ARTIKEL-29-DATENSCHUTZGRUPPE

01119/13/DE

WP 197

Stellungnahme 6/2012 zum Entwurf des Beschlusses der Kommission über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation)[1]

Angenommen am 12. Juli 2012

[1] Die Stellungnahme bezieht sich auf den Beschluss der Kommission („Entwurf des Beschlusses der Kommission über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)“), der aus technischen Gründen in eine Verordnung („Verordnung über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)“) umgewandelt wurde.

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union 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 durch die Generaldirektion Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_de.htm

DIE DATENSCHUTZGRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN

BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

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

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

gestützt auf ihre Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 Einführung und Anwendungsbereich des Beschlussentwurfs

Nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG (im Folgenden „*Datenschutzrichtlinie für elektronische Kommunikation*"), kann die Europäische Kommission (im Folgenden die „*Kommission"*) nach Anhörung der maßgeblichen Beteiligten, einschließlich der Artikel-29-Datenschutzgruppe (im Folgenden *„Datenschutzgruppe"*), Durchführungsmaßnahmen zu Artikel 4 Absätze 2, 3 und 4 der Richtlinie erlassen.

Wie insbesondere im Erwägungsgrund 5 hervorgehoben wird, bezieht sich der Entwurf des Kommissionsbeschlusses (im Folgenden der „Beschluss") nur auf die Absätze 3 und 4, die Verletzungen des Schutzes personenbezogener Daten betreffen. Deshalb ist davon auszugehen, dass das *besondere Risiko der Verletzung der Netzsicherheit* Gegenstand eines anderen Beschlusses der Kommission sein wird. Der Beschluss muss außerdem im Hinblick auf den Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten[2] geprüft werden, in dem vorgeschlagen wird, die Verpflichtung zur Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten auf alle für die Datenverarbeitung Verantwortlichen auszuweiten.

Die Datenschutzgruppe begrüßt diesen Beschluss, da er zur Harmonisierung der Vorschriften beitragen wird, die in der Praxis zur Meldung von Verstößen gegen die Datensicherheit angewandt werden.

In der folgenden Stellungnahme möchte die Datenschutzgruppe die Kommission jedoch auf einige Punkte des Beschlusses aufmerksam machen, die eine Klarstellung oder Verbesserung erfordern.

---

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

2 Analyse

2.1 Terminologie und Rechtssicherheit

Die Datenschutzgruppe begrüßt die eingehenden Bemühungen der Kommission, die Bestimmungen über die Verletzung des Schutzes personenbezogener Daten in der Richtlinie klar und eindeutig zu formulieren.

Die Datenschutzgruppe hält es allerdings für bedenklich, dass häufig ungenaue Formulierungen verwendet werden, wie beispielsweise „ausreichend", „zumutbar" oder „außergewöhnliche Umstände", die zu unterschiedlichen Auslegungen und zu Rechtsunsicherheit mit negativen Folgen für alle Beteiligten führen könnten.

a) Die Begriffe „ausreichend", „zumutbar" und „angemessen"

Artikel 2 Absatz 2 besagt Folgendes: *„*Bei einer Verletzung des Schutzes personenbezogener Daten *benachrichtigt der Betreiber die zuständige nationale Behörde von der Verletzung des Schutzes personenbezogener Daten binnen 24 Stunden,* nachdem der Betreiber mit **ausreichender Sicherheit** festgestellt hat, dass eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist*".* Zur Vermeidung von Unklarheiten hinsichtlich des Zeitpunkts, ab dem die 24-stündige Frist beginnt, schlägt die Datenschutzgruppe folgende Vereinfachung dieses Satzes vor: *„*Bei einer Verletzung des Schutzes personenbezogener Daten *benachrichtigt der Betreiber die zuständige nationale Behörde von der Verletzung des Schutzes personenbezogener Daten binnen 24 Stunden nach der Feststellung der Verletzung.*"

Zudem weist die Datenschutzgruppe darauf hin, dass der Beschluss keine klaren Regelungen für die Fälle enthält, in denen ein Betreiber eine Sicherheitsverletzung feststellt, die zu einer Verletzung des Schutzes personenbezogener Daten führen kann oder geführt haben könnte, bei denen er aber nicht feststellen kann, ob der Vorfall tatsächlich eine Verletzung des Schutzes personenbezogener Daten zur Folge hatte. Im Beschluss könnte darauf hingewiesen werden, dass der Betreiber sich dessen bewusst sein muss, dass eine festgestellte Sicherheitsverletzung, auf die der Betreiber mit den in der Branche bewährten Verfahren für den Umgang mit Sicherheitsverletzungen reagiert, tatsächlich zu einer Verletzung des Schutzes personenbezogener Daten führen kann, und er deshalb in der Lage sein sollte, eine solche Verletzung zu beurteilen und die erforderlichen Schritte einzuleiten.

