PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 12/21

EL RGPD UE 2016/679 EN APLICACIÓN

¿Qué es la Lista Robinson?

Contenido

En el art. 23 de nuestra LOPDGDD están regulados los sistemas de exclusión publicitaria. **A través de estos sistemas se podrá realizar el tratamiento de los datos personales de aquellos interesados que hayan manifestado su negativa u oposición a recibir comunicaciones comerciales.**

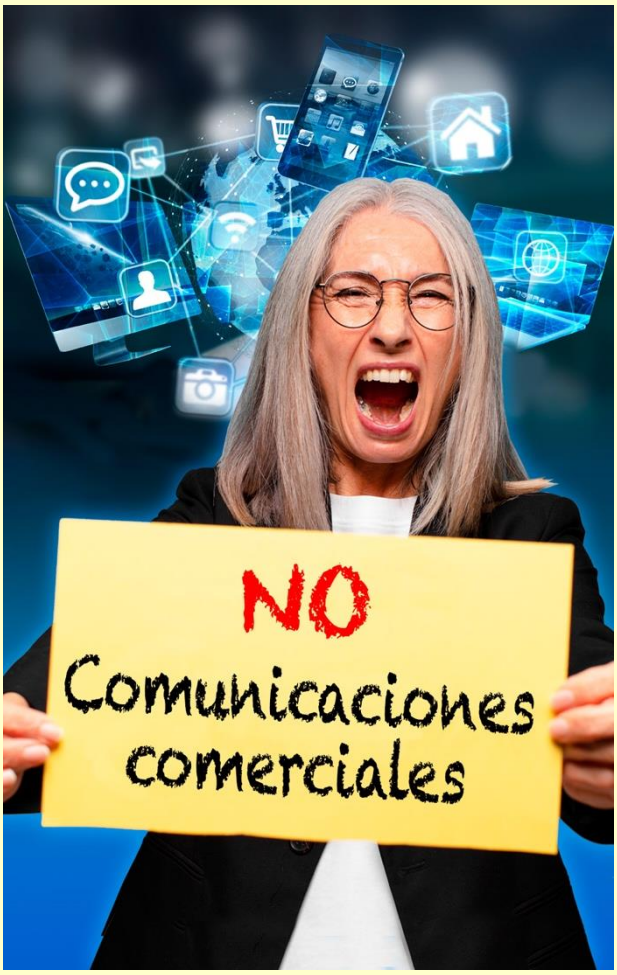
Las autoridades de control competentes harán pública en su sede electrónica una relación de los sistemas creados a tal efecto. Actualmente, solamente existe un fichero de exclusión publicitaria llamado *Lista Robinson*. Este fichero está gestionado por la Asociación Española de Economía Digital (ADIGITAL).

Los interesados pueden solicitar no recibir publicidad tanto por vía postal, vía telefónica, correo electrónico u otro medio. Estos son los principales requisitos a tener en cuenta para que la inscripción sea válida:

- No haber sido cliente de la entidad que envía la publicidad.

-No haber dado un consentimiento previo para recibir comunicaciones comerciales.

La inscripción empieza a ser eficaz a partir del segundo mes desde la fecha en que se registren los datos, por eso, es posible que durante este plazo se puedan seguir recibiendo comunicaciones comerciales.



IMPORTANTE

Las empresas que realicen comunicaciones de mercadotecnia directa tienen que consultar la Lista *Robinson* y probar que han realizado la consulta.

SANCIONES DE LA AEPD

Entidad inmobiliaria sancionada con 10.000 euros por no contestar a un derecho de supresión

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00488-2020.pdf se sanciona a una entidad inmobiliaria por no atender debidamente el derecho de supresión de sus datos personales.

La parte reclamante manifiesta que la empresa reclamada había contactado con él telefónicamente de manera reiterada para ofrecerle sus servicios inmobiliarios. En varias ocasiones les solicitó que borraran sus datos.

En el escrito se adjuntan pruebas de los mensajes y llamadas recibidas en su teléfono. En uno de los mensajes le indican que "no volverían a contactar con ella", no siendo así, ya que continuó recibiéndolos.

La AEPD en esta reclamación no está valorando los mecanismos para solicitar la supresión de los datos, sino la falta de diligencia debida por parte de la entidad ante la solicitud de la supresión de los datos personales de la afectada.

