REGLAMENTOS

REGLAMENTO (UE) Nº 611/2013 DE LA COMISIÓN

de 24 de junio de 2013

relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) ([1]), y, en particular, su artículo 4, apartado 5,

Previa consulta a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA),

Previa consulta al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ([2]) (denominado en lo sucesivo «Grupo del artículo 29»),

Previa consulta al Supervisor Europeo de Protección de Datos (SEPD),

Considerando lo siguiente:

(1) La Directiva 2002/58/CE prevé la armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Unión.

(2) En virtud del artículo 4 de la Directiva 2002/58/CE, los proveedores de servicios de comunicaciones electrónicas disponibles para el público están obligados a notificar las violaciones de datos personales a las autoridades nacionales competentes y, en algunos casos, también a los abonados y particulares afectados. Según la definición del artículo 2, letra i), de la Directiva 2002/58/CE, se considera violación de los datos personales toda violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Unión.

(3) A fin de garantizar una aplicación coherente de las medidas contempladas en el artículo 4, apartados 2, 3 y 4, de la Directiva 2002/58/CE, el artículo 4, apartado 5, de dicha Directiva confiere a la Comisión competencias para adoptar medidas técnicas de ejecución en relación con las circunstancias, la forma de presentación y los procedimientos aplicables a los requisitos de información y notificación a que se refiere el citado artículo.

(4) La aplicación de distintos requisitos nacionales en este ámbito puede entrañar inseguridad jurídica, procedimientos más complejos y farragosos, así como considerables gastos administrativos para los proveedores que desarrollan actividades transfronterizas. Por lo tanto, la Comisión considera necesario adoptar dichas medidas técnicas de ejecución.

(5) El presente Reglamento se limita a la notificación de los casos de violación de datos personales y, por consiguiente, no establece medidas técnicas de ejecución en relación con el artículo 4, apartado 2, de la Directiva 2002/58/CE, relativo a la información que ha de darse a los abonados en caso de que exista un riesgo particular de violación de la seguridad de la red.

(6) De conformidad con el artículo 4, apartado 3, párrafo primero, de la Directiva 2002/58/CE, los proveedores deben notificar a la autoridad nacional competente todos los casos de violación de datos personales. Por consiguiente, la decisión de efectuar la correspondiente notificación a la autoridad nacional competente o no hacerlo no debe dejarse a discreción del proveedor. No obstante, ello no ha de impedir que la autoridad nacional competente conceda prioridad a la investigación de determinados casos del modo que considere adecuado conforme a la legislación aplicable y adopte las medidas necesarias para evitar la notificación excesiva o insuficiente de violaciones de datos personales.

(7) Es oportuno establecer un sistema para la notificación de los casos de violación de datos personales a la autoridad nacional competente que consista, cuando se cumplan determinadas condiciones, en varias etapas sujetas a ciertos plazos. Este sistema tiene como objetivo garantizar que la autoridad nacional competente sea informada de la forma más rápida y exhaustiva posible, sin que ello entorpezca indebidamente los esfuerzos del proveedor por investigar el caso y tomar las medidas necesarias para limitarlo y remediar sus consecuencias.

([1]) DO L 201 de 31.7.2002, p. 37.
([2]) DO L 281 de 23.11.1995, p. 31.

(8) Para considerar que se ha detectado un caso de violación de datos personales a los efectos del presente Reglamento, no debe bastar meramente con sospechar que se ha producido un caso de este tipo ni con detectar un incidente de seguridad sin disponer de suficiente información al respecto, pese a todos los esfuerzos del proveedor a tal fin. En este contexto, se debe prestar especial atención a la disponibilidad de la información a que se hace referencia en el anexo I.

(9) En el marco de la aplicación del presente Reglamento, es conveniente que las autoridades nacionales competentes cooperen en los casos de violación de datos personales que tengan una dimensión transfronteriza.

(10) El presente Reglamento no prevé especificaciones adicionales con respecto al inventario de violaciones de datos personales que los proveedores deben llevar, por cuanto el artículo 4 de la Directiva 2002/58/CE ya detalla su contenido exhaustivamente. Con todo, los proveedores pueden remitirse al presente Reglamento para determinar el formato del inventario.

