Boletín 12/23

LOPD EN LA EMPRESA

Autor: Julio César Miguel Pérez

EL RGPD UE 2016/679 EN APLICACIÓN

Principio de responsabilidad proactividad (IV)

Contenido

A lo largo de estos boletines hemos visto los principios relativos al tratamiento regulados en el RGPD:

- licitud, lealtad y transparencia
- limitación de la finalidad
- principio de minimización de datos
- principio de exactitud
- limitación del plazo de conservación
- Integridad y confidencialidad

Para finalizar la revisión de estos principios, tenemos que hacer referencia al principio que engloba todos los anteriores y es el llamado principio de responsabilidad proactiva. Lo que quiere decir este principio, es que el responsable y el encargado del tratamiento de datos personales deben cumplir con todos los principios enumerados con anterioridad, y no solamente eso, además, deben ser capaces de demostrarlo. Este principio, supone que se debe de implantar un sistema interno de cumplimiento en materia de protección de datos. **Para ello, no basta con implementar medidas técnicas y organizativas, serán necesarias también, políticas que garanticen que las actividades de tratamiento se realizan conforme con la normativa en protección de datos.**

IMPORTANTE

El principio de responsabilidad proactiva implica que las medidas de seguridad técnicas y organizativas se actualicen y revisen de forma periódica.

SANCIONES DE LA AEPD

Sancionada una farmacia por no destruir debidamente documentación con datos personales

En la resolución de la AEPD https:// https://www.aepd.es/documento/ps-000538-2022.pdf, se sanciona a una farmacia por el incumplimiento del principio de integridad y confidencial.

La parte denunciante manifiesta en su reclamación que, en un contenedor público cercano a su domicilio, de forma reiterada, se encuentra una gran cantidad de documentación de índole sanitaria con datos personales, procedentes de una farmacia. Junto con la denuncia se aportaron como pruebas 49 imágenes y 68 vídeos, que demostraban los documentos depositados en el contenedor, rotos a mano en fragmentos de gran tamaño que no impedían ver la información que contenían. **La Guardia Civil también tuvo conocimiento de los hechos a través de la parte denunciante realizando después una "diligencia de exposición".**

La AEPD estimó en su resolución que las pruebas aportadas en la reclamación acreditan el incumplimiento del art. 32.1 del RGPD "Seguridad del tratamiento", puesto que la no destrucción adecuada de la documentación permitió el acceso por parte de terceros a los datos contenidos en los documentos. **La farmacia incumplió además con el principio relativo a la integridad y confidencialidad, ya que el tratamiento de los datos personales se realizó sin garantizar una seguridad adecuada.** La multa ascendió a 10.000 euros.

Los principios relativos al tratamiento han de observarse con especial diligencia por los responsables y encargados del tratamiento.

IMPORTANTE

El responsable y el encargado de tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluya la capacidad de garantizar la confidencialidad de los datos.

LA AEPD ACLARA

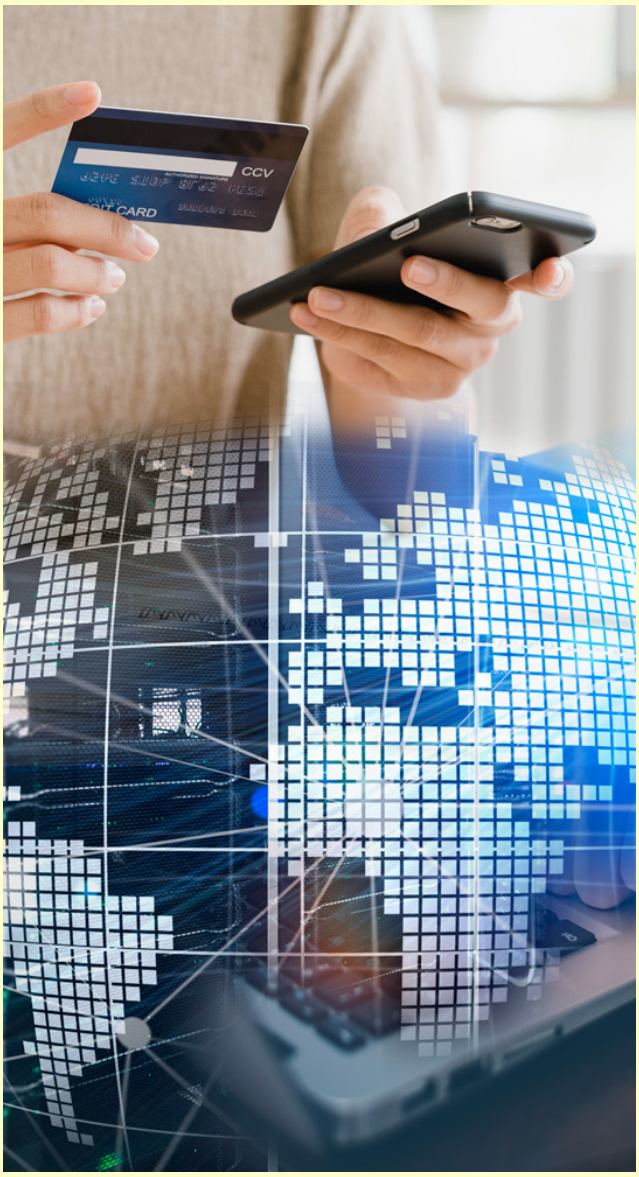
Transferencias internacionales de datos personales a terceros países: UE-EE.UU. Marco de privacidad de datos