In Artikel 2 Absatz 3, in dem die Begriffe „ausreichend" und „zumutbar" ebenfalls an zwei Stellen vorkommen,

- könnte die Formulierung *„kann der Betreiber zunächst binnen 24 Stunden,* nachdem er mit **ausreichender Sicherheit** festgestellt hat, dass eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, *eine Erstbenachrichtigung der zuständigen nationalen Behörden vornehmen"* ersetzt werden durch *„kann der Betreiber zunächst binnen 24 Stunden nach Feststellung der Verletzung eine Erstbenachrichtigung der zuständigen nationalen Behörden vornehmen"*.

- könnte die Formulierung „obwohl er alle **zumutbaren Anstrengungen** zur Nachforschung unternommen hat“ ersetzt werden durch *„trotz seiner Nachforschungen“*, ohne dass dadurch die Klarheit beeinträchtigt würde. Die zuständige nationale Behörde wird in jedem Fall die Argumente prüfen, die der Betreiber vorbringt, um eine verspätete Benachrichtigung zu rechtfertigen.

In Artikel 3 Absatz 8 wird der Begriff „zumutbar“ ebenfalls an zwei Stellen verwendet: *„Kann der Betreiber, obwohl er hierzu alle **zumutbaren Anstrengungen** unternommen hat, innerhalb der in Absatz 3 genannten Frist nicht alle Personen ermitteln, die von der Verletzung des Schutzes personenbezogener Daten beeinträchtigt werden, so kann er diese Personen durch Bekanntmachungen in großen nationalen Medien innerhalb dieser Frist benachrichtigen. Diese Bekanntmachungen müssen die in Anhang II aufgeführten Angaben enthalten, falls nötig in gekürzter Form. In diesem Fall muss der Betreiber* zudem *weiterhin **alle zumutbaren Anstrengungen unternehmen,** um diese Personen zu ermitteln und sie sobald wie möglich mit den in Anhang II aufgeführten Angaben zu benachrichtigen.*“ Die Datenschutzgruppe schlägt vor, diesen Absatz durch die Streichung der Verweise auf „zumutbare Anstrengungen“ wie folgt zu vereinfachen: *„Kann der Betreiber innerhalb der in Absatz 3 genannten Frist nicht alle Personen ermitteln, die von der Verletzung des Schutzes personenbezogener Daten beeinträchtigt werden, so kann er die Personen,* die er nicht ermitteln konnte, *durch Bekanntmachungen in großen nationalen Medien innerhalb dieser Frist benachrichtigen. Diese Bekanntmachungen müssen die in Anhang II aufgeführten Angaben enthalten, falls nötig in gekürzter Form. In diesem Fall muss der Betreiber* zudem *weiterhin Anstrengungen unternehmen, um diese Personen zu ermitteln und sie sobald wie möglich mit den in Anhang II aufgeführten Angaben zu benachrichtigen.“*

In Erwägungsgrund 6 und Artikel 3 Absatz 3 sollte die Verwendung der Begriffe „ausreichend“ und „zumutbar“ ebenfalls vermieden werden.

Auch in Artikel 3 Absatz 7 heißt es: *„Der Betreiber benachrichtigt den Teilnehmer oder die Person von der Verletzung des Schutzes personenbezogener Daten mit Hilfe von* **angemessen** gesicherten *Kommunikationsmitteln, die einen zügigen Empfang der Informationen gewährleisten“.* Die Datenschutzgruppe schlägt vor, den letzten Teil wie folgt zu ersetzen: *„mit Hilfe von Kommunikationsmitteln, die einen zügigen Empfang der Informationen gewährleisten und nach dem Stand der Technik angemessen gesichert[3] sind“.*

b) Die Formulierung „außergewöhnliche Umstände“

Unklarheiten entstehen auch durch die Formulierung *„außergewöhnliche Umstände“*. Die Datenschutzgruppe stellt fest, dass in den innerstaatlichen Rechtsvorschriften oder in der Rechtsprechung möglicherweise bereits eine Definition „außergewöhnlicher Umstände“ vorliegt, die zum Beispiel auf *„besonders schwerwiegende unvorhersehbare Ereignisse“*, wie Krieg oder erhebliche Bedrohungen der öffentlichen Sicherheit, verweist. Diese Auslegungen

[3] „Gesichert“ bedeutet „die Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten“.

erscheinen unvereinbar mit der Harmonisierung und Klarstellung, auf die der Beschluss abzielt.

