlichen gelten, wie z. B. der Qualitätsgrundsatz oder die Verpflichtung zu einer fairen und rechtmäßigen Verarbeitung und zur Wahrung der Vertraulichkeit und Sicherheit der Daten. Da keine Bezugnahme auf geltende Datenschutzgrundsätze, die eine zeitliche Begrenzung der Speicherung von Informationen auferlegen, oder auf spezielle Fristen innerhalb des Artikels erfolgt, kann die Version des Rates zudem dahin gehend ausgelegt werden, dass sie die Sammlung und Verarbeitung von Verkehrsdaten zu Sicherheitszwecken auf unbestimmte Zeit ermöglicht.

84. Darüber hinaus hat der Rat den Schutz der Privatsphäre in einigen Teilen des Textes abgeschwächt, indem er den Wortlaut potenziell weiter gefasst hat. So wurde beispielsweise der Bezug auf die „*im berechtigten Interesse des für die Verarbeitung Verantwortlichen*" gestrichen, was Bedenken darüber aufkommen lässt, welche Arten von Einrichtungen von dieser Ausnahme Gebrauch machen könnten. Es muss unbedingt vermieden werden, dass irgendein Nutzer oder eine juristische Person aus dieser Änderung Nutzen ziehen kann.

85. Die jüngsten Erfahrungen im EP und im Rat zeigen, dass es schwierig ist, gesetzlich festzulegen, in welchem Umfang und unter welchen Bedingungen die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken rechtmäßig erfolgen kann. Wahrscheinlich wird keiner der bestehenden oder künftigen Artikel die offenkundigen Risiken einer allzu breiten Anwendung der Ausnahmeregelung aus anderen als reinen Sicherheitsgründen oder einer Anwendung der Ausnahmeregelung durch Einrichtungen, die nicht in den Genuss dieser Ausnahmeregelung kommen sollten, ausräumen. Das soll nicht heißen, dass eine solche Verarbeitung auf keinen Fall stattfinden darf. Ob und in welchem Umfang sie erfolgen könnte, lässt sich aber vielleicht besser auf der Durchführungsebene beurteilen. Anbieter, die eine solche Verarbeitung planen, sollten den Umfang und die Bedingungen mit den Datenschutzbehörden und eventuell mit der Datenschutzgruppe „Artikel 29" erörtern. Alternativ dazu könnte die Datenschutzrichtlinie für elektronische Kommunikation einen Artikel umfassen, der die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken gestattet, sofern die Datenschutzbehörden dies ausdrücklich genehmigt haben.

86. Unter Berücksichtigung einerseits der Risiken, die Artikel 6 Absatz 6a für die Grundrechte, den Datenschutz und die Privatsphäre der Bürger birgt, und andererseits der Tatsache, dass — wie in dieser Stellungnahme dargelegt — dieser Artikel 6 Absatz 6a aus rechtlicher Sicht unnötig ist, ist der EDSB zu dem Schluss gelangt, dass es am besten wäre, den vorgeschlagenen Artikel 6 Absatz 6a gänzlich zu streichen.

87. Falls gegen die Empfehlung des EDSB ein Text im Sinne einer der derzeitigen Fassungen von Artikel 6 Absatz 6a angenommen wird, sollte er auf jeden Fall die oben erörterten Datenschutzgarantien enthalten. Zudem sollte er in passender Weise in die bestehende Struktur von Artikel 6 integriert werden — am besten als neuer Absatz 2a.

V. **MÖGLICHKEIT FÜR JURISTISCHE PERSONEN, GEGEN VERSTÖSSE GEGEN DIE DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION GERICHTLICH VORZUGEHEN**

88. Das EP hat Abänderung 133 angenommen, die den Anbietern von Internetzugängen und anderen juristischen Personen wie Verbraucherverbänden die Möglichkeit einräumt, gegen Verstöße gegen die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation gerichtlich vorzugehen ([19]). Leider wurde diese Abänderung weder von der Kommission noch vom Rat akzeptiert. Der EDSB betrachtet diese Abänderung als sehr positiv und empfiehlt, sie beizubehalten.

