VERORDNUNGEN

VERORDNUNG (EU) Nr. 611/2013 DER KOMMISSION

vom 24. Juni 2013

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)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

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 (Datenschutzrichtlinie für elektronische Kommunikation) ([1]), insbesondere auf Artikel 4 Absatz 5,

nach Anhörung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA),

nach Anhörung der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten, die gemäß Artikel 29 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ([2]) eingesetzt wurde („Artikel-29-Datenschutzgruppe"),

nach Konsultation des Europäischen Datenschutzbeauftragten,

in Erwägung nachstehender Gründe:

(1) Die Richtlinie 2002/58/EG sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Union zu gewährleisten.

(2) Gemäß Artikel 4 der Richtlinie 2002/58/EG sind Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet, unverzüglich die zuständige nationale Behörde und in bestimmten Fällen auch die von Verletzungen des Schutzes personenbezogener Daten betroffenen Teilnehmer und Personen zu benachrichtigen. Verletzungen des Schutzes personenbezogener Daten werden in Artikel 2 Buchstabe i der Richtlinie 2002/58/EG definiert als Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Union verarbeitet werden.

(3) Zur Gewährleistung einer einheitlichen Anwendung der in Artikel 4 Absätze 2, 3 und 4 der Richtlinie 2002/58/EG vorgesehenen Maßnahmen wird die Kommission durch Artikel 4 Absatz 5 derselben Richtlinie ermächtigt, technische Durchführungsmaßnahmen in Bezug auf die Umstände, Form und Verfahren der in dem genannten Artikel vorgeschriebenen Informationen und Benachrichtigungen zu erlassen.

(4) Unterschiedliche nationale Anforderungen in dieser Hinsicht können zu rechtlicher Unsicherheit, komplizierteren und umständlicheren Verfahren und erheblichen Verwaltungskosten für grenzübergreifend tätige Betreiber führen. Die Kommission hält es daher für notwendig, solche technischen Durchführungsmaßnahmen zu erlassen.

(5) Diese Verordnung betrifft nur die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten und enthält daher keine technischen Durchführungsmaßnahmen im Hinblick auf Artikel 4 Absatz 2 der Richtlinie 2002/58/EG bezüglich der Aufklärung der Teilnehmer über ein besonderes Risiko der Verletzung der Netzsicherheit.

(6) Wie sich aus Artikel 4 Absatz 3 erster Unterabsatz der Richtlinie 2002/58/EG ergibt, sollten die Betreiber die zuständige nationale Behörde von allen Verletzungen des Schutzes personenbezogener Daten benachrichtigen. Folglich sollte es nicht im Ermessen des Betreibers liegen, ob er die zuständige nationale Behörde benachrichtigt oder nicht. Dies sollte die betreffende zuständige nationale Behörde jedoch nicht daran hindern, der Untersuchung bestimmter Verletzungen in der Weise, die sie nach geltendem Recht für geeignet hält, Vorrang einzuräumen und erforderliche Schritte zu unternehmen, um eine überzogene oder unzureichende Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten zu verhindern.

(7) Es ist angemessen, für die Benachrichtigung der zuständigen nationalen Behörde ein System vorzusehen, das unter bestimmten Voraussetzungen mehrere Stufen umfasst, für die jeweils bestimmte Fristen gelten. Dieses System soll sicherstellen, dass die zuständige nationale Behörde so früh und so vollständig wie möglich informiert wird, ohne den Betreiber bei der Untersuchung der Verletzung und der Ergreifung der Maßnahmen zu behindern, die zur Eindämmung und Beseitigung der Folgen der Verletzung nötig sind.

([1]) ABl. L 201 vom 31.7.2002, S. 37.
([2]) ABl. L 281 vom 23.11.1995, S. 31.

(8) Weder ein bloßer Verdacht, dass eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, noch die bloße Feststellung eines Vorfalls, über den trotz größtmöglicher Bemühungen des Betreibers keine ausreichenden Informationen vorliegen, sollten ausreichen, um geltend zu machen, dass eine Verletzung des Schutzes personenbezogener Daten im Sinne dieser Verordnung festgestellt worden ist. Von besonderer Bedeutung ist in diesem Zusammenhang das Vorliegen der in Anhang I aufgeführten Informationen.

