Boletín 02/19

LOPD EN LA EMPRESA

ACM gabinete empresarial

TF TafelConsultores

EL RGPD UE 2016/679 EN APLICACIÓN

# El principio de responsabilidad proactiva

**El responsable del tratamiento tiene que cumplir con lo dispuesto en la normativa de protección de datos de una forma consciente y activa**, es decir, aplicando el principio de responsabilidad proactiva que se recoge en el art.5.2 del RGPD.

Con la incorporación de este principio se pretende que, tanto el responsable como el encargado, **no solamente no incumplan la normativa, sino que, al contrario, éstos deben aplicar las medidas más oportunas y eficaces para el tratamiento y, que además sean capaz de demostrarlas.**

**Lo que podemos hacer como responsables y encargados de tratamiento para demostrar la conformidad y cumplimiento del RGPD es seguir las líneas de actuación que nos marca el RGPD y la LOPDPGDD:**

1º Mantener un Registro de actividades de tratamiento.

2º Proteger los datos desde el diseño y por defecto; reduciendo al máximo el tratamiento de los datos personales.

3º Analizar los riesgos para aplicar medidas técnicas y organizativas eficaces.

4º Realizar Evaluaciones de impacto.

5º Notificar Violaciones de seguridad de los datos.

6º Nombrar Delegados de protección de datos.

## Contenido



**IMPORTANTE**

Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán mecanismos de certificación, sellos y marcas de protección de datos, a los que responsables y encargados podrán adherirse para demostrar su cumplimiento.

SANCIONES DE LA AEPD

# La entidad CRUZ ROJA ESPAÑOLA sancionada por no cumplir las medidas de seguridad

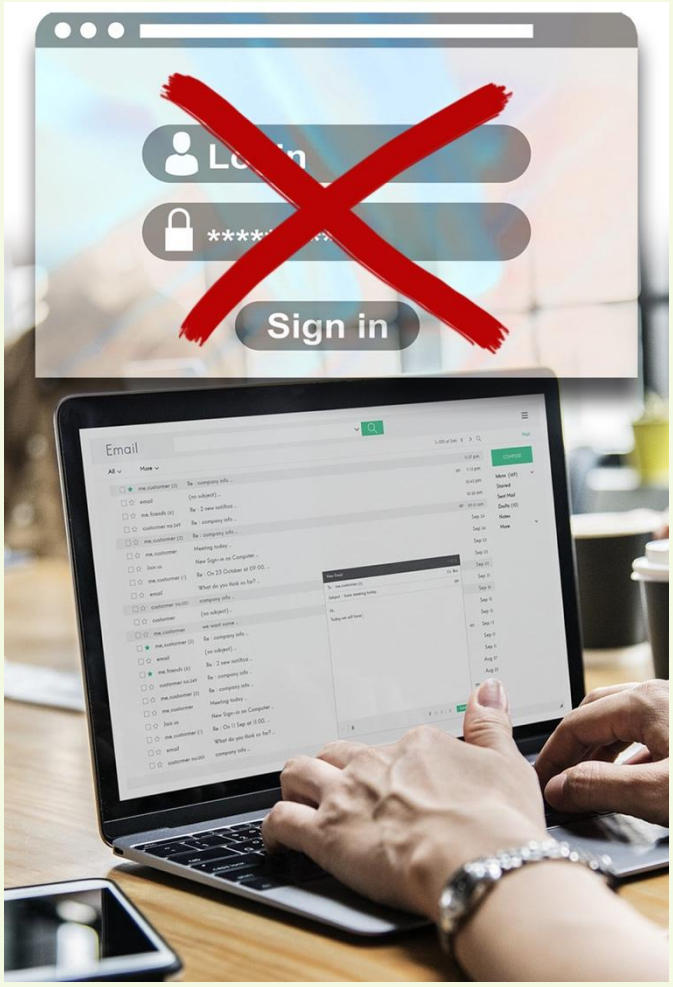
En el procedimiento sancionador PS/00537/2017 instruido por la Agencia Española de Protección de datos, se acuerda sancionar a la entidad **CRUZ ROJA por incumplimiento del artículo 9.1 de la Ley Orgánica de Protección de datos 1999, en el que se dice que: "El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado (...)."**

La denunciante expone que, accediendo a la web***URL.1 y tecleando un nombre al azar en el buscador de la parte superior derecha, **el sistema refleja nombres y apellidos de la base de datos, incluso, en algunos casos, sin necesidad de estar autenticado.** Además, cuando se incluye un nombre y apellidos, salen los e-mails de las personas referidas. Se aporta como prueba la impresión de pantalla en la que se reflejan 3 resultados de personas que incluyen tales términos.