89. Um die Bedeutung dieser Abänderung zu verstehen, muss man sich bewusst machen, dass im Bereich des Schutzes der Privatsphäre und des Datenschutzes der Schaden, der einer einzelnen Person zugefügt wird, für sie allein in der Regel nicht ausreicht, um gerichtliche Schritte einzuleiten. Einzelne Personen klagen normalerweise nicht vor Gericht, weil sie Spams erhalten haben oder weil ihr Name fälschlicherweise in ein Verzeichnis aufgenommen wurde. Die genannte Abänderung würde Verbraucherverbänden und Gewerkschaften, die Verbraucherinteressen vertreten, ermöglichen, im Namen der Verbraucher Sammelklagen bei Gericht einzureichen. Eine größere Vielfalt der Durchsetzungsmechanismen würde wahrscheinlich ebenfalls zu einer stärkeren Einhaltung der Vorschriften führen und wäre daher im Interesse einer wirksamen Anwendung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation.

90. Es gibt Beispiele innerhalb des Rechtsrahmens einiger Mitgliedstaaten, die bereits die Möglichkeit von Sammelklagen vorsehen, damit Verbraucher- oder Interessengruppen Schadenersatzansprüche gegen den Verursacher des Schadens geltend machen können.

91. Außerdem berechtigen die Wettbewerbsgesetze einiger Mitgliedstaaten ([20]) Verbraucher- und Interessengruppen (neben den *Mitbewerbern*) dazu, gegen die zuwiderhandelnde Einrichtung vor Gericht zu klagen. Hinter diesem Ansatz steht der Gedanke, dass Unternehmen, die gegen die Wettbewerbsgesetze verstoßen, wahrscheinlich einen Vorteil daraus ziehen können, da Verbraucher, die nur geringen Schaden erleiden, im Allgemeinen kaum vor Gericht klagen werden. Diese Logik kann sinngemäß auch auf den Bereich des Datenschutzes und des Schutzes der Privatsphäre übertragen werden.

92. Wichtiger noch — wie bereits gesagt — ist es, dass dadurch, dass juristische Personen wie Verbraucherverbände und Anbieter öffentlicher elektronischer Kommunikationsdienste das Recht erhalten, vor Gericht zu klagen, die Position der Verbraucher gestärkt und die generelle Einhaltung der Datenschutzvorschriften gefördert wird. Bei einem höheren Risiko gerichtlicher Schritte gegen sie werden zuwiderhandelnde Unternehmen wahrscheinlich stärker auf die Einhaltung der Datenschutzvorschriften achten, wodurch sich langfristig das Niveau des Schutzes der Privatsphäre und des Verbraucherschutzes erhöht. Aus all diesen Gründen ruft der EDSB das EP und den Rat auf, eine Bestimmung anzunehmen, die es juristischen Personen ermöglicht, gegen Verstöße gegen gleich welche Bestimmung der Datenschutzrichtlinie für elektronische Kommunikation gerichtlich vorzugehen.

VI. **FAZIT**

93. Der Gemeinsame Standpunkt des Rates, die erste Lesung des EP und der geänderte Vorschlag der Kommission enthalten in unterschiedlichem Maße positive Elemente, die dazu dienen würden, den Schutz der Privatsphäre und der personenbezogenen Daten natürlicher Personen zu verstärken.

94. Nach Auffassung des EDSB besteht hier aber Raum für Verbesserungen, insbesondere beim Gemeinsamen Standpunkt des Rates, in den leider einige Abänderungen des EP, die zur Gewährleistung eines angemessenen Schutzes der Privatsphäre und der personenbezogenen Daten natürlicher Personen beitragen sollten, nicht übernommen wurden. Der EDSB fordert das EP und den Rat nachdrücklich auf, die in der ersten Lesung des EP enthaltenen Garantien für den Schutz der Privatsphäre wiederherzustellen.

95. Außerdem hält es der EDSB für sinnvoll, einige Bestimmungen der Richtlinie zu straffen. Dies gilt insbesondere für die Bestimmungen über die Sicherheitsverletzungen, da nach Ansicht des EDSB der volle Nutzen der Benachrichtigung über Verletzungen am besten erreicht wird, wenn von Anfang an der richtige Rechtsrahmen festgelegt wird. Ferner hält es der EDSB für angebracht, den Wortlaut einiger Bestimmungen der Richtlinie zu verbessern und zu präzisieren.

