Boletín 03/24

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Ejercicio de los derechos: derecho de rectificación y oposición

Contenido

El responsable del tratamiento de los datos personales debe de facilitar al interesado/a la posibilidad de ejercitar los derechos contemplados en el RGPD.

1. **El derecho de rectificación**: supone que podremos obtener la rectificación de los datos personales que sean inexactos sin dilación indebida por parte del responsable del tratamiento. **Según los fines del tratamiento, tenemos derecho a que se completen los datos personales incompletos, incluso mediante una declaración adicional.** En la solicitud se indicará los datos a los que nos referimos y la corrección a realizar. Cuando sea necesario, se acompañará la documentación que justifique la inexactitud o carácter incompleto de los datos.

2. **El derecho de oposición** supone que podemos oponernos a que el responsable realice un tratamiento de los datos personales, cuando el tratamiento esté basado en una misión de interés público o legítimo, incluida la elaboración de perfiles y, también, **en el caso de que el tratamiento tenga como finalidad la mercadotecnia directa.**

IMPORTANTE

Si el responsable del tratamiento tiene dudas razonables en relación con la identidad del solicitante podrá pedirle información adicional para confirmar su identidad.

SANCIONES DE LA AEPD

Sancionado con 5.000€ un centro de formación por no atender debidamente un derecho de supresión

En la resolución de la AEPD https://www.aepd.es/documento/ps-00555-2023.pdf se sanciona a un centro de formación por no atender debidamente un derecho de supresión.

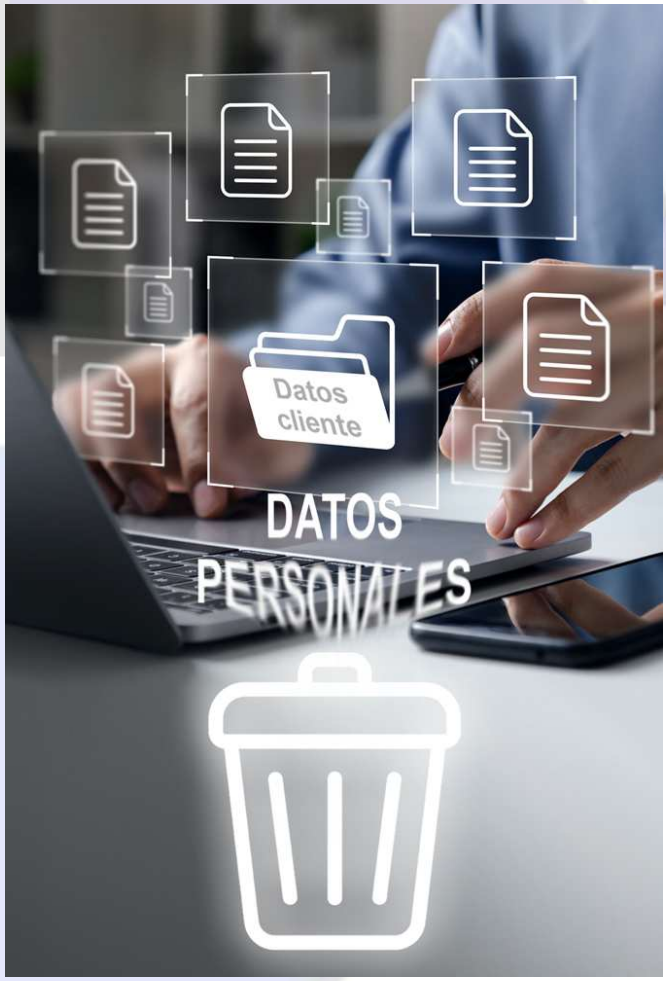
El reclamante en su escrito de reclamación manifestó que envió un correo electrónico a la dirección adecuada para el ejercicio de derechos. Fue contestado por el delegado de protección de datos indicándole que sus datos habían sido eliminados, aunque siguió recibiendo información comercial a su correo electrónico.

El reclamante a pesar de haber recibido un correo con acuse de recibo indicándole la baja se le envío un nuevo correo comercial. **La Agencia en su resolución consideró que la naturaleza de la infracción fue muy grave, puesto que los datos personales no habían sido borrados de una forma eficaz.**

El centro de formación fue sancionado con 5.000€ por el derecho de supresión, recogido en el articulo 71 del RGPD. Además, se ordenó al responsable del tratamiento, que, en el plazo de un mes, notificase a la Agencia la adopción de medidas consistentes en el borrado de todos los datos personales que posea del reclamado.

La parte reclamada procedió al pago de 3.000€ haciendo uso de las reducciones de pronto pago y reconocimiento de la responsabilidad.

Art. 17 RGPD: Derecho de supresión: el interesado tendrá derecho a obtener sin dilación indebida la supresión de sus datos personales



IMPORTANTE

El responsable del tratamiento debe actuar de forma diligente y sin dilación indebida ante el ejercicio de los derechos por parte de los interesados/as.

