25 de abril de 2017

5

SEGURIDAD DE LOS DATOS PERSONALES

Reglamento (UE) 2016/679

En este artículo vamos a analizar en detalle los diferentes aspectos relacionados con la seguridad de los datos personales que el nuevo Reglamento Europeo de Protección de Datos exigirá a partir de mayo de 2018.

Tanto la normativa actual vigente, esto es, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo, como el nuevo Reglamento Europeo de Protección de Datos, establecen la obligación de implementar medidas técnicas y organizativas para la salvaguarda de la información relativa a las personas.

En este sentido, el artículo 32 del nuevo Reglamento de Protección de Datos enumera de forma general, diferentes medidas que, entre otras, deberán ser tenidas en cuenta en el tratamiento de los datos de carácter personal:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La diferencia con la actual normativa es que ésta establece una serie de medidas concretas en función de la tipología de los datos. Con el nuevo Reglamento Europeo el responsable del tratamiento deberá barajar una serie de medidas que deberán aplicarse en función del *estado de la técnica, de los costes de aplicación, y de la naturaleza, el alcance, el contexto y los fines del tratamiento, así como de los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.*

Con el nuevo Reglamento, se deberá tener especialmente en cuenta los riesgos que presente el tratamiento de los datos, concretamente, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de los datos personales

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Notificación de una violación de la seguridad

El nuevo Reglamento establece la obligación de notificar a la autoridad de control cualquier violación de la seguridad de los datos personales. Esta notificación deberá realizarse dentro de las 72 horas siguientes a partir del momento en que se haya tenido constancia de ella. En caso de que la notificación no se presente en este plazo, ésta deberá incluir los motivos de tal dilación.

Asimismo, las notificaciones deberán contener al menos la siguiente información:

- la naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
- el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- las posibles consecuencias de la violación de la seguridad de los datos personales;
- las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Además, establece el Reglamento, el responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas de tal forma que la autoridad de control pueda verificar el cumplimiento de lo dispuesto por el Reglamento.

Por otro lado, en el caso en el que se considere que sea probable que la violación de la seguridad de los datos personales implique un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará inmediatamente a los interesados. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, incluyendo como mínimo el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; las posibles consecuencias de la violación de la seguridad de los datos personales; y las medidas adoptadas o propuestas por el responsable del tratamiento para poner

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Esta comunicación a los interesados no será necesaria si se cumple alguna de las condiciones establecidas por el Reglamento:

a) *el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;*
b) *el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1 (Artículo 34.1.);*
c) *suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.*

Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Por tanto, si con la actual normativa vigente, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se establece de forma detallada una serie de medidas aplicables en función del tipo de datos objeto del tratamiento, con el nuevo Reglamento Europeo de Protección de Datos los responsables del fichero y los encargados del tratamiento deberán establecer las medidas técnicas y organizativas necesarias para garantizar el nivel de seguridad adecuado según los riesgos identificados.

Todo ello implica que el responsable del fichero deberá tener en cuenta más variables, que las medidas de seguridad establecidas en el actual reglamento, identificando posibles riesgos y vulnerabilidades.

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

5

Evaluación de impacto relativa a la protección de datos

Otro aspecto novedoso del Reglamento Europeo de Protección de Datos es la *Evaluación del impacto*. El nuevo Reglamento establece lo siguiente:

> *Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.* (Art. 35.1)

Por tanto, el responsable deberá realizar antes de iniciar el tratamiento de los datos, un análisis del impacto de dicho tratamiento.

¿Cuándo deberemos realizar este análisis previo?

Según el Reglamento Europeo, a) cuando se realice una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) cuando se realice un tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1 del Reglamento (origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física), o de los datos personales relativos a condenas e infracciones penales, o c) observación sistemática a gran escala de una zona de acceso público.

Asimismo, la Autoridad de Control publicará una lista con los tipos de tratamiento que requieran o no requieran de una evaluación previa de impacto.

¿Qué deberá incluir el análisis previo?

> *a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;*

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1;

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Consulta previa

¿Qué ocurre si la evaluación previa indica que existe un alto riesgo para los derechos y libertades de las personas físicas?

En este caso, el responsable del tratamiento deberá realizar una *consulta* a la autoridad de control antes de iniciar el tratamiento.

En función de la información recabada, y si la autoridad de control entiende que puede llegar a haber una infracción del Reglamento, dicha autoridad deberá asesorar al responsable o al encargado, sin perjuicio de los poderes que el nuevo Reglamento le otorga, como por ejemplo, para investigar en relación al caso presentado en la consulta previa.

Conclusión

Con la entrada en vigor del nuevo Reglamento Europeo, el responsable del tratamiento deberá adoptar una postura proactiva ante la gestión y tratamiento de sus bases de datos. No será tan "sencillo" como hasta ahora, que veníamos aplicando las medidas de seguridad establecidas por el Reglamento de desarrollo; a partir de mayo de 2018, tanto responsables, como encargados deberán hacer un análisis y valoraciones previos del tratamiento de sus bases de datos y en función de los resultados y de los posibles riesgos detectados, aplicar las medidas técnicas y organizativas que garanticen una correcta protección de la información.

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com