(9) Im Zuge der Durchführung dieser Verordnung sollten die zuständigen nationalen Behörden in Fällen grenzübergreifender Verletzungen des Schutzes personenbezogener Daten zusammenarbeiten.

(10) Diese Verordnung enthält keine zusätzlichen Vorgaben für das von den Betreibern zu führende Verzeichnis der Verletzungen des Schutzes personenbezogener Daten, da dessen Inhalt durch Artikel 4 der Richtlinie 2002/58/EG bereits umfassend geregelt wird. Die Betreiber können sich aber bei der Festlegung des Verzeichnisformats auf diese Verordnung stützen.

(11) Alle zuständigen nationalen Behörden sollten gesicherte elektronische Mittel bereitstellen, damit die Betreiber Verletzungen des Schutzes personenbezogener Daten in einem einheitlichen Format melden können, das auf einem Standard wie XML beruht und die in Anhang I aufgeführten Informationen in den betreffenden Sprachen enthält, damit alle Betreiber in der Union ein ähnliches Benachrichtigungsverfahren verwenden können, unabhängig davon, wo sie sich befinden oder wo die Verletzung des Schutzes personenbezogener Daten stattgefunden hat. In diesem Zusammenhang sollte die Kommission die Einrichtung der gesicherten elektronischen Mittel dadurch erleichtern, dass sie — falls nötig — Sitzungen mit den zuständigen nationalen Behörden einberuft.

(12) Bei der Beurteilung, ob sich eine Verletzung des Schutzes personenbezogener Daten wahrscheinlich nachteilig auf die personenbezogenen Daten oder die Privatsphäre eines Teilnehmers oder einer Person auswirken wird, sollten vor allem Art und Inhalt der personenbezogenen Daten berücksichtigt werden; dies gilt insbesondere für Daten, die finanzielle Informationen wie Kreditkartendaten oder Einzelheiten über Bankkonten enthalten, für besondere Datenkategorien, die in Artikel 8 Absatz 1 der Richtlinie 95/46/EG genannt werden, sowie für bestimmte Daten im besonderen Zusammenhang mit der Erbringung von Telefon- und Internetdienstleistungen, z. B. E-Mail-Daten, Standortdaten, Internet-Protokolldateien, Webbrowser-Verläufe und Aufstellungen von Einzelverbindungen.

(13) Unter außergewöhnlichen Umständen sollte es dem Betreiber gestattet werden, die Benachrichtigung des Teilnehmers oder der Person aufzuschieben, falls durch die Benachrichtigung des Teilnehmers oder der Person die ordnungsgemäße Untersuchung der Verletzung des Schutzes personenbezogener Daten gefährdet würde. Außergewöhnliche Umstände wären in diesem Zusammenhang beispielsweise strafrechtliche Ermittlungen wie auch andere Verletzungen des Schutzes personenbezogener Daten, die zwar keine schwere Straftat darstellen, aber ein Aufschieben der Benachrichtigung dennoch als angemessen erscheinen lassen. Auf jeden Fall sollte die zuständige Behörde im Einzelfall unter Berücksichtigung der gegebenen Umstände beurteilen, ob sie der Aufschiebung zustimmt oder eine Benachrichtigung verlangt.

(14) Die Betreiber sollten zwar aufgrund ihrer direkten vertraglichen Beziehung im Besitz der Kontaktangaben ihrer Teilnehmer sein, verfügen aber möglicherweise über keine derartigen Angaben zu anderen Personen, auf die sich eine Verletzung des Schutzes personenbezogener Daten nachteilig auswirken könnte. In solchen Fällen sollte es den Betreibern gestattet sein, derartige Personen zunächst durch Bekanntmachungen in großen nationalen oder regionalen Medien, z. B. in Zeitungen, zu benachrichtigen und anschließend so bald wie möglich eine individuelle Benachrichtigung entsprechend dieser Verordnung nachzuholen. Der Betreiber ist daher an sich nicht zur Bekanntmachung in den Medien verpflichtet, sondern ist hierzu — falls er dies wünscht — berechtigt, solange er noch alle betroffenen Personen ermittelt.

