PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 07/21

EL RGPD UE 2016/679 EN APLICACIÓN

Nuevas cláusulas contractuales tipo de la Comisión Europea

El RGPD permite realizar la transferencia de datos personales a un tercer país mediante garantías adecuadas. Una de ellas es la utilización de cláusulas tipo de protección de datos adoptadas por la Comisión. Se han aprobado recientemente unas nuevas cláusulas tipo, **derogando la Decisión 2001/497/CE y la Decisión 2010/87/UE que se venían utilizando actualmente.**

En este sentido, si se hubiera celebrado algún contrato de acceso a datos con un encargado o responsable del tratamiento ubicado fuera de la Unión Europea tendremos en cuenta el siguiente plazo de validez:

- Ambas Decisiones se derogan a partir del día 27 de septiembre de 2021.
- Los contratos celebrados con fecha anterior al 27 de septiembre de 2021 son válidos hasta el día 27 de septiembre de 2022, siempre y cuando las operaciones de tratamiento que sean objeto del contrato permanezcan inalteradas.

El nuevo conjunto de cláusulas contractuales recoge diferentes tipos de transferencias:

Modulo 1: de responsable a responsable
Modulo 2: de responsable a encargado
Modulo 3: de encargado a encargado
Modulo 4: de encargado a responsable

Contenido

IMPORTANTE

Seguirá siendo necesario que el exportador, ayudado por el importador, analice el nivel de protección proporcionado.

SANCIONES DE LA AEPD

Una inmobiliaria es sancionada con 2.000 euros por no facilitar la información en protección de datos

En la Resolución de la AEPD https://www.aepd.es/es/documento/ps-00177-2021.pdf , se sanciona a una inmobiliaria por no informar debidamente al cliente.

Es una infracción considera muy grave la omisión del deber de informar al afectado acerca de su tratamiento de datos.

La reclamada manifiesta en su escrito que en el momento de realizar la señal para la adquisición de la vivienda no se le entregó ninguna información en materia de protección de datos sobre el tratamiento de los datos personales facilitados.

Durante el periodo de alegaciones, se solicita a la inmobiliaria reclamada que presentara pruebas de su adecuación a la normativa de protección de datos. **En la documentación que ésta envía a la AEPD para demostrar su cumplimiento se hacía alusión a la antigua ley orgánica de protección de datos 15/1999.** Por lo tanto, no cumple con las exigencias de información que se recogen en el artículo 13 del RGPD.

En este caso, para graduar la sanción se atendieron a los siguientes criterios:

- La reclamada no tiene infracciones previas.
- No ha obtenido beneficios directos.
- La reclamada no tiene la consideración de gran empresa.

La sanción ascendió a 2.000 euros. La reclamada se acogió a las dos reducciones posibles, por reconocimiento de responsabilidad y pronto pago, siendo finalmente sancionada con 1.600 euros.

IMPORTANTE

Los ciudadanos están cada vez más concienciados con el ejercicio de sus derechos para proteger sus datos personales frente al incumplimiento del responsable.

LA AEPD ACLARA

El deber de informar y otras medidas de Responsabilidad proactiva en APPS para dispositivos móviles

La AEPD publicó una nota técnica orientada al deber de informar y otras medidas de responsabilidad proactiva en apps, destinada a las entidades involucradas en el desarrollo, distribución y explotación de apps para móviles.

Algunas de las directrices que encontramos en esta nota técnica son las siguientes:

1. **La política de privacidad, con toda la información del art.13 y art.14 del RGPD, debe estar disponible tanto en la aplicación como en la tienda de aplicaciones,** y no existir discrepancias entre ellas.

2. El acceso a la política de privacidad se hará de forma sencilla y el número de interacciones, a ser posible será un máximo de dos clics.

3. **El responsable tiene que identificarse claramente en la política de privacidad.** Si estuviera establecido fuera de la UE es necesario que designe un representante.

4. **El lenguaje utilizado será de acuerdo con su nivel de conocimiento y edad.**

5. **Informar sobre la gestión de permisos para el acceso a datos y recursos y la extensión de los mismos.**

6. Cuando sea necesario solicitar el consentimiento este será granular, de forma selectiva e independiente para los distintos tratamientos y finalidades.

7. **Hay que incluir información concreta de los periodos de retención de los datos y el destino final.**

IMPORTANTE

Los responsables de tratamiento que encarguen el desarrollo, y/o explotación de aplicaciones a terceras partes deben suscribir un contrato de acceso a datos.

ACTUALIDAD LOPD

Nueva guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto

Fuente: AEPD

(Madrid, 29 de junio de 2021). La Agencia Española de Protección de Datos (AEPD) ha presentado hoy la guía 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales', un documento que incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos.

El documento, **dirigido a responsables, encargados de tratamientos y delegados de protección de datos (DPD)**, ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

El RGPD establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de establecer las medidas que sean necesarias para **garantizar los derechos y libertades de las personas**. Además, en aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el Reglamento dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos (EIPD) para mitigar esos riesgos.

La guía presentada hoy es **aplicable a cualquier tratamiento, con independencia de su nivel de riesgo**. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la EIPD y, en su caso, la consulta previa a la que se refiere el artículo 36 del RGPD, que establece que el responsable debe consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto sigue ofreciendo un riesgo residual alto o muy alto tras haber tomado medidas.

La Guía consta de tres apartados: el primero contiene una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades; el segundo incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo, y el último está enfocado en los casos en los sea preciso realizar una EIPD, con las orientaciones necesarias para llevarla a cabo.

Puede ver más información en el siguiente enlace

Guía para la gestión del riesgo y evaluación de impacto en tratamientos de datos personales

EL PROFESIONAL RESPONDE

Ransomware, la principal amenaza para las empresas (II)

En el anterior boletín hacíamos referencia a la definición de *ransomware* y cómo se podría propagar en la empresa. **En esta ocasión, definiremos los principales tipos de *ransomware* de menor a mayor importancia:**

1. ***Hoax ransomware*: simula el cifrado** utilizando técnicas de ingeniería social para extorsionar al usuario.

2. ***Scareware*: es un señuelo de falso *software***. Suele aparecer en forma de anuncio molesto emergente informando de una supuesta infección por virus, para ello te sugiere que descargues un programa de limpieza que es casi siempre un malware. El anuncio no suele suponer una amenaza, pero sí los enlaces que contiene.

3. **Bloqueadores de pantalla: impiden el uso del dispositivo mostrando una ventana que ocupa toda la pantalla y no se permite cerrar, suelen aparecer mensajes informando del cifrado de archivos y el procedimiento para recuperarlos.** Aunque no es cierto, ya que solo se ha producido el bloqueo, o bien simulan un mensaje de las fuerzas de seguridad indicando que se han detectado actividades ilegales y por ello han de pagar un rescate para desbloquearlo.

4. ***Ransomware* de cifrado; es el más peligroso.** A veces utilizan un tipo de cifrado llamado *wiper* que no devuelve el acceso a los archivos, sino que los elimina.

5. ***Doxware*: amenaza al usuario con hacer públicos los datos personales extraídos.**

IMPORTANTE

Los avances en la complejidad de los algoritmos de cifrado permiten cifrar tanto el equipo infectado como los servicios en la nube que estén logueados al ordenador infectado.