96. Vor diesem Hintergrund fordert der EDSB das EP und den Rat nachdrücklich auf, ihre Bemühungen um die Verbesserung und Präzisierung einiger Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation zu intensivieren und gleichzeitig die vom EP in erster Lesung angenommenen Abänderungen wieder aufzunehmen, die auf die Gewährleistung eines angemessenen Niveaus des Schutzes der Privatsphäre und des Datenschutzes abzielen. Zu diesem Zweck werden nachstehend unter den Nummern 97, 98, 99 und 100 die bestehenden Probleme zusammengefasst und einige Empfehlungen und Formulierungsvorschläge unterbreitet. Der EDSB ruft alle beteiligten Seiten auf, diesen Empfehlungen und Vorschlägen Rechnung zu tragen, da sich die Datenschutzrichtlinie für elektronische Kommunikation auf dem Weg zu ihrer endgültigen Annahme befindet.

Sicherheitsverletzungen

97. Das Europäische Parlament, die Kommission und der Rat haben jeweils unterschiedliche Konzepte für die Meldung von Sicherheitsverletzungen angenommen. Unterschiede zwischen den drei Modellen bestehen unter anderem im Hinblick auf die Einrichtungen, für die die Pflicht, der Standard oder der Auslöser für die Benachrichtigung gelten soll, die betroffenen Personen, die Anspruch auf eine Benachrichtigung haben, usw. Daher müssen das EP und der Rat sich mit allen Kräften für einen soliden Rechtsrahmen in Bezug auf Sicherheitsverletzungen einsetzen. Zu diesem Zweck sollten das EP und der Rat Folgendes vorsehen:

([19]) Artikel 13 Absatz 6 (erste Lesung des EP).

([20]) Siehe z.B. § 8 des deutschen Gesetzes gegen den unlauteren Wettbewerb (UWG).

— *Beibehaltung* der Definition der Sicherheitsverletzung in den Texten von EP, Rat und Kommission, da sie ausreichend weit gefasst ist, um die meisten relevanten Situationen abzudecken, in denen eine Benachrichtigung über Sicherheitsverletzungen gerechtfertigt sein könnte;

— *Aufnahme* der Betreiber von Diensten der Informationsgesellschaft unter die Einrichtungen, für die die vorgeschlagene Meldepflicht gelten soll. Online-Händler, Online-Banken und Online-Apotheken sind wahrscheinlich in gleichem, wenn nicht in höherem Maße als Telekommunikationsunternehmen von Sicherheitsverletzungen betroffen. Die Bürger werden eine Benachrichtigung nicht nur dann erwarten, wenn es zu Sicherheitsverletzungen bei Anbietern von Internetzugängen kommt, sondern insbesondere auch dann, wenn diese bei ihrer Online-Bank oder ihrer Online-Apotheke auftreten.

— Was den Auslöser für die Benachrichtigung anbelangt, so ist der Standard *„verursacht mit großer Wahrscheinlichkeit Schaden“* ein geeigneter Standard, der für die Funktionalität der Regelung sorgt. Dabei muss aber sichergestellt werden, dass „Schaden verursachen“ genügend weit gefasst wird, um alle einschlägigen Beispiele für negative Auswirkungen auf die Privatsphäre oder andere legitime Interessen der Bürger abzudecken. Andernfalls wäre es besser, einen neuen Standard einzuführen, wonach die Benachrichtigung obligatorisch wäre, *„wenn die Sicherheitsverletzung mit großer Wahrscheinlichkeit nachteilige Folgen für die betreffenden Personen hat“*. So würde das Konzept des Rates, wonach durch die Sicherheitsverletzung die Privatsphäre einer Person *schwerwiegend* beeinträchtigt werden muss, nur einen unzureichenden Schutz für die Bürger insofern bieten, als ein solcher Standard erfordert, dass die Auswirkungen auf die Privatsphäre „schwerwiegend“ sein müssen. Zudem bietet dies Raum für eine subjektive Beurteilung.