(11) Es necesario que todas las autoridades nacionales competentes pongan un soporte electrónico seguro a disposición de los proveedores para que estos notifiquen los casos de violación de datos personales en un formato común, basado en normas tales como la XML, que contenga la información establecida en el anexo I en las lenguas pertinentes, de modo que todos los proveedores de la Unión puedan seguir un procedimiento de notificación similar, independientemente del lugar en que estén ubicados o en que se haya producido la violación de datos personales. A este respecto, la Comisión ha de facilitar la implantación de un soporte electrónico seguro organizando, cuando sea necesario, reuniones con las autoridades nacionales competentes.

(12) Para evaluar si una violación de datos personales puede tener efectos negativos en los datos personales o la intimidad de un abonado o particular, han de tomarse especialmente en consideración la naturaleza y el contenido de los datos personales en cuestión, en particular cuando se trate de datos financieros como los referentes a tarjetas de crédito y cuentas bancarias; de las categorías especiales de datos contempladas en el artículo 8, apartado 1, de la Directiva 95/46/CE; y de determinados datos específicamente vinculados a la prestación de servicios de telefonía o internet como, por ejemplo, datos de correo electrónico, datos de localización, registros de internet, historiales de navegación en internet y listas de llamadas detalladas.

(13) En circunstancias excepcionales, es conveniente autorizar al proveedor a demorar la notificación al abonado o al particular cuando dicha notificación pueda comprometer la investigación adecuada del caso de violación de datos personales. En este contexto, pueden considerarse circunstancias excepcionales las investigaciones judiciales, así como otros casos de violación de datos personales que no constituyen un delito grave, pero respecto de los que podría ser conveniente retrasar la notificación. En cualquier caso, ha de corresponder a la autoridad nacional competente evaluar, caso por caso y en función de las circunstancias, si procede autorizar ese retraso o exigir que se efectúe la notificación.

(14) Los proveedores deberían disponer de los datos de contacto de sus abonados, habida cuenta de su relación contractual directa, pero es posible que no exista esta información en el caso de otros particulares que se hayan visto perjudicados por una violación de datos personales. En tal caso, conviene autorizar a los proveedores a efectuar una notificación inicial a dichos particulares mediante anuncios en los principales medios de comunicación nacionales o regionales, tales como los periódicos, que irá seguida lo antes posible de una notificación individual de conformidad con el presente Reglamento. Por consiguiente, el proveedor no está obligado como tal a efectuar notificaciones en los medios de comunicación, sino que más bien está facultado para hacerlo, si así lo desea, cuando aún está tratando de identificar a todos los particulares afectados.

(15) La información sobre la violación debe referirse exclusivamente a esta y no adjuntarse a información sobre otros asuntos. Por ejemplo, incluir información sobre una violación de datos personales en una factura corriente no ha de considerarse un medio adecuado para notificar una violación de datos personales.

(16) El presente Reglamento no establece medidas tecnológicas específicas de protección que justifiquen excepciones a la obligación de notificar los casos de violación de datos personales a abonados o particulares, por cuanto dichas medidas pueden evolucionar con el tiempo en función de los avances tecnológicos. Con todo, la Comisión ha de poder publicar una lista indicativa de esas medidas tecnológicas específicas de protección acordes con las prácticas actuales.

(17) El recurso al cifrado o a las funciones resumen *(hashing)* no ha de considerarse suficiente por sí mismo como para que los proveedores puedan aducir, de forma más amplia, que han cumplido la obligación de seguridad general establecida en el artículo 17 de la Directiva 95/46/CE. A este respecto, es importante que los proveedores apliquen también medidas técnicas y de organización para prevenir, detectar y bloquear los casos de violación de datos personales. Los proveedores deben tener en cuenta cualquier riesgo residual que pueda subsistir tras haberse practicado controles, al objeto de comprender en qué circunstancias puede producirse una violación de datos personales.

(18) Cuando el proveedor recurra a otro proveedor para prestar una parte del servicio, por ejemplo en relación con la facturación o funciones de gestión, ese otro proveedor, que no mantiene relación contractual directa alguna con

el usuario final, no ha de estar obligado a efectuar notificaciones en caso de violación de datos personales. En cambio, sí debe avisar e informar al proveedor con el que tiene una relación contractual directa. Ello ha de ser también aplicable en el contexto de la prestación al por mayor de servicios de comunicaciones electrónicas, ámbito en el que el proveedor mayorista no suele tener una relación contractual directa con el usuario final.