(15) Die Informationen über die Verletzung sollten sich ausschließlich auf die Verletzung beziehen und nicht mit Informationen zu anderen Themen verbunden werden. Beispielsweise sollten Informationen über eine Verletzung des Schutzes personenbezogener Daten, die in einer regulären Rechnung erscheinen, nicht als geeignetes Mittel zur Benachrichtigung über eine Verletzung personenbezogener Daten angesehen werden.

(16) In dieser Verordnung werden keine bestimmten technischen Schutzmaßnahmen vorgeschrieben, die eine Ausnahme von der Pflicht zur Benachrichtigung der Teilnehmer oder Personen von Verletzungen des Schutzes personenbezogener Daten rechtfertigen könnten, weil sich diese mit dem technischen Fortschritt ändern können. Dennoch sollte die Kommission in der Lage sein, entsprechend der aktuellen Praxis eine Aufstellung solcher spezifischen technischen Schutzmaßnahmen zu veröffentlichen.

(17) Allein die Anwendung von Verschlüsselung oder Streuspeicherung (Hashing) sollte nicht als ausreichend dafür angesehen werden, dass Betreiber pauschal behaupten können, sie erfüllten die allgemeine Schutzpflicht gemäß Artikel 17 der Richtlinie 95/46/EG. In dieser Hinsicht sollten die Betreiber auch geeignete organisatorische und technische Vorkehrungen treffen, um Verletzungen des Schutzes personenbezogener Daten vorzubeugen bzw. diese festzustellen und zu blockieren. Die Betreiber sollten auch ein verbleibendes Restrisiko betrachten, das nach der Umsetzung von Kontrollen noch fortbestehen könnte, um zu verstehen, wo Verletzungen des Schutzes personenbezogener Daten möglicherweise auftreten könnten.

(18) Wenn der Betreiber einen Teil der Dienstleistung, z. B. in Bezug auf Abrechnungs- oder Verwaltungsfunktionen, von einem anderen Betreiber ausführen lässt, so sollte der andere Betreiber, der in keinem direkten Vertragsverhältnis zum Endkunden steht, nicht verpflichtet sein, im Falle einer Verletzung des Schutzes personenbezogener

Daten selbst Benachrichtigungen vorzunehmen. Stattdessen sollte der Dritte den Betreiber, mit dem er in einer direkten Vertragsbeziehung steht, warnen und informieren. Dies gilt auch im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste auf der Vorleistungsebene, wo der Vorleister üblicherweise in keinem direkten Vertragsverhältnis zum Endkunden steht.

(19) Durch die Richtlinie 95/46/EG wird ein allgemeiner Rahmen für den Schutz personenbezogener Daten in der Europäischen Union festgelegt. Die Kommission hat einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Ersetzung der Richtlinie 95/46/EG („Datenschutzverordnung") vorgelegt. Die vorgeschlagene Datenschutzverordnung würde, aufbauend auf Artikel 4 Absatz 3 der Richtlinie 2002/58/EG, für alle für die Verarbeitung Verantwortlichen eine Verpflichtung einführen, Verletzungen des Schutzes personenbezogener Daten zu melden. Die vorliegende Verordnung der Kommission steht mit diesem Vorschlag in vollem Einklang.

(20) Die vorgeschlagene Datenschutzverordnung enthält auch eine begrenzte Anzahl technischer Anpassungen der Richtlinie 2002/58/EG, die der Umwandlung der Richtlinie 95/46/EG in eine Verordnung Rechnung tragen. Die materiellen rechtlichen Folgen, die sich für die Richtlinie 2002/58/EG aus der neuen Verordnung ergeben, werden Gegenstand einer Überprüfung durch die Kommission sein.

(21) Die Durchführung dieser Verordnung sollte alle drei Jahre ab ihrem Inkrafttreten überprüft werden; gleichzeitig sollte der Inhalt dieser Verordnung im Lichte des dann geltenden Rechtsrahmens, einschließlich der vorgeschlagenen Datenschutzverordnung, überprüft werden. Die Überprüfung dieser Verordnung sollte — soweit möglich — mit etwaigen künftigen Überprüfungen der Richtlinie 2002/58/EG verknüpft werden.

