El desempeño de las funciones de Delegado de Protección de Datos

Gestión de procesos críticos y casos prácticos

Pere Simón Castellano

BOSCH

Wolters Kluwer

BOSCH

El desempeño de las funciones de Delegado de Protección de Datos

Gestión de procesos críticos y casos prácticos

Pere Simón Castellano

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www. wolterskluwer.es

Primera edición: Diciembre 2018

Depósito Legal: M-37403-2018
ISBN versión impresa: 978-84-9090-341-4
ISBN versión electrónica: 978-84-9090-342-1

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S. A.
Printed in Spain

El DPO en la gestión de una brecha de seguridad

Los sistemas de una entidad bancaria son hackeados como consecuencia de ataque a un sistema de comunicaciones inseguras, y se produce un robo de información relativa a las credenciales bancarias y demás información confidencial, si bien se desconoce si el objetivo era sacar un beneficio económico con la venta de datos o por espionaje industrial.

CUESTIONES

1. ¿Cuáles son las obligaciones del responsable del tratamiento según el RGPD?

2. ¿Cuál es el procedimiento para realizar las notificaciones en caso de violaciones de seguridad?

3. ¿Y las excepciones a la obligación de notificación?

4. ¿Qué medidas de seguridad deberían haberse adoptado para mitigar el riesgo? En tal caso, ¿sería necesario comunicar la brecha a los afectados?

5. ¿Cómo ejercería un DPO sus funciones en este supuesto? Destaca su papel previo y posterior a la violación de seguridad.

CUESTIONES RESUELTAS

1. ¿Cuáles son las obligaciones del responsable del tratamiento según el RGPD?

En primer lugar (1) deberá adoptar las medidas de seguridad necesarias para evitar un nuevo robo de información y, en su caso, mitigar los efectos negativos de esa violación de seguridad. Este primer paso incluye convocar a los interlocutores que pueden ayudar a minimizar los riesgos de la fuga de información; aplicar las medidas para la recuperación frente al ataque que han sufrido los sistemas informáticos; finalmente, implementar las medidas de contención a la mayor brevedad posible.

Para ello, el responsable deberá convocar con carácter urgente a los siguientes interlocutores:

— Al Delegado de Protección de Datos, a efectos de que pueda asesorar sobre cómo gestionar la crisis o incidente de seguridad, así como coordinar las medidas de recuperación y de seguridad que se deberán adoptar.
— Al responsable de los sistemas informáticos, para valorar conjuntamente las medidas técnicas necesarias para solucionar la crisis.

La principal será medida a adoptar será, en primer lugar, aplicar las medidas de seguridad necesarias para detener el robo de información o minimizar al máximo sus efectos, lo que implicará, por parte del personal del departamento de informática, revisar todos los sistemas de seguridad para solucionar la crisis.

Paralelamente, se convocará a los responsables internos del fichero origen del robo de datos para analizar, junto al DPO, los siguientes aspectos en relación con la sustracción de datos:

a) El volumen de afectados por el robo de datos.
b) La categoría o el tipo de datos personales sustraídos.
c) Delimitar la categoría de interesados afectados.
d) Poner en conocimiento la violación de seguridad a las autoridades competentes, teniendo en cuenta la tipología de datos sustraídos.

En segundo lugar (2) deberá ponerse en conocimiento de las autoridades policiales, para denunciar la violación y recabar su opinión para la comunicación de la violación de seguridad a los interesados para evitar que una prematura comunicación pueda obstaculizar innecesariamente una investigación de las circunstancias de la violación de seguridad.

Una vez analizadas estas cuestiones (3) se deberá valorar la gravedad de la violación de seguridad y, el tipo de perjuicios que pueden causar a los afectados, a efectos de determinar las medidas a adoptar, en base al riesgo para las libertades y derechos de las personas físicas involucradas. En función del resultado de ese ejercicio de valoración de la gravedad de la brecha, será necesario o no notificar la violación de seguridad al interesado y a la autoridad de control correspondiente. Recuérdese que como hemos estudiado en esta monografía, siempre es obligatorio notificar la brecha a la autoridad de control en un plazo máximo de 72 horas desde que se tiene conocimiento de la misma. Sin embargo, puede no hacerse en tiempo y forma y notificarse con posterioridad cuando existe una justificación y se explicitan los motivos de la tardanza. En el presente caso, de fuga o robo de información en una entidad bancaria, no parece razonable que no se notifique dentro de ese plazo, si bien es cierto que previamente o paralelamente habría que interponer la correspondiente denuncia ante la policía o directamente al juzgado de guardia, por las consecuencias penales que indudablemente revisten los hechos del supuesto que ahora nos ocupa.

Partiendo de la base de que se tiene constancia del robo de credenciales bancarias y otros datos confidenciales de los interesados, independientemente de que se desconozca el motivo de la sustracción, al tratarse de datos que pueden entrañar diversos perjuicios

a los interesados como pérdidas financieras, usurpación de la identidad e incluso una pérdida sobre el control y uso de sus datos, se deberán tomar las siguientes medidas con carácter urgente:

