Boletín 03/25

LOPD EN LA EMPRESA

Autor: Julio César Miguel Pérez

EL RGPD UE 2016/679 EN APLICACIÓN

Consentimiento específico e informado (II)

El Reglamento General de Protección de Datos (RGPD) exige que el consentimiento sea específico e informado. Para ello, las empresas deben garantizar que los usuarios comprendan claramente el uso de sus datos personales.

Según las Directrices sobre el Consentimiento, del Comité Europeo de Protección de datos cumplir con este principio implica tres aspectos clave. **Primero, la especificación del fin, lo que significa que el tratamiento debe tener un propósito explícito y legítimo sin desviaciones. Segundo, la disociación en las solicitudes de consentimiento, permitiendo a los usuarios aceptar o rechazar cada finalidad de manera independiente. Y tercero, la separación clara entre la información sobre el consentimiento y otros asuntos, detallando qué datos se tratarán para cada fin.**

El consentimiento es válido solo si el interesado tiene un control real y puede aceptarlo o rechazarlo sin consecuencias negativas. El responsable del tratamiento debe garantizar que cumple con los requisitos del RGPD. Si el consentimiento no se obtiene adecuadamente, el interesado pierde su control efectivo y el tratamiento de datos basado en él será ilícito, comprometiendo la legitimación del tratamiento de los datos personales.

Contenido

1. Consentimiento específico e informado (II).
2. Sancionada una empresa por publicar imágenes en sus redes sociales sin consentimiento del interesado.
3. Legitimación para el tratamiento de los datos de salud (I).
4. La AEPD participa en una acción europea para analizar la aplicación del derecho de supresión.
5. ¿Cómo puedo proteger mi dominio *web* ante un *Cybersquatting*? (I).

IMPORTANTE

El responsable del tratamiento debe garantizar que el interesado comprende claramente la finalidad del consentimiento otorgado.

SANCIONES DE LA AEPD

Sancionada una empresa por publicar imágenes en sus redes sociales sin consentimiento del interesado

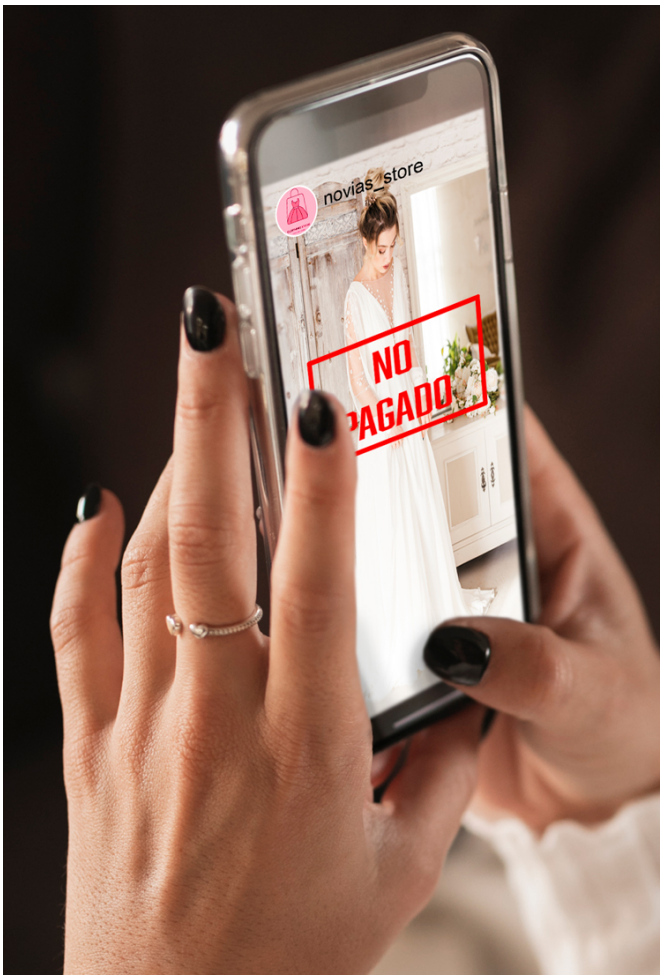
En la resolución de la AEPD https://www.aepd.es/documento/ps-00066-2022.pdf se sanciona con 10.000€ a una empresa textil de diseño de ropa por publicar una imagen en sus redes sociales sin la legitimación adecuada.

La reclamante interpuso una denuncia ante la AEPD indicando que la empresa textil publicó en su red de Instagram una fotografía en la que aparecía vestida con su traje de boda, sin que en ningún momento se le hubiera concedido el consentimiento. **La imagen fue utilizada por la empresa para reclamar el pago del vestido. Aunque la compañía alegó que había pixelado el rostro y que la foto estuvo publicada menos de una hora, la AEPD determinó que la persona seguía siendo identificable.**

La empresa argumentó que la imagen había sido publicada previamente por la propia afectada y que, al ser etiquetada en esa publicación, se entendía como una acción afirmativa y consentimiento tácito. la AEPD concluye en su resolución que el consentimiento debe ser **explícito, libre e informado**, y que la empresa no tenía ninguna base legal para el tratamiento de la imagen.

Asimismo, la AEPD destacó que la falta de pago del vestido no justifica el uso de datos personales sin consentimiento. Estimando como concurrentes en calidad de agravantes la intencionalidad de la publicación, puesto que las fotos fueran eliminadas una vez que se abonaron los costes.