(22) Die Durchführung dieser Verordnung kann u. a. auf der Grundlage der von den zuständigen nationalen Behörden geführten Statistiken über die ihnen gemeldeten Verletzungen des Schutzes personenbezogener Daten bewertet werden. Diese Statistiken können beispielsweise Angaben darüber enthalten, wieviele Verletzungen des Schutzes personenbezogener Daten den zuständigen nationalen Behörden gemeldet wurden, von wievielen Verletzungen des Schutzes personenbezogener Daten die betroffenen Teilnehmer oder Personen benachrichtigt wurden, wieviel Zeit zur Behebung der Verletzung des Schutzes personenbezogener Daten benötigt wurde und ob technische Schutzmaßnahmen getroffen wurden. Diese Statistiken sollen der Kommission und den Mitgliedstaaten kohärente und vergleichbare statistische Daten liefern und weder die Identität der meldenden Betreiber noch die Identität betroffener Teilnehmer oder Personen offenlegen. Die Kommission kann zu diesem Zweck regelmäßige Sitzungen mit zuständigen nationalen Behörden und anderen interessierten Beteiligten abhalten.

(23) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des Kommunikationsausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Geltungsbereich

Diese Verordnung gilt für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten durch Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste („Betreiber").

Artikel 2

Benachrichtigung der zuständigen nationalen Behörde

(1) Der Betreiber benachrichtigt die zuständige nationale Behörde von allen Verletzungen des Schutzes personenbezogener Daten.

(2) Der Betreiber benachrichtigt die zuständige nationale Behörde von der Verletzung des Schutzes personenbezogener Daten binnen 24 Stunden nach Feststellung der Verletzung, soweit dies möglich ist.

In seiner Benachrichtigung der zuständigen nationalen Behörde macht der Betreiber die in Anhang I aufgeführten Angaben.

Eine Verletzung des Schutzes personenbezogener Daten gilt als festgestellt, sobald der Betreiber vom Auftreten einer Sicherheitsverletzung, die zu einer Verletzung des Schutzes personenbezogener Daten geführt hat, hinreichende Kenntnis insoweit erlangt hat, dass er eine sinnvolle Benachrichtigung nach den Vorschriften dieser Verordnung vornehmen kann.

(3) Falls nicht alle in Anhang I aufgeführten Angaben vorliegen und eine weitere Untersuchung der Verletzung des Schutzes personenbezogener Daten erforderlich ist, kann der Betreiber zunächst binnen 24 Stunden nach Feststellung der Verletzung eine Erstbenachrichtigung der zuständigen nationalen Behörde vornehmen. Diese Erstbenachrichtigung der zuständigen nationalen Behörde muss die in Anhang I Abschnitt 1 aufgeführten Angaben enthalten. Anschließend nimmt der Betreiber so bald wie möglich, spätestens aber binnen drei Tagen nach der Erstbenachrichtigung, eine zweite Benachrichtigung der zuständigen nationalen Behörde vor. Diese zweite Benachrichtigung muss die in Anhang I Abschnitt 2 aufgeführten Angaben enthalten und die bereits zuvor gemachten Angaben gegebenenfalls aktualisieren.

Ist der Betreiber trotz seiner Nachforschungen nicht in der Lage, alle diese Angaben binnen drei Tagen nach der Erstbenachrichtigung zu machen, übermittelt er der zuständigen nationalen Behörde alle Angaben, die ihm innerhalb des genannten Zeitraums vorliegen, und eine Begründung für die verspätete Mitteilung der verbleibenden Angaben. Der Betreiber muss der zuständigen nationalen Behörde so bald wie möglich die verbleibenden Angaben mitteilen und die bereits zuvor gemachten Angaben aktualisieren.

(4) Die zuständige nationale Behörde stellt allen Betreibern, die in dem betreffenden Mitgliedstaat niedergelassen sind, gesicherte elektronische Mittel für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten sowie Informationen über die Verfahren für den Zugang hierzu und für deren Benutzung zur Verfügung. Falls notwendig beruft die Kommission Sitzungen mit den zuständigen nationalen Behörden ein, um die Durchführung dieser Verordnung zu erleichtern.

(5) Betrifft die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder Personen aus anderen Mitgliedstaaten als dem der von der Verletzung benachrichtigten zuständigen nationalen Behörde, so unterrichtet die zuständige nationale Behörde die anderen betroffenen nationalen Behörden.

Um die Anwendung dieser Bestimmung zu erleichtern, erstellt und führt die Kommission eine Liste der zuständigen nationalen Behörden und der jeweiligen Ansprechpartner.