LA AEPD ACLARA

Cifrado y Privacidad: cifrado en el RGPD

En la página web de la AEPD podemos encontrar una amplia información sobre el uso de cifrado o técnicas criptográficas. Se trata de técnicas que tanto el responsable del tratamiento como el encargado pueden y deben emplear para reducir el riesgo en el tratamiento de datos de carácter personal.

En el RGPD encontramos un número considerable de referencias al cifrado, así, por ejemplo, en el art. 32 "Seguridad del tratamiento" se indica que el responsable y el encargado de tratamiento según el estado de la técnica, los costes de aplicación, y la naturaleza del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas aplicarán medidas técnicas y organizativas para garantizar un nivel adecuado al riesgo, incluyendo entro otros: La seudonimización y el cifrado de datos personales.

En este sentido las técnicas de seudoanimización más utilizadas son el cifrado con clave secreta. El Dictamen 05/2014 sobre técnicas de anonimización del Grupo del Artículo 29 establece los límites del cifrado con relación a los datos de carácter personal. **El uso del cifrado es una garantía que se puede incorporar en un tratamiento para gestionar el riesgo, sobre todo, cuando la comunicación se realice a través de Internet, cuando los datos personales se utilicen para otra finalidad o cuando se haya producido una brecha de seguridad.**

IMPORTANTE

La utilización del cifrado no elimina la naturaleza de dato de carácter personal, por lo que la información cifrada no es una información anonimizada.

ACTUALIDAD LOPD

La AEPD participa en una acción europea para analizar la aplicación del derecho de acceso

Fuente: AEPD

(29 de febrero de 2024). La Agencia Española de Protección de Datos (AEPD) participa en una acción europea coordinada para conocer cómo aplican las organizaciones en la práctica el derecho de acceso que ejercitan los ciudadanos, dentro del marco de actuaciones del Comité Europeo de Protección de Datos (CEPD) de 2024. El CEPD ha seleccionado esta temática ya que el derecho de acceso permite a las personas **conocer qué datos tiene sobre ellas una organización** y, en muchas ocasiones, se convierte en la **puerta de entrada para ejercitar otros derechos** de protección de datos como el de rectificación o supresión.

Las autoridades de control del Espacio Económico Europeo participarán en esta acción a lo largo del año. La AEPD, por su parte, analizará las prácticas de una muestra variada de responsables del tratamiento, tanto del sector público como privado, para conocer tanto las buenas prácticas como si existe alguna problemática relacionada con la atención al ejercicio del derecho de acceso. En 2023, el CEPD adoptó las Directrices sobre los derechos de los interesados - Derecho de acceso para ayudar a las organizaciones a responder a las solicitudes en consonancia con los requisitos establecidos en el Reglamento General de Protección de Datos.

Los resultados de esta acción se analizarán de manera coordinada y las Autoridades podrán decidir sobre posibles acciones adicionales de supervisión y aplicación en sus respectivos países. Además, los resultados serán agregados, generando una visión amplia y permitiendo un seguimiento específico en el ámbito del Espacio Económico Europeo. Finalmente, el Comité publicará un informe sobre el resultado de este análisis una vez concluidas las acciones.

Esta acción es la tercera iniciativa en el marco del Marco de Aplicación Coordinada (MCE), entre cuyos objetivos se encuentra la cooperación entre las autoridades de protección de datos. Las acciones coordinadas anteriores analizaron el uso de servicios en la nube por parte del sector público y la designación y situación de los Delegados de Protección de Datos en las organizaciones.

Puede ver más información en el siguiente enlace:

Directrices sobre los derechos de los interesado- Derecho de acceso

EL PROFESIONAL RESPONDE

La identidad digital corporativa: riesgos y amenazas (II)

La utilización de los medios sociales por parte de la empresa para la creación de su identidad digital, le reporta unos beneficios positivos, pero al mismo tiempo, se han de tener en cuenta las amenazas e impactos negativos en su imagen y reputación online.

Desde el punto de vista de la seguridad las principales amenazas son las siguientes:

1. **Suplantación de identidad.** Los atacantes crean perfiles falsos con el propósito del robo de información sensible de los usuarios de la empresa suplantada. Para conseguir este cometido utilizan diferentes técnicas:
   a. ***Phishing:*** usurpación del correo electrónico de la entidad y perfil de las redes sociales, para que el receptor crea en su veracidad y facilite sus datos privados.
   b. ***Pharming***: creación de página web fraudulenta que suplanta a la oficial.

2. **Ataque de denegación de servicio distribuido, o ataque *DDoS.*** Los equipos utilizados para lanzar el ataque forman parte de una red de ordenadores zombis que el ciberatacante controla de forma remota.

3. **Utilización no consentida de derechos de propiedad industrial.**

IMPORTANTE

La empresa debe conocer las amenazas que pueden provocar impactos negativos en la identidad digital y su reputación *online*.

AUTOR: JULIO CÉSAR MIGUEL PÉREZ