Daher empfiehlt die Datenschutzgruppe, im Beschluss folgende Klarstellung vorzunehmen:

1) Im letzten Absatz von Artikel 2 Absatz 3 könnte die Formulierung „**Unter außergewöhnlichen Umständen**, unter denen der Betreiber, obwohl er hierzu **alle zumutbaren Anstrengungen** zur Nachforschung unternommen hat …" ersetzt werden durch *„Ist der Betreiber trotz seiner Nachforschungen …"*.

Der Einheitlichkeit halber sollte in Erwägungsgrund 6 ein ähnlicher Wortlaut verwendet werden.

Außerdem empfiehlt die Datenschutzgruppe, in den Beschluss einen ausdrücklichen Verweis auf Artikel 15 Buchstabe a der Datenschutzrichtlinie für elektronische Kommunikation aufzunehmen, um hervorzuheben, dass eine fehlende oder unvollständige Anzeige von Verletzungen des Schutzes personenbezogener Daten einen Verstoß gegen die für den Schutz personenbezogener Daten geltenden Rechtsvorschriften darstellen dürfte.

2) Artikel 3 Absatz 6 des Beschlusses besagt Folgendes: *„Unter außergewöhnlichen Umständen, unter denen die ordnungsgemäße Untersuchung der Verletzung des Schutzes personenbezogener Daten durch die Benachrichtigung des Teilnehmers oder der Person gefährdet würde, kann der Betreiber nach Zustimmung der zuständigen nationalen Behörde die Benachrichtigung des Teilnehmers oder der Person* für eine bestimmte Zeit *aufschieben".* Die Datenschutzgruppe begrüßt die Tatsache, dass die Benachrichtigung der zuständigen Behörde nicht grundsätzlich aufgeschoben wird, und sie kann nachvollziehen, dass unter bestimmten Umständen ein Aufschub der Benachrichtigung von Personen notwendig werden kann, um beispielsweise einer polizeilichen Ermittlung nicht vorzugreifen. Die Verwendung der Formulierung „außergewöhnliche Umstände" führt jedoch zu Rechtsunsicherheit hinsichtlich des Umfangs dieser Ausnahmeregelung und könnte den Betreibern einen großen Ermessensspielraum für die Aufschiebung der Benachrichtigung betroffener Personen einräumen. Die Datenschutzgruppe ersucht die Kommission, ausdrücklich festzulegen, welche Umstände als „außergewöhnliche Umstände" im Sinne des Textes[4] gelten. In diesem Zusammenhang sollte dem Schutz von Personen stets Priorität eingeräumt werden, wenn es darum geht, zwischen dem rechtmäßigen Interesse einer polizeilichen Ermittlung und der Verpflichtung zur Benachrichtigung von Personen in Fällen abzuwägen, in denen solche

[4] Die Kommission kann beispielsweise den Wortlaut von Artikel 1 der Richtlinie 2006/24/EG verwenden, in dem ausdrücklich verwiesen wird auf „Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden", wenn sie explizit auf schwerwiegende Fälle, in denen polizeilich ermittelt wird, Bezug nehmen möchte. Soll die Formulierung „außergewöhnliche Umstände" konkret auf die Cyberkriminalität verweisen, so kann die Kommission einen anderen Wortlaut verwenden.

Informationen wirksam zur Minderung möglicher nachteiliger Auswirkungen der Verletzung beitragen können.

c) Weitere Anmerkungen

In Erwägungsgrund 6 beginnt der erste Satz mit der Formulierung „*Die Betreiber **sollten** die zuständige nationale Behörde ...*“. Die Datenschutzgruppe schlägt vor, hier anstelle von „Die Betreiber sollten …“ die Formulierung „Die Betreiber benachrichtigen …“ zu verwenden, um die Einheitlichkeit mit Artikel 2 Absatz 1 des Beschlusses sowie der Richtlinie sicherzustellen.

Außerdem regt die Datenschutzgruppe an, Artikel 3 Absatz 5 des Beschlusses zu streichen, da er keine zusätzlichen Informationen, Empfehlungen oder Anforderungen in Bezug auf den Text enthält, der bereits in der Richtlinie sowie in Artikel 3 Absatz 1 des Beschlusses vorhanden ist.