— Zwar hat die Beteiligung einer Behörde an der Entscheidung, ob eine betroffene Einrichtung die Bürger zu benachrichtigen hat, sicherlich positive Auswirkungen, aber sie kann unpraktisch oder schwer anwendbar sein und könnte auch Mittel von anderen wichtigen Prioritäten abziehen. Der EDSB befürchtet, dass durch ein solches System sogar der Schutz der Personen verringert und unangemessener Druck auf die Behörden ausgeübt werden kann, falls die Behörden nicht äußerst schnell reagieren können. Insgesamt rät der EDSB also, ein System *einzuführen*, bei dem es den betroffenen Einrichtungen überlassen bleibt, die Notwendigkeit einer Benachrichtigung zu beurteilen.

— Damit die Behörden die Aufsicht über die von den betroffenen Einrichtungen vorgenommene Beurteilung hinsichtlich der Benachrichtigung ausüben können, sind folgende Garantien *zu verwirklichen*:

  — *Gewährleistung*, dass diese Einrichtungen verpflichtet sind, den Behörden alle Sicherheitsverletzungen zu melden, die dem geforderten Standard entsprechen;

  — *Übertragung* einer Aufsichtsfunktion an die Behörden, damit diese im Interesse der Wirksamkeit selektiv vorgehen können. Zu diesem Zweck sollte folgender Text aufgenommen werden: *„Falls der betreffende Teilnehmer oder die betreffende Person nicht bereits benachrichtigt wurde, kann die zuständige einzelstaatliche Behörde, nachdem sie die Art der Sicherheitsverletzung geprüft hat, den Anbieter von öffentlichen elektronischen Kommunikationsdiensten oder den Betreiber von Diensten der Informationsgesellschaft auffordern, dies zu tun.“*

  — *Annahme* einer neuen Bestimmung, die von den Einrichtungen verlangt, ein detailliertes und umfassendes Protokoll der internen Prüfung zu führen. Dies könnte durch die Annahme eines Textes mit folgendem Wortlaut erreicht werden: *„Die Anbieter von öffentlichen elektronischen Kommunikationsdiensten und die Betreiber von Diensten der Informationsgesellschaft führen und bewahren umfassende Aufzeichnungen, in denen alle aufgetretenen Sicherheitsverletzungen, die diesbezüglichen relevanten technischen Informationen und die getroffenen Korrekturmaßnahmen ausführlich dargelegt sind. Die Aufzeichnungen müssen ferner einen Verweis auf alle Benachrichtigungen der betreffenden Teilnehmer oder der betreffenden Personen und der zuständigen nationalen Behörden, einschließlich ihres Datums und ihres Inhalts, enthalten. Diese Aufzeichnungen sind der zuständigen nationalen Behörde auf Anfrage vorzulegen.“*

— Um eine einheitliche Umsetzung des Rahmens für Sicherheitsverletzungen zu gewährleisten, wird die Kommission ermächtigt, nach Konsultation des EDSB, der Datenschutzgruppe „Artikel 29“ und anderer einschlägiger Interessenträger technische Durchführungsmaßnahmen zu erlassen.

— In Bezug auf die zu benachrichtigenden Personen ist die Begriffswahl der Kommission oder des EP — „betreffende Personen“ oder „betroffene Nutzer“ *zu verwenden*, da diese alle Personen erfasst, deren personenbezogene Daten kompromittiert wurden.

Öffentlich zugängliche private Netze

98. Kommunikationsdienste werden der Öffentlichkeit häufig nicht über öffentliche Netze zur Verfügung gestellt, sondern über privat betriebene Netze (z. B. Hot Spots in Hotels und Flughäfen), die wohl nicht unter diese Richtlinie fallen. Das EP hat die Abänderung 121 (Artikel 3) angenommen, durch die der Anwendungsbereich der Richtlinie erweitert wird, damit öffentliche und private Kommunikationsnetze sowie öffentlich zugängliche private Netze erfasst werden. In diesem Zusammenhang sollten das EP und der Rat folgende Maßnahmen einleiten:

— *Bewahrung* der Abänderung 121 in ihrem Wesen, aber *Umformulierung*, damit nur *„die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen oder öffentlich zugänglichen privaten Kommunikationsnetzen in der Gemeinschaft, …“* in den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation fällt. Rein privat betriebene Netze (im Gegensatz zu öffentlich zugänglichen privaten Netzen) wären nicht ausdrücklich betroffen;

