PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)
RGPD-LOPD en la empresa
www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 09/24

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamiento de categorías especiales de datos (I)

Contenido

Los datos personales considerados de categorías especiales son aquellos que revelan información particularmente sensible sobre las personas:

1. **Origen racial o étnico**: Información que revela la raza, etnia, o nacionalidad de una persona.
2. **Opiniones políticas**: Datos relacionados con la afiliación o actividades políticas.
3. **Convicciones religiosas o filosóficas**: Creencias religiosas, filosóficas o espirituales de una persona.
4. **Afiliación sindical**: Información sobre la pertenencia a un sindicato.
5. **Datos genéticos**: Información relacionada con las características genéticas de una persona, como resultados de pruebas genéticas.
6. **Datos biométricos**: Características físicas, fisiológicas o de comportamiento que permiten la identificación única de una persona, como huellas dactilares, reconocimiento facial o iris.
7. **Datos de salud**: Información relacionada con la salud física o mental de una persona, incluidos historiales médicos o diagnósticos.
8. **Vida sexual u orientación sexual**: Datos sobre la vida sexual, prácticas sexuales, o preferencias sexuales de una persona.

IMPORTANTE

El artículo 9 del RGPD establece una protección para los datos sensibles, garantizando que solo se traten con estrictas condiciones legales.

SANCIONES DE LA AEPD

Sancionada una empresa por enviar las nóminas de todo su personal laboral al correo de una trabajadora

En la resolución de la AEPD https://www.aepd.es/documento/ps-00238-2024.pdf se sanciona con 270.000€ a la empresa reclamada por enviar un correo a una trabajadora con un documento adjunto en *PDF* en el que se incluía su nómina y la del resto de los 446 empleados/as de la plantilla.

En el proceso de investigación la AEPD requiere a la empresa reclamada la motivación de por qué no fue notificada la brecha, instándola a que realice la comunicación.

Se sanciona a la entidad con 300.000€ por no haber garantizado la confidencialidad de los datos, ya que se remitió un correo con un documento PDF con los datos de las nóminas de todos los empleados/as.

Como agravante se estimó que enviar este tipo de documentos con los datos de nombre, dirección, DNI, número de Seguridad Social, número de la cuenta bancaria y salario, entre otros, por correo electrónico, supone una vulnerabilidad en materia de seguridad, ya que, al no estar cifrados los datos, cualquier atacante podría acceder a esos datos en tránsito.

Se estableció también una sanción de 150.000€ por no haber aplicado las medidas de seguridad técnicas y organizativas para garantizar la seguridad de los datos personales. La actuación negligente del trabajador de la entidad reclamada no le exime de responsabilidad.

Como factor de graduación en calidad de agravante en la sanción se tuvo en cuenta la vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

IMPORTANTE

Se deben proteger especialmente aquellos datos cuya difusión provoque daños y perjuicios inmediatos, por ejemplo, datos de localización o financieros.

LA AEPD ACLARA

Neurodatos y neurotecnología: privacidad y protección de datos personales (II)

En el apartado de Innovación y Tecnología la AEPD expone información relevante en materia de protección de datos, centrándose en este caso en los neurodatos.

Las interfaces cerebro-computador permiten captar la actividad cerebral, que depende de factores internos y externos al individuo y de su base genética. Estas tecnologías recogen neurodatos, los cuales, al estar asociados a personas identificables, se consideran datos personales. Además, los neurodatos pueden ser utilizados para perfilado, inferencia de nuevos datos, y hasta para la modificación del comportamiento o autenticación biométrica. Con el uso de inteligencia artificial, estos datos pueden revelar información sobre pensamientos, sentimientos y salud, e incluso predecir comportamientos futuros.

A diferencia de la información genética, la neurotecnología no solo recoge datos en tiempo real, sino que también puede generar estímulos neurológicos que alteren la actividad cerebral y, por tanto, el comportamiento de la persona, tanto a corto como a largo plazo.