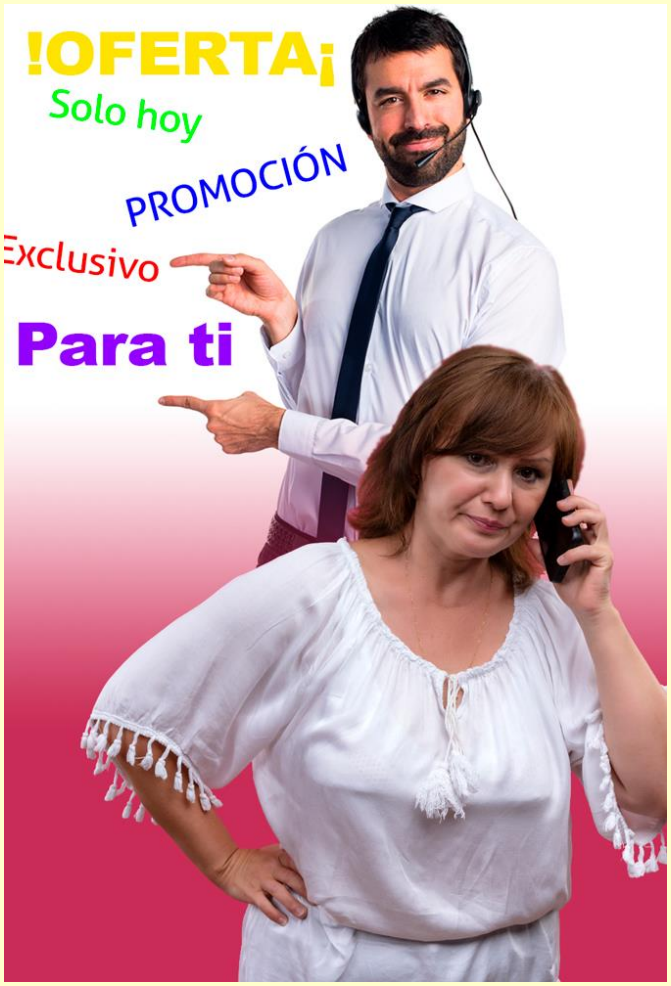
Se le aplican los siguientes criterios de atenuación:

- Medidas tomadas por el responsable. No constan nuevos tratamientos de datos ilícitos por parte de la entidad.

- Circunstancias actuales de la empresa influenciadas por la situación social.

- Inexistencia de beneficios obtenidos como consecuencia de la comisión de la infracción.

Los agravantes que se tuvieron en cuenta fueron la duración de la infracción y la falta de diligencia de la entidad.



IMPORTANTE

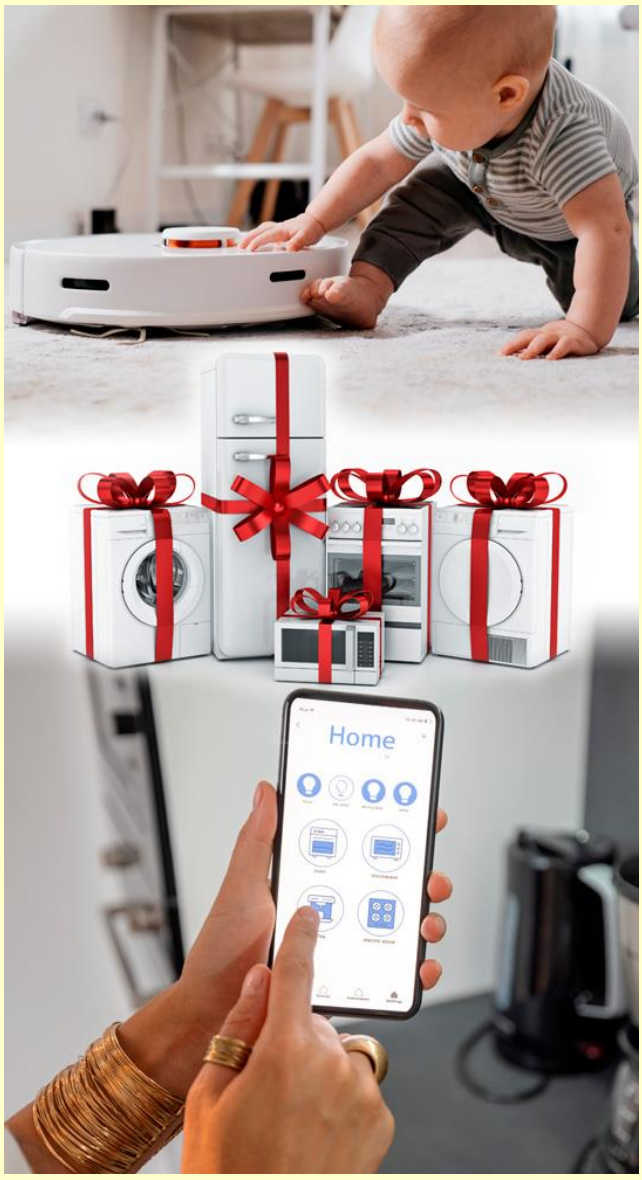
El responsable del tratamiento tiene que contestar a los derechos solicitados sin dilación indebida, y, en cualquier caso, en el plazo de un mes a partir de la recepción.

LA AEPD ACLARA

Fichas prácticas: recomendaciones para el uso seguro del Internet de la Cosas

En el apartado de Guías y Herramientas de la AEPD nos encontramos con una serie de fichas interesantes que deben conocerse.

En esta ocasión, y siendo el mes de diciembre un mes propicio para regalar y recibir regalos tecnológicos y dispositivos inteligentes, la AEPD nos da las siguientes recomendaciones para mejorar la privacidad:



1ª El derecho fundamental de la protección de datos depende de ti: no se deben dar más datos de los necesarios. Revisa la información que ofrece el fabricante y consulta a su DPD.