El Reglamento General de Protección de datos (RGPD) en su artículo 83.2 estable las circunstancias agravantes en la imposición de las multas administrativas.



IMPORTANTE

Las empresas deben obtener un consentimiento válido antes de usar datos personales, especialmente cuando van a ser difundidas en redes sociales.

LA AEPD ACLARA

Legitimación para el tratamiento de los datos de salud (I)

La Agencia Española de Protección de Datos (AEPD) ofrece en su sitio web un espacio sobre el tratamiento de los datos en materia de salud.

Según el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), estos datos se consideran de categoría especial, por lo que su tratamiento solo es legítimo bajo condiciones específicas.

En este ámbito, es necesario diferenciar entre el "consentimiento informado" para una actuación sanitaria (que se rige por la legislación sanitaria) y el consentimiento para el tratamiento de los datos personales, incluidos los de salud. Contrario a lo que suele pensarse, el consentimiento del paciente no es siempre obligatorio. El artículo 9.2 del RGPD permite el tratamiento de datos de salud sin consentimiento cuando sea necesario para la asistencia sanitaria, fines de medicina preventiva o laboral o un diagnóstico médico. En estos casos, la legitimación se basa en el interés público en el ámbito de la salud pública o en la relación contractual entre el profesional sanitario y el paciente.

Asimismo, existen otras bases jurídicas, como la protección de intereses vitales, aplicable en situaciones de emergencia donde el paciente no pueda dar su consentimiento. También se permite el tratamiento de datos en procesos judiciales o cuando lo exige la legislación en materia de salud pública.

IMPORTANTE

El tratamiento de datos personales abarca su recopilación, uso, acceso, comunicación, almacenamiento, modificación, cesión a terceros y eliminación.

ACTUALIDAD LOPD

La AEPD participa en una acción europea para analizar la aplicación del derecho de supresión

Fuente: AEPD

(5 de marzo de 2025). La Agencia Española de Protección de Datos (AEPD) participa en una acción europea coordinada para conocer **cómo aplican las organizaciones en la práctica el derecho de supresión** (art. 17, RGPD) que ejercitan los ciudadanos. Esta iniciativa forma parte del marco de actuaciones del Comité Europeo de Protección de Datos (CEPD) de 2025.

El Comité, durante su reunión plenaria de octubre de 2024, seleccionó esta temática debido a que se trata de uno de los derechos del RGPD que los ciudadanos más ejercitan ante los responsables del tratamiento y, a la vez, del que las Autoridades de protección de datos reciben con más frecuencia reclamaciones de la ciudadanía.

Durante este año, 32 Autoridades de Protección de Datos europeas participarán en esta acción. La Agencia, por su parte, analizará las prácticas de **una muestra de responsables del tratamiento, tanto del sector público como privado**, para conocer tanto las buenas prácticas como si existe alguna problemática relacionada con la atención al ejercicio del derecho de supresión.

Los resultados de esta acción s**e analizarán de manera coordinada** y las Autoridades podrán decidir sobre posibles acciones adicionales de supervisión y aplicación en sus respectivos países. Además, los resultados serán agregados, generando **una visión amplia** y permitiendo un seguimiento específico en el ámbito del Espacio Económico Europeo. Finalmente, el Comité publicará un informe sobre el resultado de este análisis una vez concluidas las acciones.

Esta acción es la cuarta iniciativa del Marco de Aplicación Coordinada, entre cuyos objetivos se encuentra la **cooperación entre las autoridades** de protección de datos. Las acciones coordinadas anteriores analizaron

Puede ver información relacionada con otras acciones coordinadas en el siguiente enlace:

Cumplimiento del derecho de acceso por parte de las organizaciones

EL PROFESIONAL RESPONDE

¿Cómo puedo proteger mi dominio *web* ante un *Cybersquatting*? (I)

El *cybersquatting*, o apropiación de nombres de dominio, es una técnica fraudulenta en la que ciberdelincuentes registran dominios similares a marcas legítimas para lucrarse o utilizarlos con fines ilícitos.

Según la Organización Mundial de la Propiedad Intelectual (OMPI), se considera *cybersquatting* cuando el dominio es idéntico o similar a una marca registrada, que el propietario del nombre de dominio fraudulento no tenga derecho o interés legítimo sobre la marca registrada y que se usa con mala fe.

El principio de *"first come, first served"* en Internet permite que el primero en registrar un dominio sea su propietario, lo que facilita este fraude. Los ciberdelincuentes emplean diversas técnicas:

Adición: Se agrega un carácter extra al final del dominio original.

Sustitución: Se sustituye un carácter del dominio por otro diferente.

Similitud visual: Se cambia un carácter por otro que, aunque distinto, parece similar.

Uso de guiones: Se inserta un guion en algún punto del dominio para alterar su estructura.

Intercalado de caracteres: Se introduce un carácter adicional entre el primero y el último del dominio.

Omisión: Se suprime un carácter del nombre de dominio original.

Subdominio: Se registra una parte del dominio real y se complementa con un subdominio.

IMPORTANTE

Podemos recurrir a la vía judicial, respaldada por la Ley de Marcas y de Competencia Desleal. En el caso de dominios.es existe un sistema de resolución extrajudicial de conflictos.