Artikel 3

Benachrichtigung der Teilnehmer oder Personen

(1) Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten die personenbezogenen Daten eines Teilnehmers oder einer Person oder deren Privatsphäre beeinträchtigt werden, so benachrichtigt der Betreiber zusätzlich zu der Benachrichtigung gemäß Artikel 2 auch den Teilnehmer bzw. die Person von der Verletzung.

(2) Ob eine Verletzung des Schutzes personenbezogener Daten wahrscheinlich die personenbezogenen Daten oder die Privatsphäre eines Teilnehmers oder einer Person beeinträchtigt, wird insbesondere unter Berücksichtigung folgender Umstände beurteilt:

a) Art und Inhalt der betroffenen personenbezogenen Daten, insbesondere wenn diese finanzielle Informationen, besondere Datenkategorien gemäß Artikel 8 Absatz 1 der Richtlinie 95/46/EG sowie Standortdaten, Internet-Protokolldateien, Webbrowser-Verläufe, E-Mail-Daten und Aufstellungen von Einzelverbindungen betreffen;

b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten für den betroffenen Teilnehmer oder die betroffene Person, insbesondere wenn die Verletzung einen Identitätsdiebstahl oder Betrug, eine physische Schädigung, ein psychisches Leid, eine Demütigung oder Rufschädigung zur Folge haben könnte;

c) die Umstände der Verletzung des Schutzes personenbezogener Daten, insbesondere wenn die Daten gestohlen wurden oder wenn der Betreiber weiß, dass die Daten im Besitz eines unbefugten Dritten sind.

(3) Die Benachrichtigung des Teilnehmers oder der Person muss ohne unangemessene Verzögerung nach Feststellung der Verletzung des Schutzes personenbezogener Daten gemäß Artikel 2 Absatz 2 dritter Unterabsatz erfolgen. Sie erfolgt unabhängig von der Meldung der Verletzung des Schutzes personenbezogener Daten bei der zuständigen nationalen Behörde gemäß Artikel 2.

(4) In seiner Benachrichtigung des Teilnehmers oder der Person macht der Betreiber die in Anhang II genannten Angaben. Die Benachrichtigung des Teilnehmers oder der Person muss in einer sprachlich klaren und leicht verständlichen Weise erfolgen. Der Betreiber darf die Benachrichtigung nicht als Gelegenheit zur Verkaufsförderung oder Werbung für neue oder zusätzliche Dienste nutzen.

(5) 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 aufschieben, bis die zuständige nationale Behörde eine Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten gemäß diesem Artikel für möglich hält.

(6) Der Betreiber benachrichtigt den Teilnehmer oder die Person von der Verletzung des Schutzes personenbezogener Daten mit Hilfe von Kommunikationsmitteln, die einen zügigen Empfang der Informationen gewährleisten und nach dem Stand der Technik angemessen gesichert sind. Die Informationen über die Verletzung müssen sich ausschließlich auf die Verletzung beziehen und dürfen nicht mit Informationen zu anderen Themen verbunden werden.

(7) Kann der Betreiber, der in einem direkten Vertragsverhältnis zum Endnutzer steht, 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 wahrscheinlich beeinträchtigt werden, so kann er diese Personen durch Bekanntmachungen in großen nationalen oder regionalen Medien der betreffenden Mitgliedstaaten innerhalb dieser Frist benachrichtigen. Diese Bekanntmachungen müssen die in Anhang II aufgeführten Angaben erhalten, falls nötig in gekürzter Form. In diesem Fall muss der Betreiber weiterhin alle zumutbaren Anstrengungen unternehmen, um diese Personen zu ermitteln und sie so bald wie möglich mit den in Anhang II aufgeführten Angaben zu benachrichtigen.

Artikel 4

Technische Schutzmaßnahmen

(1) Abweichend von Artikel 3 Absatz 1 braucht der Betreiber die betroffenen Teilnehmer oder Personen nicht von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn er zur Zufriedenheit der zuständigen nationalen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Durch diese technischen Schutzmaßnahmen müssen die Daten für alle Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht 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

b) 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.