Los servicios de inspección de la Agencia, en fase de actuaciones previas, verifican la falta de confidencialidad de la página web, instando a la entidad a que actúe para subsanar el error técnico. La empresa informática que lleva el mantenimiento de la web procede a darle solución en un plazo de dos días.

**La AEPD finalmente cuantificó la sanción en la cantidad de 4.500 euros.**

Se deben tratar los datos para que se garantice una seguridad adecuada de los mismos, evitando su uso no autorizado o ilícito tanto de forma intencionada como accidental.



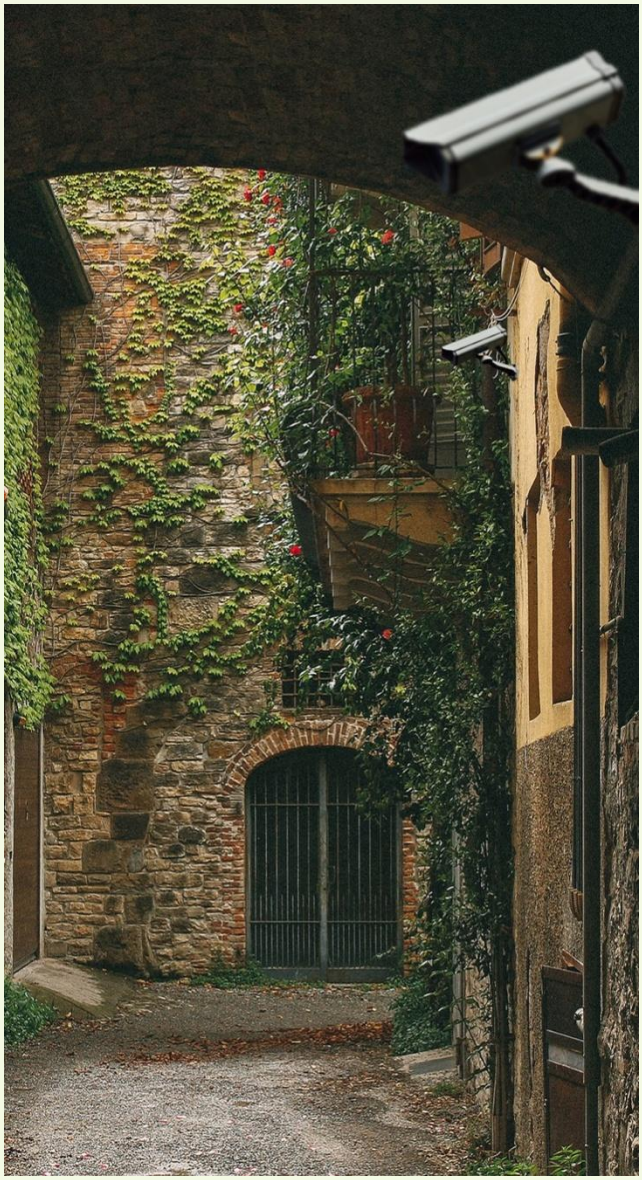

**IMPORTANTE**

Art.72.1.a de la LOPDPGDD: Vulnerar el principio de integridad y confidencialidad de la información supone una Infracción muy grave.

LA AEPD ACLARA

# Videovigilancia y servidumbres de paso en fincas colindantes

El gabinete jurídico ha resuelto la consulta de un ciudadano, planteada al respecto de **la instalación en un inmueble de dos cámaras de videovigilancia, éstas captaban las imágenes en la zona de su patio donde se encuentra la servidumbre de paso a favor de los titulares de la finca colindante.**



El hecho de la colocación de las cámaras ha supuesto muchos enfrentamientos entre los vecinos. Por lo que, con la consulta, se pretende conocer si se está vulnerando o no el derecho a la protección de la imagen.

El consultante adjunta los planos de ubicación de la vivienda y de las cámaras, limitadas a la zona de servidumbre de paso.

**El tratamiento de los datos de esas imágenes no se encuentra excluido del ámbito de aplicación del RGPD, ya que las videocámaras se sitúan en un lugar por el que pueden pasar no solamente los titulares de la vivienda, sino también los titulares de la finca colindante.** Por otro lado, las cámaras son conforme al RGPD puesto que la finalidad legítima de su instalación sería la seguridad del inmueble.