— entsprechende *Änderung* aller Durchführungsbestimmungen, so dass sie sich neben öffentlichen Netzen ausdrücklich auch auf öffentlich zugängliche Netze beziehen;

— *Aufnahme* folgender Definition: „*Öffentlich zugängliches privates Netz' bezeichnet ein privat betriebenes Netz, zu dem Angehörige der breiten Öffentlichkeit normalerweise unbeschränkten Zugang haben, ganz gleich ob entgeltlich oder unentgeltlich oder in Verbindung mit anderen Dienstleistungen oder Angeboten, sofern sie die geltenden Bedingungen akzeptieren*." Dies wird für mehr Rechtssicherheit im Hinblick auf die Einrichtungen sorgen, die unter den neuen Anwendungsbereich fallen.

— *Annahme* eines neuen Erwägungsgrunds, dem zufolge die Kommission eine öffentliche Konsultation zur Anwendung der Datenschutzrichtlinie für elektronische Kommunikation auf alle privaten Netze mit Beiträgen des EDSB, der Datenschutzgruppe „Artikel 29" und anderer einschlägiger Interessenvertreter durchführen wird. Dabei ist zu präzisieren, dass die Kommission im Ergebnis der öffentlichen Konsultation geeignete Vorschläge unterbreiten sollte, um die Arten von Einrichtungen, die unter diese Richtlinie fallen sollten, zu erweitern oder zu begrenzen.

Verarbeitung von Verkehrsdaten zu Sicherheitszwecken

99. Das EP hat in erster Lesung die Abänderung 181 (Artikel 6 Absatz 6a) angenommen, die die Verarbeitung von Verkehrsdaten zu Sicherheitszwecken erlaubt. Der Gemeinsame Standpunkt des Rates enthält eine neue Version, in der einige der Garantien für den Schutz der Privatsphäre abgeschwächt werden. In diesem Zusammenhang empfiehlt der EDSB dem EP und dem Rat, Folgendes vorzusehen:

— gänzliche *Ablehnung* dieses Artikels, da er unnötig ist und bei Missbrauch den Datenschutz und den Schutz der Privatsphäre natürlicher Personen übermäßig gefährden könnte;

— alternativ dazu *Aufnahme* der Datenschutzgarantien, die in der vorliegenden Stellungnahme behandelt werden (und jenen in der Abänderung des EP gleichen), falls doch eine Variante der aktuellen Version von Artikel 6 Absatz 6a angenommen werden soll.

Gerichtliches Vorgehen gegen Verstöße gegen die Datenschutzrichtlinie für elektronische Kommunikation

100. Das Parlament hat die Abänderung 133 (Artikel 13 Absatz 6) angenommen, die es juristischen Personen ermöglicht, gegen Verstöße gegen die Bestimmungen der Richtlinie gerichtlich vorzugehen. Leider wurde sie vom Rat nicht übernommen. Der Rat und das EP sollten Folgendes vorsehen:

— *Billigung* der Bestimmung, die juristischen Personen wie Verbraucherverbänden und Berufsgenossenschaften das Recht einräumt, gegen Verstöße gegen gleich welche Bestimmung der Richtlinie (nicht nur gegen Verstöße gegen die Spam-Bestimmungen, wie es derzeit in dem Gemeinsamen Standpunkt und dem geänderten Vorschlag vorgesehen ist) gerichtlich vorzugehen. Eine größere Vielfalt der Durchsetzungsmechanismen wird eine bessere Einhaltung und wirksamere Anwendung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation insgesamt begünstigen.

Der Herausforderung begegnen

101. In allen obengenannten Belangen müssen sich das EP und der Rat der Herausforderung stellen, geeignete Vorschriften und Bestimmungen auszuarbeiten, die praktikabel und funktional sind und das Recht der Bürger auf Schutz der Privatsphäre und Datenschutz achten. Der EDSB hofft, dass sich die beteiligten Seiten nach Kräften bemühen werden, diese Herausforderung zu bewältigen, und dass diese Stellungnahme einen Beitrag dazu leisten kann.

Geschehen zu Brüssel am 9. Januar 2009.

Peter HUSTINX

Europäischer Datenschutzbeauftragter