PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 05/22

EL RGPD UE 2016/679 EN APLICACIÓN

Listado de tratamientos concretos de la LOPDGDD (II)

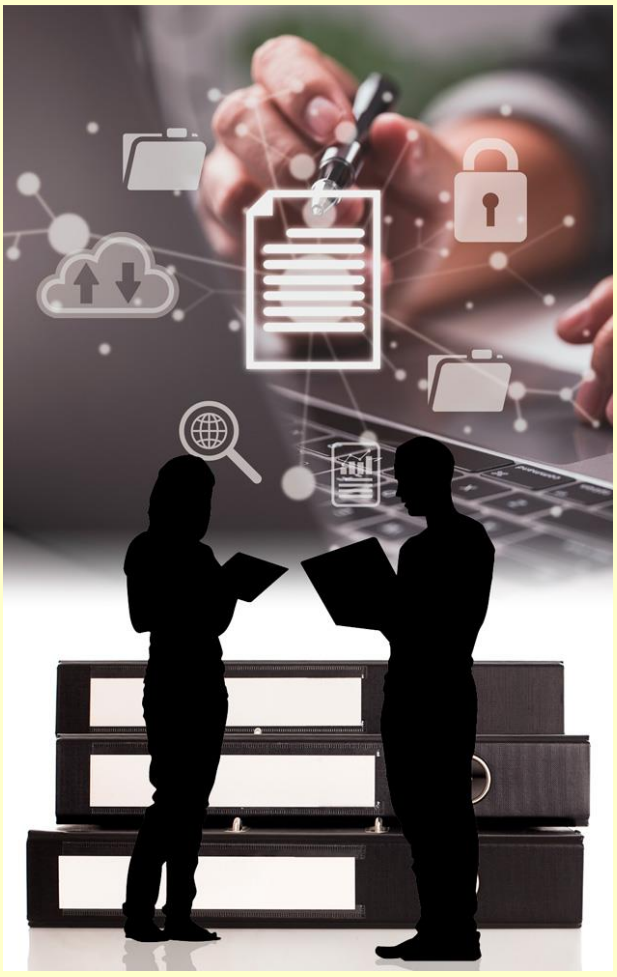
Contenido

En el anterior boletín nos referíamos a la importancia del registro de actividades de tratamiento. **En nuestra ley orgánica (LOPDGDD) se regulan una serie de tratamientos de forma concreta. El responsable del tratamiento debe tenerlo en cuenta para aplicar la normativa adecuadamente.**

Los tratamientos regulados son los siguientes:

- Tratamiento de datos de contacto, empresarios individuales y de profesionales liberales.
- Tratamiento de los sistemas de información crediticia.
- Tratamientos relacionados con operaciones mercantiles.
- Tratamiento con fines de videovigilancia.
- Sistemas de exclusión publicitaria.
- Sistemas de información de denuncias internas.
- Tratamiento de datos en el ámbito de la función estadística pública.
- Tratamiento de datos con fines de archivo en interés público.
- Tratamiento de datos relativos a infracciones y sanciones administrativas.

Añadiríamos en este listado, aquellos que vengan indicados en su normativa específica.



IMPORTANTE

Todos los responsables y encargados de tratamiento tienen que realizar un registro de las actividades de tratamiento que efectúan bajo su responsabilidad.

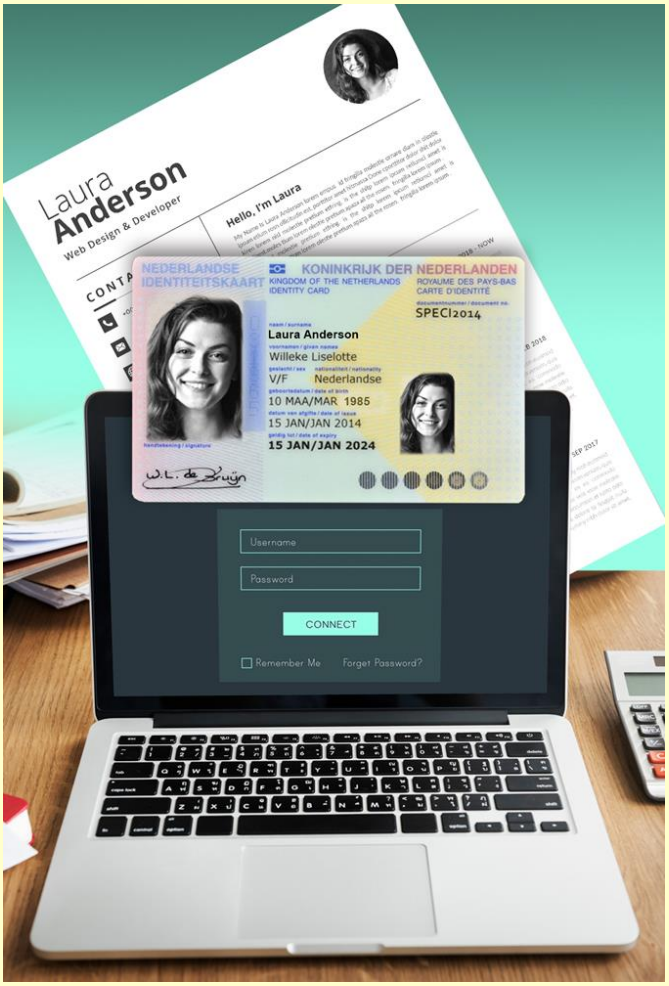
SANCIONES DE LA AEPD

Multinacional sancionada con 250.000€ por un protocolo inadecuado de atención de derechos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00003-2021.pdf se sanciona a una multinacional, consultora líder a nivel internacional en selección de candidatos.

No contestar en el plazo de un mes una solicitud de derechos supone una infracción grave.

La reclamante, una ciudadana holandesa, interpuso la reclamación ante la Autoridad de control de Países Bajos, y se dio traslado a la AEPD, que actuó como autoridad de control principal, al encontrarse el servicio de cumplimiento legal de la multinacional en Barcelona. Aunque en un principio, la autoridad española no encontró indicios de incumplimiento, varias autoridades europeas formularon objeciones al procedimiento, por lo que finalmente, la entidad reclamada fue sancionada.



La reclamante manifestó que envió su CV a la citada multinacional a través de su página web mediante contraseña y usuario. Solicitando un tiempo después el ejercicio del derecho de acceso a sus datos personales. Para ello, se le requirió por parte de la entidad reclamada, que debía aportar su DNI.

En la resolución la AEPD, estimó que solicitar el DNI para identificar al interesado del ejercicio del derecho resultaba excesivo, ya que, existían otros medios de comprobación, como el usuario y contraseña de la reclamada. No se tuvo en cuenta el principio de minimización de datos. Se le sancionó con 250.000€.

IMPORTANTE

La entidad reclamada no había implementado un protocolo adecuado para atender el ejercicio de derechos en materia de protección de datos.

LA AEPD ACLARA

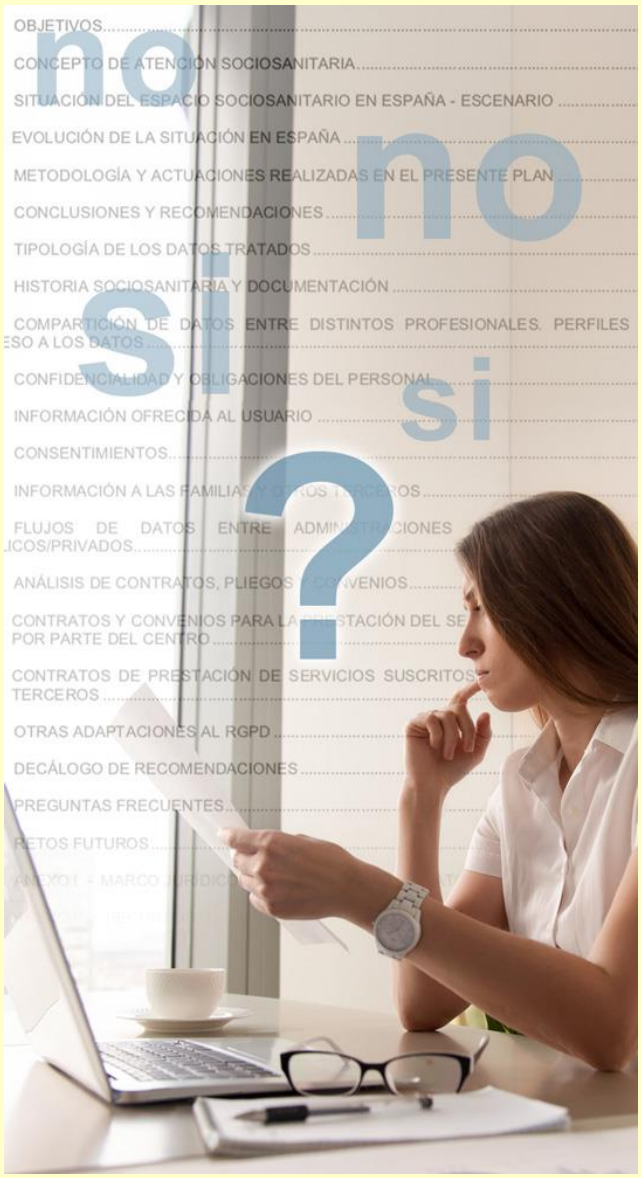
Guía para la notificación de brechas de datos personales a los afectados (II)

En el apartado de la AEPD Guías y Herramientas, encontramos la Guía para la notificación de brechas de datos personales.

En esta guía se concretan los supuestos en los que el responsable del tratamiento tiene que notificar la brecha de datos personales a los interesados afectados. Estos son todas las personas físicas cuyos datos personales se han visto afectados por una brecha y les puede ocasionar consecuencias.

El responsable deberá comunicar a la mayor brevedad posible cuando exista un alto riesgo para los derechos y libertades de las personas, la falta de confidencialidad, integridad o disponibilidad de sus datos. Incluyendo, la falta de disponibilidad de los servicios asociados a esos datos personales. Se comunicará siempre que los daños producidos sean irreversibles.

En cambio, no será necesaria la comunicación cuando, el responsable haya tomado medidas técnicas y organizativas adecuadas, que eviten los riesgos, que minimicen los daños, o bien, que los haga reversibles. Tampoco será necesaria su comunicación, cuando con posterioridad a la brecha, el responsable haya adoptado medidas que mitigen total o parcialmente el posible impacto. **Así, por ejemplo, cuando aplique medidas como la revocación, cancelación o bloqueo de credenciales de acceso o el restablecimiento del servicio y copias de seguridad que faciliten la disponibilidad e integridad de los datos.**
Tanto la decisión de comunicar, o la no necesidad de comunicar debe ser documentada.



IMPORTANTE

La AEPD ha publicado el informe de brechas de seguridad del mes de marzo de 2022

ACTUALIDAD LOPD

Brechas de datos personales: entornos de desarrollo y preproducción

Fuente: AEPD

La ingeniería de sistemas establece la conveniencia de trabajar con varios entornos diferenciados: habitualmente, desarrollo, preproducción y producción. De forma general, lo recomendable es trabajar en el entorno de desarrollo, realizar las pruebas en el entorno de preproducción y finalmente desplegar aplicaciones y servicios en el entorno de producción. Desde la óptica de protección de datos, hay que tener en cuenta esta diferenciación y limitar la exposición de datos personales reales, y/o que estén en los sistemas de producción, en las fases de desarrollo y pruebas por el riesgo que puede suponer para los derechos y libertades de las personas.

Todavía es habitual encontrar entornos de desarrollo y preproducción en los que las medidas técnicas y organizativas orientadas a implementar las medidas y garantías establecidas en el Reglamento General de Protección de Datos (RGPD) se relajan, o quedan expuestos a internet sin medidas de seguridad o abandonados y en desuso por lo que las medidas de seguridad pronto quedan obsoletas. Pero tampoco hay que olvidar que en algunos casos se empleen datos reales para pruebas de depuración de errores en labores de mantenimiento y/o desarrollo.

Con la aplicación del RGPD y la LOPDGDD, la situación respecto al uso de datos personales para pruebas en general, y en particular en entornos de desarrollo, se puede resumir brevemente a continuación.

En primer lugar, el RGPD en su artículo 32 Seguridad del tratamiento, establece que el responsable y el encargado de tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados. Luego el responsable y el encargado deben determinar las medidas de seguridad apropiadas con respecto al uso de datos personales reales en entornos de preproducción y pruebas. Además, deben establecer estas medidas teniendo en cuenta el nivel de riesgo específicamente con relación a la protección de datos, de igual forma que han de tener en cuenta los riesgos para la organización, como en cualquier entorno de producción. (…)

Conforme al principio de minimización de datos y el principio de protección de datos desde el diseño y por defecto, cuando sea posible debe evitarse la utilización de datos personales en entornos de desarrollo y preproducción, o cualquier otro entorno de pruebas.

Además, las pruebas de software con datos personales son, o forman parte de, tratamientos de datos personales y el responsable del tratamiento debe cumplir con todas las obligaciones que se desprenden del RGPD.

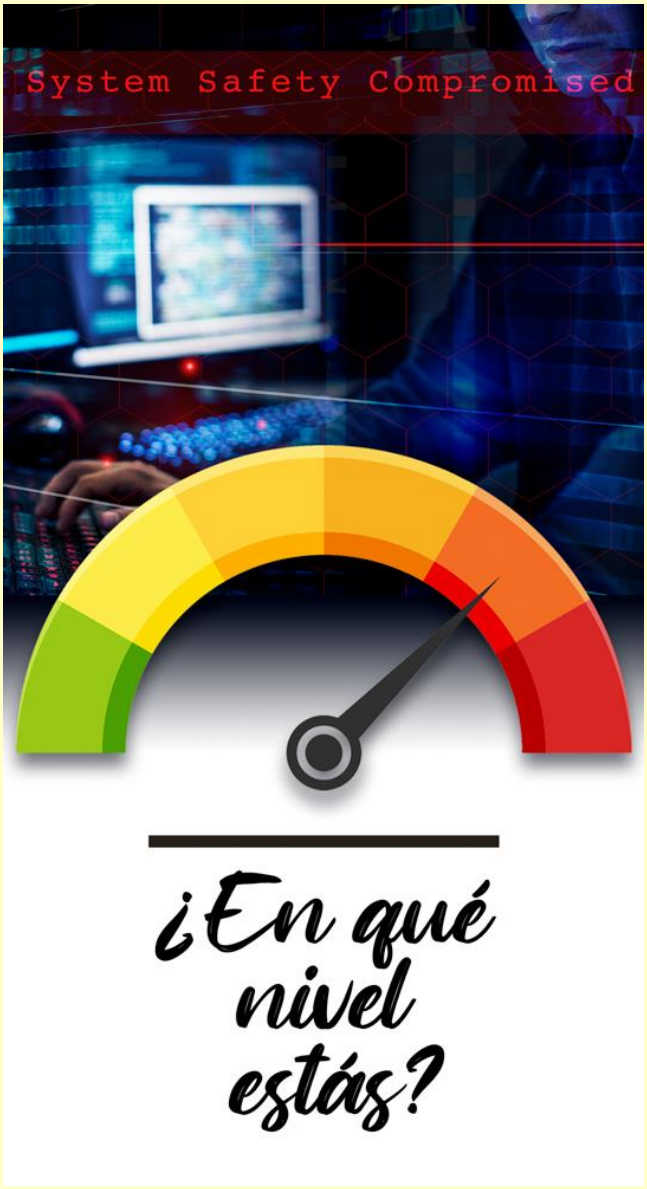
Puede ver más información en el siguiente enlace

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Los principales riesgos y amenazas en las redes inalámbricas (II)

Se hace necesario, hoy en día, conocer las principales amenazas a las que se encuentran expuestas las redes inalámbricas. Su conocimiento nos podrá ser de utilidad para aplicar medidas de seguridad adecuadas.



Ataques por fuerza bruta: Con este método se pretende hacer uso de todas las contraseñas posibles y averiguar las claves criptográficas de aquellas que dan acceso a la red wifi. En Internet se pueden encontrar herramientas gratuitas para hacerse con aquellas claves de redes que no tengan claves robustas.

Denegación de servicio: A través de este ataque envían peticiones de servicio masivas a los puntos de acceso sobrecargándoles, de manera que se impide a los usuarios legítimos hacer uso del servicio que presta.

Man-in-the-middle: El atacante se sitúa entre el emisor y el receptor, suplantando a una de las partes. De esta forma se hace creer a la otra parte que está hablando con el legítimo destinatario de la comunicación.

Mac Spoofing: Con este tipo de ataques se trata de suplantar la dirección *MAC,* que es un identificador único e irrepetible que identifica todo dispositivo conectado a una red. Este ataque se produciría siempre y cuando el punto de acceso tuviera configurada una lista de este tipo de direcciones permitidas.

IMPORTANTE

Realizar un análisis de riesgos adecuado a la entidad, podría reducir las consecuencias de las amenazas de las redes inalámbricas.