(19) La Directiva 95/46/CE establece un marco general para la protección de los datos personales en la Unión Europea. La Comisión ha presentado una propuesta de Reglamento del Parlamento Europeo y del Consejo para sustituir la Directiva 95/46/CE (Reglamento sobre protección de datos). El Reglamento sobre protección de datos que se propone impone a todos los responsables del tratamiento de datos la obligación de notificar las violaciones de datos personales, sobre la base del artículo 4, apartado 3, de la Directiva 2002/58/CE. El presente Reglamento de la Comisión es plenamente coherente con la medida propuesta.

(20) El Reglamento sobre protección de datos propuesto también introduce un número limitado de modificaciones de carácter técnico en la Directiva 2002/58/CE, habida cuenta de la transformación de la Directiva 95/46/CE en un Reglamento. Las consecuencias legales sustantivas del nuevo Reglamento para la Directiva 2002/58/CE serán objeto de un examen por parte de la Comisión.

(21) La aplicación del presente Reglamento debe revisarse a los tres años de su entrada en vigor, y su contenido ha de examinarse a la luz del marco jurídico vigente en ese momento, incluido el Reglamento sobre protección de datos propuesto. La revisión del presente Reglamento ha de vincularse, cuando sea posible, a cualquier futura revisión de la Directiva 2002/58/CE.

(22) La aplicación del presente Reglamento puede evaluarse sobre la base, entre otros datos, de las estadísticas elaboradas por las autoridades nacionales competentes sobre los casos de violación de datos personales que se les notifiquen. Dichas estadísticas pueden incluir, por ejemplo, información sobre el número de casos de violación de datos personales notificados a la autoridad nacional competente, a los abonados o a los particulares, el tiempo que se haya tardado en resolver el caso, y las medidas tecnológicas de protección que, en su caso, se hayan adoptado. Estas estadísticas deben proporcionar a la Comisión y a los Estados miembros datos estadísticos coherentes y comparables, sin divulgar la identidad del proveedor que haya efectuado la notificación ni la de los abonados o particulares afectados. Asimismo, la Comisión puede celebrar reuniones periódicas a tal fin con las autoridades nacionales competentes y otras partes interesadas.

(23) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité de Comunicaciones.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Ámbito de aplicación

El presente Reglamento se aplicará a la notificación de los casos de violación de datos personales por parte de los proveedores de servicios de comunicaciones electrónicas disponibles para el público (denominados en lo sucesivo «los proveedores»).

Artículo 2

Notificación a la autoridad nacional competente

1. Los proveedores notificarán todos los casos de violación de datos personales a la autoridad nacional competente.

2. En la medida de lo posible, los proveedores notificarán los casos de violación de datos personales a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso.

Los proveedores consignarán en su notificación a la autoridad nacional competente la información recogida en el anexo I.

Se considerará que se ha detectado un caso de violación de datos personales cuando el proveedor tenga conocimiento suficiente de que se ha producido un incidente de seguridad que compromete datos personales para efectuar una notificación válida conforme a lo establecido en el presente Reglamento.

3. Cuando no se disponga de toda la información indicada en el anexo I y sea preciso investigar más exhaustivamente el caso de violación de datos personales, se autorizará al proveedor a enviar una notificación inicial a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso. Esta notificación inicial incluirá la información contemplada en el anexo I, sección 1. El proveedor remitirá una segunda notificación a la autoridad nacional competente lo antes posible y, a más tardar, dentro de los tres días siguientes a la notificación inicial. En esta segunda notificación se incluirá la información indicada en el anexo I, sección 2, y, cuando proceda, se actualizará la información ya proporcionada.

Cuando, a pesar de las pesquisas realizadas, el proveedor no pueda proporcionar toda la información en el plazo de los tres días siguientes a la notificación inicial, deberá notificar toda la información de que disponga dentro de ese plazo y presentar a la autoridad nacional competente una justificación motivada de la tardía notificación de la información restante. El proveedor notificará esa información restante a la autoridad nacional competente y, cuando proceda, actualizará la información ya proporcionada, en el plazo más breve posible.