Las transferencias internacionales de datos suponen la circulación de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Las transferencias de datos personales a terceros países y organizaciones internacionales están reguladas en el RGPD. Existen diferentes mecanismos para poder realizar estas transferencias de datos personales. **En este caso, nos vamos a referir a las transferencias internacionales de datos basadas en una decisión de adecuación, y en concreto, la decisión de 10 de julio de 2023 *"EU- USA Data Privacy Framework".***

Los países que hasta la fecha han sido declarados con un nivel de protección adecuado por la Comisión Europea son; Suiza; Canadá; Argentina; Guernsey; Isla de Man; Jersey; Islas de Feroe; Andorra; Israel; Uruguay; Nueva Zelanda; Japón; Reino Unido y República de Corea.

Al listado anterior, habría que añadir desde el día 10 de julio de 2023 a los EE. UU. **En base a esta decisión de adecuación relativa al Marco de Privacidad de Datos, los datos personales podrán circular de forma segura desde la UE a las empresas estadounidenses que participen en el Marco, sin la necesidad de establecer garantías adicionales de protección de datos.**



IMPORTANTE

Para realizar una transferencia internacional de datos además de la decisión de adecuación, se tendrá que conformar un contrato de acceso a datos por cuenta de terceros.

ACTUALIDAD LOPD

La AEPD publica una guía sobre la utilización de datos biométricos para el control de presencia y acceso

Fuente: AEPD

(23 de noviembre de 2023). La Agencia Española de Protección de Datos (AEPD) ha publicado la Guía Tratamientos de control de presencia mediante sistemas biométricos, un documento que fija los criterios para la **utilización de la biometría** para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas que tenerse en cuenta para que un tratamiento de datos personales que utilice esa tecnología cumpla con el Reglamento General de Protección de Datos (RGPD) entre otras normativas.

Los sistemas biométricos y el tratamiento de los datos que se pueden obtener a partir de ellos están evolucionando muy rápidamente. Los nuevos sistemas aumentan el detalle de la información recogida e incluso permiten la posibilidad de recoger información sin la cooperación de la persona, que en ocasiones ni siquiera es consciente de ello. A ello se suma el desarrollo de la inteligencia artificial, que puede utilizarse para inferir información adicional sobre las personas.

La Agencia considera el tratamiento de datos biométricos, **tanto para identificación como para autenticación**, como un tratamiento de **alto riesgo** que incluye **categorías especiales de datos**. Tal y como establece el RGPD, para poder tratar esas categorías es **necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime**.

En el caso de registro de jornada y control de acceso **con fines laborales**, si el levantamiento de la prohibición se basa en el artículo 9.2.b) del RGPD, el responsable debe contar con una norma con rango de ley que autorice específicamente utilizar datos biométricos para dicha finalidad. La Agencia especifica que, en el marco de estos tratamientos, el consentimiento no puede levantar la prohibición o ser una base para determinar la licitud de este, al existir un desequilibrio entre la persona a la que se somete al tratamiento y quien lo está llevando a cabo.