En resumen, los neurodatos, según un concepto amplio adoptado por el RGPD, son datos personales, y en algunos casos, pueden ser considerados especialmente sensibles. Esta tecnología abre nuevas posibilidades e importantes retos en cuanto a la protección de la privacidad y los derechos individuales.

IMPORTANTE

Los datos genéticos considerados datos de categoría especial por el RGPD, y los datos cerebrales o neurodatos comparten características y cualidades. El cerebro será un identificador tan único como una huella dactilar

ACTUALIDAD LOPD

Métodos probabilísticos y cumplimiento del RGPD

Fuente: AEPD

(2 de septiembre de 2024). El uso de métodos probabilísticos para tratar datos personales puede conducir al incumplimiento del RGPD, especialmente si se tienen en cuenta el principio de exactitud y el cumplimiento de los requisitos para superar con éxito una prueba de idoneidad. Esto no significa necesariamente que estos métodos no se puedan utilizar en absoluto: una operación probabilística podría ser una de las operaciones incluidas en un tratamiento de datos que cumpla los requisitos de exactitud e idoneidad. En estas situaciones, es fundamental que el tratamiento de datos personales ejecute las operaciones necesarias para detectar y gestionar las imprecisiones o errores producidos por las operaciones probabilísticas en casos concretos. No se debe confundir la exactitud de una operación dentro de un tratamiento de datos con la exactitud del tratamiento de datos en sí, que debe permitirle cumplir la finalidad explícita que se haya especificado para dicho tratamiento.

En los últimos años hemos sido testigos de una transformación sin precedentes en los campos de la estadística, el aprendizaje automático (*machine learning*, ML) y la inteligencia artificial (IA). Estos avances han sido impulsados principalmente por el desarrollo y la aplicación de métodos probabilísticos, que han demostrado ser herramientas poderosas para procesar grandes cantidades de datos. Estos métodos permiten que los modelos de ML e IA aprendan de los datos y mejoren con el tiempo, adaptándose a patrones complejos y a menudo cambiantes.

La capacidad de estos métodos para manejar la incertidumbre y hacer predicciones a partir de los datos disponibles ha llevado a su adopción generalizada en una gran variedad de dominios de aplicación. Los métodos probabilísticos son la base de muchos de los servicios y aplicaciones digitales actuales, desde los sistemas de recomendación que sugieren productos o contenidos relevantes hasta las soluciones de segmentación que agrupan a los usuarios en función de sus características o preferencias predichas. Los responsables de tratamiento deben tener cuidado al considerar los umbrales de error para los métodos probabilísticos.

Puede ver más información en el siguiente enlace:

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Cómo afecta a las empresas el virus de *ransomware* (I)

Uno de los principales virus que está en constante evolución es el *ransomware.* A lo largo de este boletín y siguientes profundizaremos en su evolución y buenas prácticas para protegernos. Su rápido crecimiento está relacionado con los avances de criptografía y el elevado número de dispositivos conectados a Internet. El *ransomware* afecta a cualquier usuario, negocio, y servicios críticos como hospitales o centrales energéticas.

El objetivo del *ransomware* es bloquear el acceso al dispositivo afectado o a parte de la información contenida en dicho dispositivo, y solicitar un rescate a cambio de su desbloqueo. El nombre procede de la palabra *"ransom"* que significa rescate y *"ware"* cuyo significado es producto en inglés. Así, cuando el ciberdelincuente cifra los datos pide un rescate. A cambio del pago, a la empresa se la promete facilitar un mecanismo para desbloquear el ordenador. En este sentido, la recomendación es no pagar el rescate para evitar este tipo de amenazas. **El pago en criptodivisas (moneda virtual) permite que el ciberdelincuente reciba el rescate de forma anónima, dificultando su seguimiento por parte de la policía.**

El ataque de ransomware no solo bloquea los datos, sino que también crea una brecha de seguridad al exponer información en Internet, lo que genera multas por incumplir el RGPD.

IMPORTANTE

No es aconsejable pagar el rescate, ya que no asegura recuperar el acceso a los datos. Además, podrías ser víctima de nuevos ataques y recibir demandas de sumas mayores.