2.2 Benachrichtigung der zuständigen nationalen Behörde

In Artikel 4 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation ist Folgendes festgelegt: *„Im Falle einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste unverzüglich die zuständige nationale Behörde von der Verletzung.“*

Der im Beschluss verwendete Begriff *„unangemessene Verzögerung“* bezeichnet Verzögerungen, die über die beiden festgelegten Fristen hinausgehen: erstens die Frist von 24 Stunden nach Feststellung der Verletzung, innerhalb deren eine „Erstbenachrichtigung“ mit ersten Angaben erfolgen muss, und zweitens die Frist von drei Tagen nach dieser Erstbenachrichtigung, innerhalb deren eine vollständige Benachrichtigung zu übermitteln ist. In Anhang I des Beschlusses sind die Mindestvorgaben zum Inhalt der Erstbenachrichtigung (Abschnitt 1) und der vollständigen Benachrichtigung (Abschnitt 2) festgelegt.

Unter dem Vorbehalt der oben erläuterten Anmerkungen zur Verwendung der Begriffe „ausreichend“ und „zumutbar“ begrüßt die Datenschutzgruppe die Tatsache, dass spezifische Verzögerungen in den Beschluss aufgenommen werden. Sie unterstützt ferner das zweistufige Benachrichtigungsmodell, durch das Reaktionsfähigkeit und die Vollständigkeit der Benachrichtigungen kombiniert werden können.

Die Datenschutzgruppe schlägt mehrere Änderungen vor, um die Kommunikation zwischen dem Betreiber und der Behörde zu erleichtern und eine bessere Harmonisierung[5] zu erreichen.

---

[5] Bei der Erarbeitung zukünftiger Rechtsvorschriften über Verletzungen des Schutzes personenbezogener Daten könnte die Kommission unter anderem prüfen, ob die zuständigen Behörden von allen Verletzungen des Schutzes personenbezogener Daten benachrichtigt werden müssen oder ob in bestimmten Fällen Ausnahmeregelungen gelten, sofern alle Verletzungen in dem Verzeichnis erfasst werden, das von dem für die Verarbeitung Verantwortlichen geführt wird.

a) Zu übermittelnde Informationen und Erstbenachrichtigung

Das absolute Minimum an Informationen, die ein Betreiber der zuständigen Behörde innerhalb von 24 Stunden nach Feststellung der Verletzung übermitteln muss, beschränkt sich auf den Namen des Betreibers und den Namen des Ansprechpartners (Anhang I, Abschnitt 1). Somit ist diese Erstbenachrichtigung, wenn sie keine zusätzlichen Informationen enthält, für die zuständige Behörde nur von geringem Wert. Nach Auffassung der Datenschutzgruppe sollte von den Betreibern verlangt werden, dass sie mehr Informationen als von der Kommission vorgeschlagen an die zuständige Behörde übermitteln, damit die Betreiber so zur Einführung wirksamer Maßnahmen zum Schutz personenbezogener Daten angehalten werden. Die Datenschutzgruppe ist der Meinung, dass ein Betreiber die zuständige Behörde über alle Einzelheiten informieren sollte, die ihm zum Zeitpunkt der Erstbenachrichtigung bekannt sind. Zumindest sollte für die Erstbenachrichtigung eine bestimmte Anzahl weiterer Angaben verbindlich vorgeschrieben werden. Nach Auffassung der Datenschutzgruppe hat der Betreiber, nachdem er eine Verletzung des Schutzes personenbezogener Daten festgestellt hat, zumindest Kenntnis von der Art der betroffenen personenbezogenen Daten, von den Umständen der Verletzung oder von der Art der Gefährdung (Verlust, Diebstahl, Vervielfältigung usw.) sowie davon, wie die Verletzung festgestellt wurde (verwendete Software zur Erkennung von Verletzungen, Auswertung der Protokolle, Meldung eines Vorfalls durch einen Mitarbeiter usw.). Diese Informationen sollten in die Erstbenachrichtigung aufgenommen und in der zweiten Benachrichtigung ergänzt und/oder berichtigt werden.

Die Datenschutzgruppe schlägt vor, in Anhang I Abschnitt 1 des Beschlusses folgende Informationen aufzunehmen:

- Umstände der Verletzung des Schutzes personenbezogener Daten/Art der Gefährdung (z. B. Verlust, Diebstahl, Vervielfältigung)
- Art und Weise, wie die Verletzung festgestellt wurde
- Datum und Zeitpunkt der Feststellung des Vorfalls und Datum und Zeitpunkt, an dem sich der Vorfall ereignete
- Art und Inhalt der betroffenen personenbezogenen Daten
- Durchgeführte Kontrollen (insbesondere in Bezug auf die Unverständlichkeit personenbezogener Daten)

Die Datenschutzgruppe hat dieses Thema bereits in ihrer Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation aufgegriffen.

Im Beschluss sollte außerdem in eindeutiger Form darauf hingewiesen werden, dass der Betreiber die Angaben in der Erstbenachrichtigung in der vollständigen zweiten Benachrichtigung ändern kann.

