

EL RGPD UE 2016/679 EN APLICACIÓN

Transparencia e información a los interesados

Uno de los pilares básicos en los que se fundamenta el RGPD y nuestra Ley Orgánica de protección de datos y garantía de derechos digitales asegurar una transparencia en la trazabilidad de los datos personales, de forma que de confianza al interesado en el tratamiento de sus datos.

La normativa nos permite cumplir con el deber de informar facilitando una información básica ¿Cuál es el contenido mínimo que debe comprender? Cuando los datos hayan sido facilitados por el propio interesado, el responsable le dará una primera información básica que ha de contener los puntos siguientes recogidos en el art.11 de la LOPD PGDD:

- a) La identidad del responsable y de su representante en su caso.
- b) La finalidad del tratamiento.
- c) La posibilidad de ejercer los derechos en materia de protección de datos.
- d) La elaboración de perfiles en el caso de que se diera esa circunstancia y la posibilidad de oponerse a la adopción de decisiones individuales automatizadas.

En el caso de que los datos no procedieran del interesado, incluiríamos también las categorías de datos objeto del tratamiento y las fuentes de las que proceden los datos.

Contenido

1. Transparencia e información a los interesados.
2. Una página web sancionada por incumplir el deber de informar.
3. Informe del estudio y análisis sobre políticas de privacidad en Internet.
4. Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva.
5. ¿Cómo se tienen que realizar las transferencias de datos a Reino Unido?



IMPORTANTE

En ambos casos debe indicarse una dirección electrónica u otro medio inmediato para acceder de forma sencilla a la información adicional.

SANCIONES DE LA AEPD

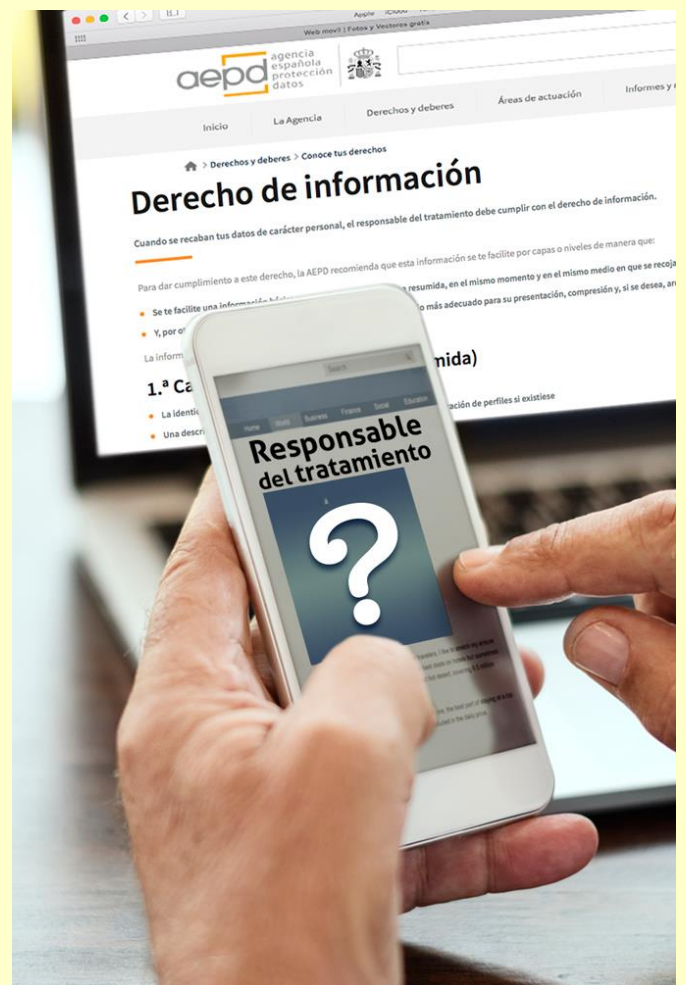
Una página web sancionada por incumplir el deber de informar

En el procedimiento [sancionador https://www.aepd.es/es/documento/ps-00423-2019.pdf](https://www.aepd.es/es/documento/ps-00423-2019.pdf), instruido por la AEPD, se sanciona a la entidad de MYMOVILES EUROPA 2000, S.L.(en adelante el reclamado) por no tener indicado en el aviso legal de su página web la identidad y además, carecer de políticas de privacidad.

El reclamante presentó un escrito ante la AEPD en el que dejaba constancia de que la página web de la entidad reclamada no estaba cumpliendo debidamente con el deber de informar, ya que, a pesar de tener un formulario de recogida de datos no facilitaba ningún documento en el que se informara al interesado sobre quién era el responsable, la finalidad o legitimación del tratamiento, entre otros aspectos que deben de recoger las políticas de privacidad. En el escrito de reclamación se aportaba como prueba la captura de pantalla del aviso legal de la web y de los términos y condiciones de la misma.

La AEPD inició los trámites oportunos de investigación previa para el esclarecimiento de los hechos. En el periodo de alegaciones no recibió contestación alguna por parte del reclamado. La falta de información a los interesados supone un incumplimiento del art.13 del RGPD y del principio de transparencia, ésta se considera una infracción leve. La multa administrativa que finalmente impuso la AEPD alcanzó los 1.500 euros, ya que se aplicaron los criterios de graduación tales como que no se habían obtenido beneficios directos.

La información debe facilitarse en un lenguaje claro y sencillo, de forma concisa, transparente e inteligible, que sea fácil de entender.



IMPORTANTE

El tratamiento de los datos personales implica siempre un deber de informar al interesado, que debe ser facilitado en el momento de la recogida de los datos.