4. La autoridad nacional competente pondrá a disposición de todos los proveedores establecidos en el Estado miembro de que se trate un soporte electrónico seguro para notificar los casos de violación de datos personales, así como información sobre los procedimientos para acceder a dicho soporte y utilizarlo. Cuando sea necesario, la Comisión convocará reuniones con las autoridades nacionales competentes a fin de facilitar la aplicación de esta disposición.

5. Cuando una violación de datos personales afecte a abonados o particulares de Estados miembros distintos de aquel de la autoridad nacional competente a la que se haya notificado el caso de violación de datos personales, la autoridad nacional competente informará a las demás autoridades nacionales afectadas.

A fin de facilitar la aplicación de esta disposición, la Comisión elaborará y mantendrá al día una lista de las autoridades nacionales competentes y los puntos de contacto correspondientes.

Artículo 3

Notificación al abonado o particular

1. Cuando un caso de violación de datos personales pueda afectar negativamente a los datos personales o a la intimidad de un abonado o particular, el proveedor, además de remitir la notificación contemplada en el artículo 2, también notificará el caso al abonado o particular.

2. Se evaluará si un caso de violación de datos personales puede afectar negativamente a los datos personales o a la intimidad de un abonado o particular atendiendo, en particular, a las siguientes circunstancias:

a) la naturaleza y el contenido de los datos personales en cuestión, en particular si se trata de datos financieros, de categorías especiales de datos contempladas en el artículo 8, apartado 1, de la Directiva 95/46/CE, así como de datos de localización, registros de internet, historiales de navegación en internet, datos de correo electrónico y listas de llamadas detalladas;

b) las posibles consecuencias de la violación de datos personales para el abonado o particular afectado, en particular cuando la violación pueda entrañar fraude o usurpación de identidad, daños físicos, sufrimiento psicológico, humillación o perjuicio para su reputación;

c) las circunstancias en que se haya producido la violación de datos personales, teniendo en cuenta, en particular, el lugar en que hayan sido robados los datos o el momento en que el proveedor haya tenido conocimiento de que los datos se hallan en poder de un tercero no autorizado.

3. La notificación al abonado o particular se efectuará sin dilación injustificada tras haberse detectado la violación de datos personales, tal y como se establece en el artículo 2, apartado 2, párrafo tercero. Dicha notificación no dependerá de la notificación de la violación de datos personales a la autoridad nacional competente mencionada en el artículo 2.

4. El proveedor incluirá en su notificación al abonado o particular la información establecida en el anexo II. La notificación al abonado o particular se redactará en un lenguaje claro y fácilmente comprensible. El proveedor no deberá valerse de la notificación para promover o anunciar servicios nuevos o adicionales.

5. En circunstancias excepcionales, cuando la notificación al abonado o particular pueda comprometer la investigación del caso de violación de datos personales, el proveedor podrá, previa autorización de la autoridad nacional competente, demorar la notificación al abonado o particular hasta que la autoridad nacional competente considere que puede notificarse la violación de datos personales de conformidad con el presente artículo.

6. El proveedor notificará la violación de datos personales al abonado o particular por vías de comunicación que garanticen una pronta recepción de la información y sean seguras con arreglo al estado actual de la técnica. La información sobre el caso se referirá exclusivamente a este y no se adjuntará a información sobre otros asuntos.

7. Cuando, pese a haber hecho todo lo posible, el proveedor que tenga una relación contractual directa con el usuario final no pueda identificar en el plazo a que hace referencia el apartado 3 a todos los particulares que puedan verse perjudicados por la violación de datos personales, podrá notificarles esa información insertando anuncios en los principales medios de comunicación nacionales o regionales de los Estados miembros en cuestión dentro del citado plazo. Tales anuncios contendrán la información indicada en el anexo II, si procede de forma resumida. En este caso, el proveedor seguirá haciendo todo lo posible para identificar a dichos particulares y notificarles la información contemplada en el anexo II lo antes posible.