Abschließend schlägt die Datenschutzgruppe vor, die Aufzählungspunkte durch Ziffern zu ersetzen, um so Verweise auf die in Anhang I aufgeführten Einzelheiten der Benachrichtigung zu ermöglichen. Dies ist auch bei der Entwicklung eines einheitlichen Ansatzes für die Benachrichtigung auf elektronischem Weg nützlich.

b) Elektronische Mittel

Der Einsatz elektronischer Mittel erscheint für die Übermittlung von Benachrichtigungen als geeignet; die Datenschutzgruppe unterstützt daher die Initiative der Europäischen Kommission, derartige Mittel nach Möglichkeit zu fördern. Diese elektronischen Mittel müssen jedoch nicht umgehend in allen Mitgliedstaaten eingeführt werden: Zunächst muss ein einheitliches Format für elektronische Benachrichtigungen definiert werden und es müssen geeignete Sicherheitsmaßnahmen festgelegt und die elektronischen Mittel (Portal und/oder andere Systeme, wie z. B. sichere E-Mail) entwickelt und getestet werden, mit denen dieser Mechanismus in allen Mitgliedstaaten unterstützt wird.

Im Beschluss sollte daher festgelegt werden, dass in Zusammenarbeit mit den maßgeblichen Beteiligten ein einfaches und einheitliches europäisches Format für elektronische Benachrichtigungen (z. B. in XML) entwickelt werden soll. Sobald dieses einheitliche Format festgelegt worden ist, sollte die Europäische Kommission eine Frist von mindestens zwölf Monaten für die Einführung der Benachrichtigung durch elektronische Mittel einräumen. In der Übergangsphase sollten auch andere Benachrichtigungsverfahren zulässig sein.

Die Datenschutzgruppe bittet die Kommission um Auskunft darüber, ob und wie sie ein mögliches Projekt der Datenschutzgruppe und einzelner Datenschutzbehörden finanziell und logistisch unterstützen könnte, dessen Ziel darin besteht, ein einheitliches Format festzulegen und eine technische Lösung einzuführen, die für die Benachrichtigung der Datenschutzbehörden über Verletzungen des Schutzes personenbezogener Daten, die durch die für die Verarbeitung Verantwortlichen vorgenommen wird, und für den Informationsaustausch über die Verletzung, der in grenzübergreifenden Fällen zwischen den Behörden erfolgt, eingesetzt werden. Bei diesem Projekt sollen auch die Lösungen berücksichtigt werden, die in einigen Mitgliedstaaten bereits eingesetzt oder derzeit entwickelt werden.

c) Benachrichtigung von anderen betroffenen nationalen Behörden

In Artikel 2 Absatz 5 schreibt der Beschluss die Benachrichtigung der anderen betroffenen nationalen Behörden vor: *„Betrifft die Verletzung des Schutzes personenbezogener Daten*

Teilnehmer oder Personen aus anderen Mitgliedstaaten als dem der von der Verletzung benachrichtigten zuständigen nationalen Behörde …".

Die Datenschutzgruppe begrüßt und unterstützt die aktive Zusammenarbeit der Behörden und ist sich der Notwendigkeit der Zusammenarbeit der zuständigen nationalen Behörden vollkommen bewusst. Sämtliche Mitglieder der Datenschutzgruppe bekennen sich zu ihrer Verpflichtung, in diesem Bereich zusammenzuarbeiten.

Diese Verpflichtung ist in der Richtlinie jedoch nicht festgelegt, womit sich für die Datenschutzgruppe die Frage stellt, welche Rechtsgrundlage für eine solche Verpflichtung besteht und welche praktischen Auswirkungen eine unterlassene Benachrichtigung der anderen nationalen Behörden nach sich zieht. Darüber hinaus weist die Datenschutzgruppe darauf hin, dass die in Anhang I vorgegebene Form der Benachrichtigung der zuständigen nationalen Behörde keine Möglichkeit bietet, den Wohnort oder die Nationalität der von der Verletzung betroffenen Personen festzustellen, und dass im Beschluss eine klare Definition der „Teilnehmer oder Personen in anderen Mitgliedstaaten" fehlt.

Aus diesem Grund fordert die Datenschutzgruppe die Kommission auf, den Anwendungsbereich der Bestimmung in Artikel 2 Absatz 5 genauer zu beschreiben und die praktischen Instrumente zu benennen, die die zuständigen Behörden für die Zusammenarbeit nutzen sollten.

2.3 Benachrichtigung der Teilnehmer oder der betroffenen Personen

Die Datenschutzgruppe begrüßt es, dass in dem Beschluss ein Verfahren für die Fälle beschrieben wird, in denen betroffene Personen nicht direkt zu erreichen sind.