LA AEPD ACLARA

Informe del estudio y análisis sobre políticas de privacidad en Internet

En el siguiente [informe](https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf) elaborado por la AEPD <https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf>, se pretende hacer un estudio del cumplimiento del deber de informar en el entorno online en los sectores de hoteles, transporte, comercio electrónico y seguros. Se han revisado las políticas de privacidad y formularios de recogida de datos personales.

En conclusión, se destaca en el informe que en general, los documentos que se detallan son demasiado extensos y no facilitan al usuario medio que finalice su lectura, además, las bases que legitiman el tratamiento en ocasiones no son adecuadas, ya que se encuadran en un interés legítimo cuando en realidad no es así.

En el informe podemos encontrar una serie de recomendaciones para cumplir debidamente con el principio de transparencia, así entre otros aspectos, se indican pautas para facilitar la información sobre las finalidades del tratamiento. Casi todas las políticas de privacidad analizadas son muy extensas en su redacción y no permiten una fácil lectura. La AEPD, recomienda agrupar las finalidades por categorías, para ello da una serie de ejemplos (*prestación del servicio, comunicaciones comerciales, cumplimiento de obligaciones legales entre otras*). Habría que evitar una enumeración demasiado extensa. Al final del informe, con carácter general, se dan indicaciones para la presentación de la información.



IMPORTANTE

Se recomienda solicitar un consentimiento para cada una de los grupos de finalidades que se sustenten en esa base legítima.

ACTUALIDAD LOPD

Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva



Fuente: [AEPD](#)

El consentimiento debe ser “libre, específico, informado e inequívoco”, tal y como se describe en las [Directrices sobre el consentimiento en el sentido del Reglamento 2016/679](#). Además, debe ofrecerse control al interesado sobre el mismo y darle la posibilidad de aceptar o rechazar los términos bajo los que se presta. El sujeto de datos debe conocer una información mínima, previa a la prestación del consentimiento, que resulta crucial para que pueda tomar una decisión válida y claramente informada. Esta información se establece en el artículo 13 del RGPD, entre la que se encuentra la identidad del responsable, el propósito de cada operación del tratamiento para la que consiente, el tipo de datos que se van a recoger y posteriormente utilizar, si se van tomar o no decisiones basadas únicamente en el tratamiento automatizado de los datos, posibles riesgos si se producen transferencias internacionales y la existencia del derecho a retirar el consentimiento prestado y de los mecanismos para hacerlo.

Esta información muchas veces se presta ‘escondida’ en largas políticas de privacidad asociadas a la aplicación o servicio prestado y que, acumuladas en el tiempo y vinculadas a diferentes tratamientos de distintos responsables, conducen al interesado a la pérdida de control de sus datos, quién los tiene y para qué finalidad, limitando, en consecuencia, ese derecho antes mencionado.

Por otro lado, de acuerdo con artículo 7 del Reglamento, cuando el tratamiento se realice amparado en el consentimiento, este debe poder ser verificable debiendo el responsable ser capaz de poder demostrar que el interesado lo prestó de manera válida. El RGPD no establece un mecanismo en concreto sobre cómo el responsable debe ser capaz de probar que ha obtenido un consentimiento válido, teniendo libertad para implementar la forma de obtención y registro que más se adapte a los procesos de la organización, pero, al menos, debe poder acreditar quién otorgó el consentimiento, cuándo, cómo y para qué, así como la información que se le suministró en el momento de obtenerlo. Esa obligación subsiste en tanto que se siga realizando el tratamiento de los datos personales bajo las condiciones iniciales en que los datos fueron recabados y debe ser verificable en caso de auditoría o inspección.

De ahí que resulte de interés la implementación de herramientas que ofrezcan garantías a los distintos intervinientes en el proceso de consentimiento y les permitan gestionar este en torno al tratamiento de los datos personales que se está realizando.

Puede ver más información en el siguiente enlace

Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva

<https://www.aepd.es/es/prensa-y-comunicacion/blog/recibo-del-consentimiento-una-herramienta-de-transparencia-y>

EL PROFESIONAL RESPONDE

¿Cómo se tienen que realizar las transferencias de datos al Reino Unido?

Tras la salida del Reino Unido de la Unión Europea el pasado 31 de enero, se nos plantea la duda de si es posible seguir realizando las transferencias de datos personales con las mismas garantías que se estaban aplicando hasta ahora.

Según el Acuerdo de Retirada que tendrá vigor hasta el día 31 de diciembre, no se consideran transferencias a terceros países por lo que no será necesario utilizar ninguno de los instrumentos que recoge el RGPD.

Ahora bien, ¿qué ocurrirá cuando finalice el periodo transitorio? Habrá que esperar a los acuerdos que puedan darse en esta materia de protección de datos. En el comunicado emitido por el gobierno, parece que la opción que puede resultar más adecuada y previsible es que la Comisión Europea adopte una “decisión de adecuación”.

La Comisión Europea evaluará el ordenamiento jurídico y la práctica en materia de protección de datos, en esta fase podrá negociar la introducción de cambios normativos.

En el caso de que se llevará a cabo la declaración de adecuación mediante la decisión de la Comisión, el envío de datos al Reino Unido se realizará sin ningún otro tipo de requisito formal. En la página de la AEPD en el apartado de transferencias a terceros países y organizaciones internacionales están recogidos todos los países que cuentan con esa decisión de adecuación.



IMPORTANTE

Además de tener un nivel adecuado, lo que deberán celebrar es un contrato de acceso a datos por cuenta de terceros.