(3) Die Kommission kann nach Anhörung der zuständigen nationalen Behörden über die Artikel-29-Datenschutzgruppe, der Europäischen Agentur für Netz- und Informationssicherheit und des Europäischen Datenschutzbeauftragten entsprechend der aktuellen Praxis eine vorläufige Aufstellung geeigneter technischer Schutzmaßnahmen gemäß Absatz 1 veröffentlichen.

Artikel 5

Erbringung von Leistungen durch einen anderen Betreiber

Wird ein anderer Betreiber, der in keinem direkten Vertragsverhältnis zu den Teilnehmern steht, mit der Erbringung eines Teils des elektronischen Kommunikationsdienstes beauftragt, muss dieser andere Betreiber im Falle einer Verletzung des Schutzes personenbezogener Daten den beauftragenden Betreiber sofort informieren.

Artikel 6

Berichterstattung und Überprüfung

Innerhalb von drei Jahren nach dem Inkrafttreten dieser Verordnung legt die Kommission einen Bericht über die Durchführung dieser Verordnung, ihre Wirksamkeit und ihre Auswirkungen auf Betreiber, Teilnehmer und Personen vor. Auf der Grundlage dieses Berichts nimmt die Kommission eine Überprüfung dieser Verordnung vor.

Artikel 7

Inkrafttreten

Diese Verordnung tritt am 25. August 2013 in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 24. Juni 2013

Für die Kommission
Der Präsident
José Manuel BARROSO

ANHANG I

Inhalt der Benachrichtigung der zuständigen nationalen Behörde

Abschnitt 1

Angaben zum Betreiber

1. Name des Betreibers
2. Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen
3. Angabe, ob es sich um eine erste oder zweite Benachrichtigung handelt

Erstinformation über die Verletzung des Schutzes personenbezogener Daten (ggf. in späteren Benachrichtigungen zu ergänzen)

4. Datum und Zeitpunkt des Vorfalls (falls bekannt, kann nötigenfalls geschätzt werden) und der Feststellung des Vorfalls
5. Umstände der Verletzung des Schutzes personenbezogener Daten (z. B. Verlust, Diebstahl, Vervielfältigung)
6. Art und Inhalt der betroffenen personenbezogenen Daten
7. Technische und organisatorische Maßnahmen, die der Betreiber in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat (oder ergreifen wird)
8. Erbringung relevanter Leistungen durch einen anderen Betreiber (falls zutreffend)

Abschnitt 2

Weitere Informationen über die Verletzung des Schutzes personenbezogener Daten

9. Zusammenfassung des Vorfalls, der die Verletzung des Schutzes personenbezogener Daten verursacht hat (mit Angabe des physischen Orts der Verletzung und der betroffenen Datenträger)
10. Anzahl der betroffenen Teilnehmer oder Personen
11. Mögliche Folgen und mögliche nachteilige Auswirkungen auf Teilnehmer oder Personen
12. Technische und organisatorische Maßnahmen, die der Betreiber zur Minderung möglicher nachteiliger Auswirkungen ergriffen hat

Mögliche zusätzliche Benachrichtigung der Teilnehmer oder Personen

13. Inhalt der Benachrichtigung
14. Verwendete Kommunikationsmittel
15. Anzahl der benachrichtigten Teilnehmer oder Personen

Mögliche grenzübergreifende Fragen

16. Verletzung des Schutzes personenbezogener Daten, die Teilnehmer oder Personen in anderen Mitgliedstaaten betrifft
17. Benachrichtigung anderer zuständiger nationaler Behörden.

ANHANG II

Inhalt der Benachrichtigung der Teilnehmer oder der Personen

1. Name des Betreibers

2. Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen

3. Zusammenfassung des Vorfalls, der zu der Verletzung des Schutzes personenbezogener Daten geführt hat

4. Vermutetes Datum des Vorfalls

5. Art und Inhalt der betroffenen personenbezogenen Daten entsprechend Artikel 3 Absatz 2

6. Wahrscheinliche Folgen der Verletzung des Schutzes personenbezogener Daten für den betroffenen Teilnehmer oder die betroffene Person entsprechend Artikel 3 Absatz 2

7. Umstände der Verletzung des Schutzes personenbezogener Daten entsprechend Artikel 3 Absatz 2

8. Vom Betreiber ergriffene Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

9. Vom Betreiber empfohlene Maßnahmen zur Minderung etwaiger nachteiliger Auswirkungen.