Die Datenschutzgruppe begrüßt außerdem die Beschreibung der Umstände, die bei der Beurteilung der Frage zu berücksichtigen sind, ob durch die Verletzung des Schutzes personenbezogener Daten die personenbezogenen Daten eines Teilnehmers oder einer Person oder deren Privatsphäre beeinträchtigt werden, wie in Artikel 3 Absatz 2 des Beschlusses erläutert wird.

In Artikel 3 Absatz 7 wird darauf hingewiesen, dass die Aufnahme von „Informationen über die Verletzung des Schutzes personenbezogener Daten in eine reguläre Rechnung" kein geeignetes Mittel zur Benachrichtigung von Personen ist. Es ist jedoch nicht eindeutig, ob es sich dabei nur um ein Beispiel handelt, oder ob der Beschluss darauf abzielt, lediglich die Verwendung von Rechnungen als Mittel zur Information von Personen über eine Verletzung des Schutzes personenbezogener Daten zu untersagen. Grundsätzlich ist die Datenschutzgruppe der Auffassung, dass sich Informationen über eine Verletzung des Schutzes personenbezogener Daten deutlich von anderen Informationen abheben sollten, die zwischen Betreibern und Personen ausgetauscht werden. Die Datenschutzgruppe schlägt daher vor, dass im Beschluss festgelegt wird, dass die Informationen über die Verletzung des Schutzes personenbezogener Daten sich gezielt auf die Verletzung beziehen müssen und nicht mit Informationen über ein anderes Thema verknüpft werden dürfen.

Was den Einsatz der Medien angeht, um Personen zu erreichen, die der Betreiber nicht ermitteln konnte, gibt die Datenschutzgruppe zu bedenken, dass die großen nationalen Medien nicht grundsätzlich die geeignetsten Medien sind, z. B. in Fällen, in denen ein lokaler Betreiber Personen innerhalb eines begrenzten geografischen Gebiets erreichen will. Um diesen Punkt besonders hervorzuheben, könnten in Artikel 3 Absatz 8 nach „durch Bekanntmachungen in großen nationalen“ die Worte „oder regionalen“ eingefügt werden.

Außerdem sollten, wie im folgenden Abschnitt erläutert wird, ausführlichere Leitlinien bereitgestellt werden, die die Behörden und die Betreiber bei der objektiven und einheitlichen Beurteilung der Schwere von Verletzungen des Schutzes personenbezogener Daten unterstützen.

2.4 Beurteilung der Schwere und der nachteiligen Auswirkungen

Im Zuge der Umsetzung der Richtlinie 2009/136/EG wächst die Zahl der bei den zuständigen Behörden eingehenden Benachrichtigungen von Verletzungen des Schutzes personenbezogener Daten, welche in ihrem Ausmaß und Schweregrad stark variieren. Es ist wichtig, dass die Behörden die besonders problematischen Verletzungen feststellen, um somit die Schwerpunkte ihrer Maßnahmen festlegen zu können, die insbesondere die Möglichkeit bieten, die Betreiber unter bestimmten Umständen zur Benachrichtigung der betroffenen Personen zu zwingen. Darüber hinaus müssen die Betreiber die nachteiligen Auswirkungen einer Verletzung eindeutig und objektiv beurteilen, damit sie entscheiden können, ob eine Benachrichtigung der betroffenen Personen gerechtfertigt ist.

Vor dem Hintergrund dieser Überlegungen hält die Datenschutzgruppe eine einheitliche und leicht verständliche Methodik zur Beurteilung des Schweregrads für Betreiber und zuständige Behörden in Europa für erforderlich. Artikel 3 Absatz 2 sieht allerdings keine Skala oder objektiven Kriterien zur Beurteilung des Schweregrads einer Verletzung vor. Auch werden keine Schwellenwerte festgelegt, die als Grundlage für die Entscheidung darüber dienen könnten, ob der Betreiber die betroffenen Personen benachrichtigen muss.

Detailliertere Leitlinien zu diesen Punkten würden zu einer wesentlichen Verbesserung des Beschlusses beitragen. Sowohl die zuständigen Behörden als auch die Betreiber müssen den Schweregrad einer Verletzung des Schutzes personenbezogener Daten nach einheitlichen Kriterien verstehen und bewerten. Dieses Verständnis ist nicht nur auf nationaler Ebene, sondern auch auf europäischer Ebene von Bedeutung, damit eine Fragmentierung bei der Umsetzung der Richtlinie und des Beschlusses vermieden wird.