Puede ver más información en el siguiente enlace:

Guía sobre tratamientos de control de presencia mediante sistemas biométricos

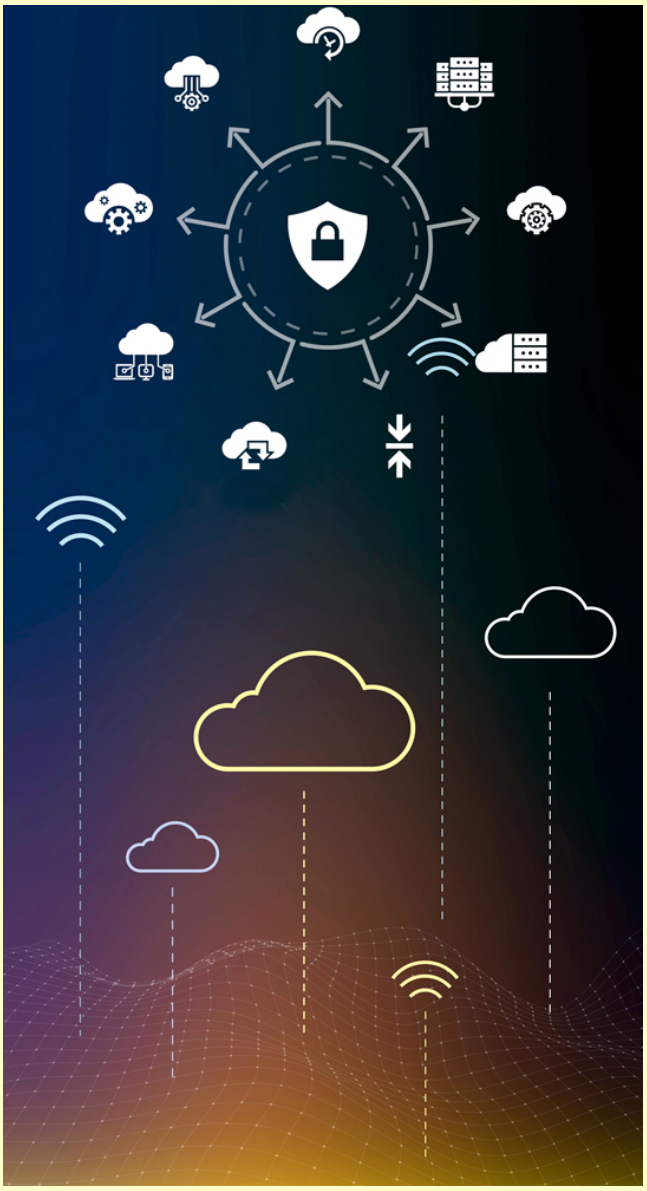
EL PROFESIONAL RESPONDE

Nuevas tecnologías y ciberseguridad: aplicaciones en la nube (I)

Las nuevas tecnologías se han incorporado en la actividad de nuestras empresas a una velocidad vertiginosa. Nos permite una mayor productividad, crecimiento económico y ahorro de costes, puesto que estos servicios en la nube aportan agilidad al negocio. El conocimiento de cómo funcionan estas aplicaciones resulta clave para poder contratar el servicio con seguridad.

En este caso, vamos a centrarnos en las aplicaciones en la nube que podemos encontrar en el mercado:

- **nube pública**: Los clientes utilizan los servicios que son procesados en el mismo servidor que otros clientes. Una de las ventajas es el ahorro de tiempo y costes, aunque por el contrario hay poca transparencia puesto que no sabemos el resto de los recursos que estamos compartiendo.
- **nube privada**: Los recursos se ofrecen de forma exclusiva para nuestra empresa. Nos ofrece un mayor control de los recursos y seguridad, aunque tiene un elevado coste.
- **nube híbrida**: incorpora servicios únicos y compartidos con otros clientes. Una de las ventajas es que se maximiza el valor y se reducen costes. El inconveniente es la falta de control de la seguridad entre ambas nubes.



IMPORTANTE

El modelo de aplicación en la nube a elegir dependerá del servicio que desarrollemos y de sus requisitos de seguridad.