2ª Elige fabricantes o proveedores que ofrezcan garantías de privacidad.

3ª Antes de adquirir el producto revisa las políticas de privacidad, la forma de ejercer los derechos, incluido el derecho a la portabilidad de datos. Que tipos de datos van a ser tratados y con qué finalidades. Si los datos se van a comunicar a terceros.

4ª Revisa y configura las preferencias y opciones de privacidad y seguridad. Debes poder otorgar consentimiento o expresar oposición a las distintas finalidades.

5ª Comprueba que el dispositivo se puede desconectar cuando no se está usando, y utiliza el modo que permite deshabilitar la captura de datos.

6ª Cuando dejes de utilizarlo definitivamente, no mantengas conectado a Internet el dispositivo obsoleto. Borra los datos antes de venderlo o reciclarlo.

IMPORTANTE

Revisar periódicamente las opciones de privacidad y seguridad e instalar las actualizaciones de seguridad disponibles.

ACTUALIDAD LOPD

Protección de la privacidad en el entorno laboral de las víctimas de acoso y mujeres supervivientes a la violencia de género

Fuente: AEPD

Entre los casos de acoso en el entorno laboral se encuentran conductas como la difusión de vídeos de carácter sexual enviados a través de aplicaciones de mensajería instantánea entre personas del trabajo, que pueden llegar incluso a hacerse virales, con los graves efectos que esto puede conllevar. Por ello, es necesario recordar que la difusión de contenidos sensibles sin consentimiento, así como la adopción o no de medidas ante esta situación, puede tener consecuencias administrativas, disciplinarias, civiles y penales para empresas y trabajadores.

Las empresas están obligadas a prevenir e identificar las prácticas de acoso y, en su caso, erradicar estas situaciones de sus organizaciones. En este sentido es recomendable la elaboración de protocolos con medidas a adoptar, entre las que deben incluirse las específicas para la protección de datos de carácter personal.

Canal Prioritario y Pacto Digital de la AEPD
Dentro de los compromisos recogidos en su Marco de Actuación de Responsabilidad Social, la Agencia puso en marcha el Canal Prioritario para la retirada urgente de contenidos sexuales o violentos publicados sin consentimiento en Internet. Una herramienta de gran utilidad para las personas afectadas en primer término, pero también para las empresas. Más de 300 organizaciones firmantes del Pacto Digital de la AEPD ya la difunden entre sus empleados y la incluyen dentro de sus protocolos de actuación ante situaciones de acoso.

Consideraciones ante supuestos de acoso
Los datos personales relativos a las víctimas de acoso en el trabajo y de las mujeres supervivientes de la violencia de género, en particular su identidad, tienen, con carácter general, la consideración de categorías especiales de datos personales y, en todo caso, son datos sensibles que exigen una protección reforzada por parte de las empresas y organizaciones en las que trabajan.

En lo referente al **registro de jornada obligatorio**, la Agencia recomienda que se adopte el sistema menos invasivo posible y este no puede ser de acceso público ni estar situado en un lugar visible. Asimismo, los datos de ese registro no pueden utilizarse para finalidades distintas al control de la jornada de trabajo, como comprobar la ubicación. Es el ejemplo de una persona trabajadora itinerante cuyo registro de jornada se realiza por geolocalización. La finalidad ese registro es comprobar cuándo comienza y finaliza su tiempo de trabajo, pero no verificar dónde se encuentra en cada momento, ya que el tratamiento de datos de geolocalización requiere de una base jurídica específica.

Puede ver más información en el siguiente enlace

La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones

EL PROFESIONAL RESPONDE

Acciones para evitar pérdidas cuando sufrimos un incidente de seguridad

Una de las principales recomendaciones a seguir es que no se pague el rescate, puesto que, no garantiza que recuperemos la información y una vez hecho el pago nos lo pueden volver a solicitar.

Poner en marcha el plan de respuesta de incidentes es otra de las recomendaciones que nos ayudará a minimizar los daños. En el plan de respuesta se habrán delimitado las pautas que se deben seguir, una de ellas, es la recogida de evidencias para una posible denuncia.

Estas son las cinco acciones que seguiremos para conseguir recuperar la actividad:

- Aislar el equipo de la red; con ello evitaremos que el ciberataque se propague a otros dispositivos.

- Cambiar todas las contraseñas; éstas han de ser robustas y únicas para cada servicio. Una vez eliminado el *ransomware* hay que volver a cambiarlas.

- Clonar el disco duro; se podrá mantener el dispositivo original para recuperar los datos sobre el clon. Se puede extraer el disco duro afectado y conservarlo como prueba.

- Desinfección del disco clonado; se tiene que utilizar un antivirus o *antimalware* actualizado.

- Recuperar y restaurar los equipos con el *software* original cuando sea posible, sino se arrancaría en modo seguro para poder recuperar la copia de seguridad.

IMPORTANTE

En esta página puedes encontrar herramientas de ayuda para descifrar el equipo
www.nomoreransom.org