Um diesem Erfordernis nachzukommen, unterstützt die Datenschutzgruppe ausdrücklich die Festlegung einer harmonisierten paneuropäischen Methodik zur Beurteilung des Schweregrads, die sich auf objektive Kriterien stützt. Die Datenschutzgruppe arbeitet derzeit

gemeinsam mit der ENISA an der Entwicklung einer solchen Methodik.[6] Die vorgeschlagene Methodik soll eine Skala des Schweregrads beinhalten, in der die nachteiligen Auswirkungen auf Personen, die notwendigen Schritte zur Ermittlung der Personen anhand der Daten und das Ausmaß der Gefährdung der Daten, die von der Verletzung betroffen sind, berücksichtigt werden. Die Anzahl der von der Verletzung betroffenen Personen sollte jedoch keinesfalls als Kriterium für die Entscheidung darüber herangezogen werden, ob eine Benachrichtigung der betroffenen Personen erforderlich ist. Die Datenschutzgruppe fordert die Kommission auf, dafür zu sorgen, dass bei der Beurteilung des Schweregrads von allen Beteiligten ein einheitlicher Ansatz verfolgt wird. Daher sollte in einem gesonderten Artikel des Beschlusses ausdrücklich auf die Entwicklung eines Rahmens für die Beurteilung des Schweregrads eingegangen werden.

Die Datenschutzgruppe schlägt zudem vor, dass im Beschluss in die in Anhang I Abschnitt 2 verlangten Angaben auch die für die Beurteilung des Schweregrads relevanten Kriterien sowie das Ergebnis der Einstufung des Schweregrads (beispielsweise „hoch“, „mittel“, „gering“ oder „unbedeutend“) und eine Begründung der jeweiligen Beurteilung aufgenommen werden.

2.5 Technische Schutzmaßnahmen und Unverständlichkeit der Daten

In Artikel 4 des Beschlusses wird ausführlicher erläutert, welche Maßnahmen als geeignet anzusehen sind, um Daten unverständlich zu machen. Diese in erster Linie auf den Empfehlungen der ENISA basierenden Umsetzungsmaßnahmen verdeutlichen, dass die Daten entweder verschlüsselt, mit einer verschlüsselten Hash-Funktion bearbeitet oder unwiederbringlich gelöscht worden sein müssen, damit sie als unverständlich gelten können. In der Beschreibung der Maßnahmen wird richtigerweise darauf verwiesen, dass die jeweiligen kryptografischen Schlüssel nicht leicht zu ermitteln und durch keine Sicherheitsverletzungen beschädigt worden sein dürfen. Die Datenschutzgruppe befürwortet derartige Maßnahmen und ist der Meinung, dass die Beteiligten damit zu wirksameren Sicherheitsvorkehrungen angehalten werden und in allen Mitgliedstaaten gleichzeitig eine größere Rechtssicherheit in Bezug auf die Unverständlichkeit von Daten erreicht wird.

Betrifft eine Verletzung des Schutzes personenbezogener Daten nur Daten, die unverständlich gemacht wurden, sollte für den Betreiber bei einer Verletzung des Schutzes personenbezogener Daten von Rechts wegen keine Verpflichtung zur Benachrichtigung der betroffenen Personen bestehen. Die Datenschutzgruppe möchte jedoch betonen, dass dieser Beschluss bei den Betreibern nicht der Eindruck hervorrufen darf, dass bereits die Einführung von Verschlüsselung, Streuspeicherung (Hashing) oder sicherer Datenlöschung als ausreichend dafür gilt, dass Betreiber pauschal für sich in Anspruch nehmen können, dass sie die allgemeine Schutzpflicht gemäß Artikel 17 der Richtlinie 95/46/EG erfüllen. In dieser

---

[6] Nach den „Empfehlungen für Leitlinien zur technischen Umsetzung von Artikel 4“ („Recommendations on technical implementation guidelines of Article 4“) der ENISA.

Hinsicht sind von den Betreibern auch geeignete organisatorische und technische Vorkehrungen zu treffen, um Verletzungen des Schutzes personenbezogener Daten vorzubeugen bzw. diese festzustellen und abzuwehren. Zu diesem Zweck benötigen die Betreiber einen Rahmen für das Risikomanagement[7], anhand dessen sie eine Entscheidung über die geeigneten Maßnahmen treffen können, die eingeführt werden sollen. Wichtig ist zudem, dass sie etwaige Restrisiken berücksichtigen, die auch nach der Einführung von Kontrollmaßnahmen noch vorhanden sein könnten, um verstehen zu können, wo möglicherweise noch Verletzungen des Schutzes personenbezogener Daten auftreten könnten. Die Datenschutzgruppe empfiehlt der Kommission, diesen Punkt in einem Erwägungsgrund des Beschlusses zu erläutern.