a) **Comunicación inmediata de la violación de seguridad a los interesados** ya que la sustracción de sus datos puede entrañar graves riesgos para sus derechos y libertades, en especial datos bancarios, para que éstos puedan tomar las precauciones necesarias para evitar un uso ilegítimo de sus datos.
La gravedad de las consecuencias del robo de credenciales bancarias para el interesado que pueden suponer un riesgo de daños y perjuicios inmediatos, implica la adopción de medidas extraordinarias como priorizar la comunicación a éstos, para que puedan pueden aplicar medidas para mitigar los potenciales efectos adversos de la violación.
Esta comunicación, en la medida de lo posible, y siempre que no suponga un retraso innecesario en la comunicación, se realizará en colaboración con la autoridad de control competente y, en su caso, conjuntamente con las autoridades policiales.
Esta notificación se realizará mediante un lenguaje claro y sencillo de manera que el interesado entienda el riesgo de la violación. La comunicación contendrá como mínimo:
    - La naturaleza de la violación y descripción de las posibles consecuencias de la brecha de seguridad.
    - Datos de contacto del Delegado de Protección de Datos o, en su caso, otro teléfono o email de contacto creado *ad hoc* para ampliar la información sobre la violación.
    - Descripción de las medidas de seguridad adoptadas o propuestas por el Responsable del tratamiento para poner remedio a la violación de seguridad, incluyendo si procede, las medidas de seguridad adoptadas para mitigar los posibles efectos negativos.

b) **Notificar a la autoridad de control correspondiente la violación de seguridad.**
El Responsable del tratamiento, tan pronto como les sea posible, por medio del Delegado de Protección de Datos y, como máximo, en el plazo de 72 horas, comunicará a la autoridad de control competente la violación de seguridad.
Esta comunicación deberá contener la máxima información posible y como mínimo:
    - La naturaleza de la violación de la seguridad de los datos personales, inclusive, 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.
    - Datos de contacto del Delegado de Protección de Datos o, en su caso, de un teléfono o email del que pueda obtenerse más información.

Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de 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.

El Responsable del Tratamiento en coordinación con el DPO deberá colaborar en todo momento y, en su caso seguir las directrices que le indique la autoridad de control.

— El Responsable del tratamiento deberá valorar las circunstancias en las que se ha producido la violación y documentarla incluyendo los hechos relacionados con ésta, los efectos producidos y las medidas correctoras aplicadas para que no se vuelvan a producir violaciones de seguridad. Deberá también comprobar si se ha registrado correctamente la incidencia indicando cada una de las circunstancias de la violación de seguridad en el registro de incidencias de seguridad.

Fruto de este análisis, el Responsable del tratamiento en coordinación con el DPO y demás responsables internos afectados, deberán adoptar todas las medidas de seguridad técnicas y organizativas necesarias para evitar que se produzcan en un futuro situaciones similares.

Adicionalmente, el Responsable del tratamiento en coordinación con el DPO podrá valorar la conveniencia de realizar una evaluación de impacto que determine el riesgo de la organización en relación con ese tratamiento de datos y así, comprobar si el riesgo que entraña el tratamiento está justificado, legitimado y ha sido debidamente minimizado mediante la implementación de las medidas de seguridad oportunas.

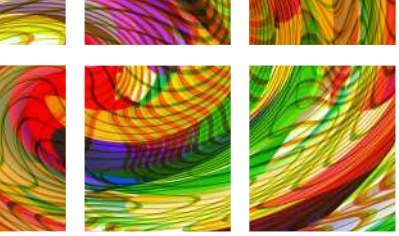
2. ¿Cuál es el procedimiento para realizar las notificaciones en caso de violaciones de seguridad?

— Notificación al interesado: A los efectos de que el interesado conozca la violación de seguridad y las consecuencias sobre sus derechos y libertades, se deberá utilizar un lenguaje claro y sencillo.

Habida cuenta de la gravedad de la violación, se adoptarán los procedimientos más efectivos para el envío (rapidez) y efectividad (verificación de entrega).

Tal como se ha especificado en el apartado anterior, se les indicará los datos de contacto del Delegado de Protección de Datos u otros miembros de la organización, para que puedan ampliar la información y, en su caso, para ser aconsejados respecto las medidas que pueden adoptar para paliar los efectos de la violación de seguridad.

— Notificación a la Autoridad de Control y Policial. Todo el proceso se deberá realizar en un plazo máximo de 72 horas. No existe un procedimiento de comunicación establecido formalmente en el RGPD, pero el Delegado de Protección de Datos como



El Reglamento General de Protección de Datos de la Unión Europea incorpora importantes novedades, entre las que destaca la figura del Delegado de Protección de Datos (DPO). Posteriormente, ha sido la nueva Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) la que ha matizado y desarrollado algunas de sus atribuciones.

Al DPO le corresponde la supervisión del cumplimiento normativo en protección de datos, la tarea de informar y asesorar de forma periódica a la gerencia o dirección y, finalmente, la mediación en caso de conflicto entre los diferentes actores implicados.

La presente obra pretende facilitar al operador jurídico el desarrollo de sus tareas y funciones, en un sector, el de la protección de datos, muy técnico y especializado. La complejidad del lenguaje, los tecnicismos propios de profesionales IT y la necesaria polivalencia del DPO son simplificados en esta monografía con el objetivo de aportar al lector los conocimientos, ideas y conceptos clave que le deben permitir desarrollar todas las tareas propias del Delegado.

Para ello, se plantean y resuelven casos prácticos que detallan la actuación del DPO en la gestión de procesos críticos: desde el asesoramiento en la realización de evaluaciones de impacto o en el desarrollo de software y APP's móviles, pasando por la supervisión de los registros de actividades de tratamiento, la definición de las bases de legitimación de los mismos y la gestión de las transferencias internacionales de datos, hasta su papel en la gestión de reclamaciones y brechas de seguridad.

La presente monografía aúna teoría y práctica, como si se tratase de una guía básica, que ofrece recursos para el desarrollo de las funciones del DPO, una profesión al alza, de presente y futuro en Europa.

ISBN: 978-84-9090-341-4
9 788490 903414
3652K28512

Wolters Kluwer