Artículo 4

Medidas tecnológicas de protección

1. No obstante lo dispuesto en el artículo 3, apartado 1, la notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la autoridad nacional competente que ha aplicado las medidas tecnológicas de protección convenientes y que estas se han aplicado a los datos afectados por la violación de seguridad. Las medidas de protección de estas características convertirán los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

2. Los datos se considerarán incomprensibles cuando:

a) se hayan cifrado de forma segura con un algoritmo normalizado, y la clave usada para descifrar los datos no haya quedado comprometida por ningún fallo de seguridad y haya sido generada de modo que no pueda ser determinada por los medios tecnológicos disponibles por ninguna persona que no esté autorizada a acceder a ella, o

b) se hayan sustituido por su valor resumen *(hash value)*, calculado mediante una función resumen con clave criptográfica normalizada, y la clave usada para resumir los datos no haya quedado comprometida por ningún fallo de seguridad y haya sido generada de modo que no pueda ser determinada por los medios tecnológicos disponibles por ninguna persona que no esté autorizada a acceder a ella.

3. Previa consulta a las autoridades nacionales competentes a través del Grupo del artículo 29, la Agencia Europea de Seguridad de las Redes y de la Información y al Supervisor Europeo de Protección de Datos, la Comisión podrá publicar una lista indicativa de las medidas tecnológicas de protección convenientes, contempladas en el apartado 1, acordes con las prácticas actuales.

Artículo 5

Recurso a otro proveedor

Cuando se contrate a otro proveedor para que preste una parte de un servicio de comunicaciones electrónicas sin tener una relación contractual directa con los abonados, ese otro proveedor informará inmediatamente al proveedor contratante en caso de violación de datos personales.

Artículo 6

Presentación de informes y revisión

En el plazo de los tres años siguientes a la entrada en vigor del presente Reglamento, la Comisión presentará un informe sobre su aplicación, eficacia y repercusión en proveedores, abonados y particulares. La Comisión revisará el presente Reglamento sobre la base de dicho informe.

Artículo 7

Entrada en vigor

El presente Reglamento entrará en vigor el 25 de agosto de 2013.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 24 de junio de 2013.

Por la Comisión
El Presidente
José Manuel BARROSO

ANEXO I

Contenido de la notificación a la autoridad nacional competente

Sección 1

Identificación del proveedor

1. Nombre del proveedor
2. Identidad y datos de contacto del responsable de la protección de datos u otro punto de contacto en el que pueda obtenerse más información
3. Indicación de si se trata de una primera o segunda notificación

Información inicial sobre el caso de violación de datos personales (en su caso, complétese en notificaciones posteriores)

4. Fecha y hora del incidente (si se conocen; en caso necesario, puede efectuarse una estimación) y de detección del incidente
5. Circunstancias en que se haya producido la violación de datos personales (por ejemplo, pérdida, robo, copia, etc.)
6. Naturaleza y contenido de los datos personales en cuestión
7. Medidas técnicas y de organización que ha aplicado (o aplicará) el proveedor a los datos personales en cuestión
8. Recurso a otros proveedores (cuando proceda)

Sección 2

Información suplementaria sobre el caso de violación de datos personales:

9. Resumen del incidente que ha causado la violación de datos personales (con indicación de la ubicación física de la violación y del soporte de almacenamiento)
10. Número de abonados o particulares afectados
11. Posibles consecuencias y efectos negativos en los abonados o particulares
12. Medidas técnicas y de organización que ha adoptado el proveedor para paliar los posibles efectos negativos

Posible notificación adicional a los abonados o particulares:

13. Contenido de la notificación
14. Medios de comunicación utilizados
15. Número de abonados o particulares a los que se ha remitido la notificación

Posibles cuestiones de carácter transfronterizo:

16. Caso de violación de datos personales que afecta a abonados o particulares de otros Estados miembros
17. Notificación a otras autoridades nacionales competentes

ANEXO II

Contenido de la notificación al abonado o particular

1. Nombre del proveedor

2. Identidad y datos de contacto del responsable de la protección de datos u otro punto de contacto en el que pueda obtenerse más información

3. Resumen del incidente que ha causado la violación de datos personales

4. Fecha estimada del incidente

5. Naturaleza y contenido de los datos personales en cuestión, con arreglo al artículo 3, apartado 2

6. Posibles consecuencias de la violación de datos personales para el abonado o particular afectado, con arreglo al artículo 3, apartado 2

7. Circunstancias en que se ha producido la violación de datos personales, con arreglo al artículo 3, apartado 2

8. Medidas adoptadas por el proveedor para subsanar la violación de datos personales

9. Medidas recomendadas por el proveedor para paliar los posibles efectos negativos.