Zur Definition des Begriffs *„unverständliche Daten"* schlägt die Datenschutzgruppe vor, den Text an mehreren Stellen geringfügig zu ändern, um Missverständnisse zu vermeiden. Zur klareren Unterscheidung zwischen Verschlüsselung und Hashing sollte Absatz 2 Buchstabe a wie folgt in zwei Teile gegliedert werden:

> *2. Daten gelten als unverständlich, wenn:*
>
> *a) sie auf sichere Weise mit einem Standardalgorithmus verschlüsselt worden sind, der zur Entschlüsselung verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zur Entschlüsselung verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann, oder*
>
> *a) sie durch ihren mit einer kryptografischen verschlüsselten Standard-Hash-Funktion berechneten Hash-Wert ersetzt worden sind, der zum Daten-Hashing verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zum Daten-Hashing verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann, oder*
>
> *c) sie unwiederbringlich gelöscht worden sind, entweder durch physische Zerstörung des Mediums, auf dem sie gespeichert waren, oder durch Anwendung eines sicheren Löschalgorithmus.*

Durch die vorgeschlagene Unterscheidung zwischen Verschlüsselung und Hashing können die folgenden wichtigen Punkte hervorgehoben werden, die aus dem aktuellen Wortlaut des Beschlusses möglicherweise nicht ganz klar hervorgehen:

---

[7] Im Mittelpunkt des Rahmens muss der Schutz personenbezogener Daten stehen und in ihm sollten die potenziellen Auswirkungen für die betroffenen Personen aufgezeigt werden, anstatt das Hauptaugenmerk allein auf für die Geschäftstätigkeit bestehende Risiken und den Schutz von Unternehmen gegen rechtliche Risiken zu richten.

1) Genau genommen spielt für die Sicherheit der Verschlüsselung die Sicherheit des Schlüssels, der zur „Entschlüsselung“ verwendet wird, eine wichtigere Rolle als der Schlüssel, der zur „Verschlüsselung“ verwendet wird. Diese Unterscheidung ist für symmetrische Algorithmen (wie etwa AES) nicht von Bedeutung, wohl aber für die asymmetrische Verschlüsselung (wie beispielsweise RSA).

2) Die Sicherheit einer verschlüsselten Hash-Funktion hängt von dem Schlüssel ab, der zur Berechnung der Hash-Funktion verwendet wird; einen Schlüssel zur „Entschlüsselung“ oder „Verschlüsselung“ gibt es nicht.

3) Beim Hashing sollte klargestellt werden, dass die ursprünglichen Daten durch einen Hash-Wert „ersetzt“ worden sind (wie z. B. in Passwortdatenbanken) und dass der Hash-Wert nicht mit anderen direkt oder indirekt identifizierbaren Daten verknüpft ist.

4) Wichtig ist außerdem, klarzustellen, dass die Geheimhaltung der jeweiligen Schlüssel gegenüber Personen gilt, die *„zum Zugriff auf den Schlüssel nicht befugt sind“*. Daher darf es, wie im Text hinzugefügt, für *„Personen, die zum Zugriff auf den Schlüssel nicht befugt sind“* nicht möglich sein, den Schlüssel durch eine umfassende Schlüsselsuche zu ermitteln.

Außerdem wird in Bezug auf die Löschung der Daten vorgeschlagen, die Formulierung *„auf sichere Weise gelöscht“* durch *„unwiederbringlich gelöscht“* zu ersetzen, um das beabsichtigte Ziel dieser Maßnahme noch deutlicher herauszustellen.

2.6 Sonstiges

Die Datenschutzgruppe stellt fest, dass der Entwurf des Beschlusses keine Bestimmung oder keinen Erwägungsgrund in Bezug auf das in Artikel 4 Absatz 4 der Richtlinie erwähnte Verzeichnis enthält. Da das Verzeichnis im Zusammenhang mit der Benachrichtigung eine wichtige Rolle spielt, schlägt die Datenschutzgruppe vor, in den Beschluss einen Erwägungsgrund aufzunehmen, der besagt, dass sich die Betreiber bei der Festlegung des Formats der Verzeichniseinträge auch auf den Beschluss stützen können.

Im Entwurf des Beschlusses der Kommission wird im Erwägungsgrund 11 außerdem darauf hingewiesen, dass von den Behörden Statistiken über Verletzungen des Schutzes personenbezogener Daten geführt werden. Die Datenschutzgruppe schlägt vor, im Beschluss bestimmte Einzelheiten – die aus dem einheitlichen Formular entnommen werden können – festzulegen, die statistisch erfasst werden.

Brüssel, den 12.7.2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM