PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 08/22

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamientos concretos: Sistemas de Información crediticia

En nuestra LOPDGDD, en concreto, el articulo 20 regula estos sistemas de información crediticia conocidos como ficheros de morosos.

El tratamiento de los datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito, será lícito, siempre y cuando se cumplan los siguientes requisitos:

- Los datos tienen que ser facilitados por el acreedor o por quién actúe por su cuenta o interés.
- Los datos se refieren a deudas ciertas, vencidas y exigibles. Además, no tiene que existir reclamación administrativa o judicial por parte del deudor.
- El acreedor debe informar al afectado en el contrato, o bien en el momento de requerir el pago, de la posibilidad de inclusión en un fichero de morosos.

La entidad que mantenga los ficheros, relativos al incumplimiento de las deudas, definidas con anterioridad, debe notificar al afectado la inclusión de sus datos. Le informará, también, sobre la posibilidad del ejercicio de los derechos en materia de protección de datos. El plazo para informar será de 30 días desde la notificación de la deuda. Durante ese plazo los datos deben quedar bloqueados.

Contenido

IMPORTANTE

Los datos podrán ser consultados por aquellos que mantengan una relación contractual con el afectado y los que vayan a celebrar contratos de crédito al consumo y crédito inmobiliario.

SANCIONES DE LA AEPD

Sancionado al propietario de tres páginas online por no informar debidamente a los internautas

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00542-2021.pdf se sanciona al propietario de tres páginas web por informar indebidamente a los usuarios y no recoger el consentimiento para el tratamiento de los datos personales.

La reclamación fue interpuesta por una sociedad jurídica que reclamaba ante la AEPD la inexistencia de información en las tres páginas web del reclamado. En los formularios de contacto no había ninguna referencia sobre la propiedad de las webs.

La AEPD en su fase de investigación, constató el funcionamiento de los formularios. A través del enlace "contacto", la web redirige al usuario a una nueva página donde se pueden introducir datos personales como el nombre o el correo electrónico. Una vez introducidos los datos personales en el formulario, no existe casilla de aceptación de la política de privacidad. Se pueden enviar los datos personales directamente haciendo click en "enviar". **En el apartado de los formularios tampoco existe ningún enlace que redirija al usuario a la "Política de Privacidad".**

El titular de las tres páginas web fue sancionado con 2.000€ por no recoger el consentimiento mediante una casilla de aceptación y, además, por no informar debidamente. **En la "Política de Privacidad" no aparecía ningún dato relacionado con la identidad del responsable del tratamiento.**

Cada vez hay una mayor conciencia entre los interesados en la protección de sus datos personales.

IMPORTANTE

El responsable debe cumplir con el principio de Transparencia e información. Facilitará al interesado toda la información básica del tratamiento de sus datos y le indicará el modo de acceder al resto información.

LA AEPD ACLARA

Consejos de la AEPD para proteger nuestros datos en vacaciones

En la página web de la AEPD en su apartado de guías, herramientas e infografías, encontramos una infografía con consejos para proteger nuestros datos personales en esta época estival.

Durante las vacaciones de verano, no se puede bajar la guardia y hay que seguir siendo activos en la protección de datos. En esta infografía, la AEPD nos da algunos consejos de cómo afrontar situaciones de riesgo.

1. Piensa dos veces antes de compartir una foto o vídeo: Los códigos de billetes y tarjetas de embarque contienen datos personales y del viaje.
2. Evita decir dónde estás: Compartir en internet fotografías de viajes o geolocalización a través de una aplicación puede facilitar información a los delincuentes.
3. Desconfía de las Wifis abiertas o públicas: Las redes abiertas pueden ser utilizadas por ciberdelincuentes para robarte datos personales y contraseñas. No intercambies información sensible ni te conectes a tu servicio de banca.
4. Adelántate al robo o pérdida de tus dispositivos: La AEPD nos recomienda que hagamos una copia de seguridad de la información que almacenamos, así como, añadir un sistema de clave o patrón para bloquear los dispositivos.

IMPORTANTE

Si tuvieras que conectarte desde un ordenador público de un hotel o un locutorio, utiliza la navegación privada del navegador y no guardes contraseñas en el dispositivo compartido.

ACTUALIDAD LOPD

La AEPD publica una guía dirigida a los profesionales del sector sanitario

Fuente: AEPD

(Madrid, 22 de junio de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado la 'Guía para profesionales del sector sanitario', un documento que **responde a las dudas más frecuentes que pueden surgir a los profesionales que intervienen en la prestación de servicios sanitarios** y que tiene por objeto facilitar el cumplimiento de la normativa de protección de datos y la garantía de los derechos de los usuarios de estos servicios.

La Guía está dirigida principalmente a los profesionales sanitarios **que desempeñen su actividad a título individual**, aunque sus orientaciones pueden resultar de utilidad para aquellos que trabajen **en el marco de establecimientos sanitarios**. Los datos de salud tienen la condición de categorías especiales y, por tanto, cuentan con un régimen reforzado de protección. En 2021 la AEPD registró 680 reclamaciones vinculadas a la sanidad, lo que representa un 75% más que en 2020, según datos de la última Memoria anual.

El documento aborda cuestiones que se plantean a menudo en este sector, como la legitimación para tratar datos de salud; quién puede acceder a la historia clínica y en qué casos; la responsabilidad y obligaciones derivadas de estos tratamientos, así como la gestión de los derechos de los pacientes o de las situaciones que puedan implicar comunicación de datos a terceros.

La Guía comienza analizando el **concepto de datos de salud**, así como la posición jurídica de quienes intervienen en la prestación de servicios sanitarios, como responsables del tratamiento o como prestadores de servicios a dichos responsables. Asimismo, se detallan las **bases jurídicas** para el tratamiento de los datos, diferenciando las específicas de los derechos de autonomía del paciente y las del tratamiento de datos personales, que incluyen otras bases de legitimación sin necesidad de consentimiento. En este apartado se abordan, entre otros interrogantes, si es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para tratar sus datos personales o podría ampararse en otras bases jurídicas; si pueden tratarse posteriormente los datos con finalidades distintas a la asistencia sanitaria o si puede constar el nombre y apellido de los profesionales en las tarjetas identificativas.

Por otro lado, el acceso a la historia clínica constituye un aspecto esencial de la asistencia sanitaria, por lo que la guía facilita **orientaciones** sobre quiénes pueden acceder a la misma para las distintas finalidades para las que están legitimados –profesionales sanitarios, residentes, centros sociosanitarios o centros privados concertados– así como los riesgos y responsabilidades en que pueden incurrir quienes accedan ilícitamente.

Puede ver más información en el siguiente enlace

Guía para profesionales del sector sanitario

EL PROFESIONAL RESPONDE

La seguridad en la nube: conceptos básicos(I)

Hoy en día, el término de *cloud computing* está presente en nuestro ámbito profesional. Se trata de una nueva forma de prestación de los servicios de tratamiento de la información. Podemos contratar diferentes servicios en la nube, como, por ejemplo, servidores de ficheros, *backup*, alojamiento, web, CRM y ERP, videoconferencias, etc. La nube nos permite utilizar recursos que facilitan la conexión desde cualquier lugar, la unificación de recursos y una implementación rápida.

En este entorno, la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube. El proveedor del servicio puede encontrarse, en cualquier lugar del mundo, y proporcionar los servicios *cloud* a través de, por ejemplo, prácticas de deslocalización, movilidad o realizando subcontrataciones adicionales. **Así, en este caso, el contratista puede desconocer la localización concreta de sus datos y, por lo tanto, no disponer del control directo de acceso y portabilidad. Todo esto nos lleva a tener que ser rigurosos en el momento de la contratación de un servicio de este tipo.** Para elegir aquel proveedor que cumpla con toda la legislación, y en especial, con la normativa en protección de datos y seguridad, son muchos los aspectos a tener en cuenta en este nuevo entorno *cloud*, que iremos analizando en los siguientes boletines.

IMPORTANTE

La empresa que utilice la nube como recurso debe tener una política de clasificación de información que indique que tipo puede subir al *cloud.*