Al propietario de la vivienda, según lo dispuesto en el Código Civil, **la servidumbre de paso no puede suponerle un menoscabo de sus derechos, por lo que está legitimado a su colocación, sin necesidad de recabar el consentimiento de terceros, cumpliendo con los demás requisitos que le exige la normativa.**

**IMPORTANTE**

El responsable siempre tiene que cumplir con el principio de transparencia de la información y el derecho a informar al interesado y además ser capaz de demostrarlo.

ACTUALIDAD LOPD

# La AEPD publica un estudio sobre cómo la huella digital de los dispositivos afecta a la privacidad de los ciudadanos

*Fuente: AEPD*

**(Madrid, 7 de febrero de 2019).** La Agencia Española de Protección de Datos (AEPD) ha publicado el estudio 'Fingerprinting o huella digital del dispositivo', un documento que analiza esta técnica de identificación y rastreo de los usuarios a través de sus dispositivos. Para su realización la Agencia ha analizado más de 14.000 páginas web dirigidas al público español, describiendo las técnicas más utilizadas para realizar ese perfilado. El estudio también incluye las medidas que pueden poner en marcha los usuarios para tratar de evitar este tipo de seguimiento y una serie de recomendaciones a la industria, tanto a los fabricantes y desarrolladores como a las compañías que explotan datos obtenidos a partir de la huella de los dispositivos.

La huella digital del dispositivo es un conjunto de datos extraídos del dispositivo del usuario que permiten individualizar de forma unívoca dicho terminal. Dado que lo habitual es que las personas no compartan sus equipos, individualizar el terminal supone individualizar a la persona que lo utiliza y, en consecuencia, poder realizar un perfil de la misma. El perfilado no se limita a recopilar y analizar los hábitos de navegación o las búsquedas que realiza, sino a extraer geolocalización, datos de configuración del sistema y las aplicaciones, programas instalados, movimientos del ratón, etc. La combinación de esta y otra información detallada en el estudio permite confeccionar una huella digital única del dispositivo que lo singulariza y, por lo tanto, diferencia de forma unívoca a cada usuario en internet.

El estudio afirma, entre otras conclusiones, que con mucha frecuencia se emplean estas técnicas para recoger datos del equipo del usuario sin ofrecerle información y sin solicitarle su consentimiento, y que el conjunto de datos recabados puede ser tan extenso, o enriquecerse de tal forma, que puede llegar a recoger incluso categorías especiales de datos. El documento añade que, en la mayoría de los casos, al usuario no se le proporcionan herramientas para poder evitar de forma efectiva la recogida de datos y no se le ofrecen medios para ejercer los derechos establecidos en el RGPD cuando se recogen o asocian a datos personales.

Puede ver más información en el siguiente enlace:

Estudio Fingerprinting o huella digital del dispositivo.

EL PROFESIONAL RESPONDE

## ¿Que ocurriría si no llevo a cabo un análisis de riesgos adecuado para implantar las medidas más eficaces?

**La respuesta a esta pregunta la encontramos en la recién publicada LOPDPGDD en su art.73** que regula como infracciones graves, entre otras:

**-El tratamiento de los datos personales sin tener en cuenta, los mayores riesgos que podrían producirse,** cuando por ejemplo implique evaluación de aspectos personales o los datos sean objeto de transferencia a terceros países sin nivel de protección.

**-Falta de adopción de medidas técnicas y organizativas que garanticen que solo se tratarán los datos personales necesarios** para los fines específicos.

**-No adoptar aquellas medidas que resulten adecuadas para garantizar el nivel adecuado de seguridad**, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables.

**Para realizar un análisis adecuado de riesgos y así, aplicar las medidas exigidas por la normativa** tenemos que identificar todos los activos involucrados en el tratamiento, analizando las amenazas y vulnerabilidades, **estimando el impacto que causaría aplicando los factores asociados a riesgos para los derechos y libertades del interesado, evaluando la probabilidad de que se materialicen las amenazas identificadas y decidiendo qué riesgos gestionamos y que medidas aplicamos.**


**IMPORTANTE**

**El tratamiento de datos personales sin realizar una previa valoración de los riesgos es una infracción grave,** por eso el responsable y encargado deben calcularlo:
**Nivel de Riesgo= Probabilidad X Impacto.**