

Service Line IP, IT & Data Protection

Implementación y sanciones del RGPD en el primer aniversario de su aplicación

Mayo 2019

Análisis comparado paneuropeo de infracciones y sanciones

Francia

En Francia, la *Commission Nationale de l'Informatique et des Libertés* (CNIL) impuso una multa de 50 millones de euros a Google LLC (nº SAN 2019-001 de enero de 2019). Esta decisión es la primera que se dicta en la aplicación del RGPD

La CNIL constató que Google incumplía las obligaciones de RGPD en materia de transparencia e información, ya que la información facilitada "se diluye en varios documentos", lo que impide que el usuario conozca correctamente su alcance. La CNIL también ha comprobado que Google no cumple con la obligación de disponer de base jurídica para el tratamiento de los datos relativos a la personalización de los anuncios y que no dispone de un consentimiento válido.

Google ha interpuesto recurso contra esta decisión ante el *Conseil d'Etat* alegando, en particular, que la CNIL no tiene jurisdicción sobre Google LLC. Google LLC considera que su sede central en Irlanda constituye su establecimiento principal en Europa y que sólo la Comisión de Protección de Datos de Irlanda tenía jurisdicción. La decisión está pendiente.

España

En España, desde la entrada en vigor del RGPD se han producido varios desarrollos relevantes. En diciembre de 2018 se aprobó una nueva ley de protección de datos (LOPDGDD) que desarrolla ciertos aspectos del RGPD.

Durante 2018, el número de reclamaciones de los interesados presentadas ante la AEPD (*Agencia Española de Protección de Datos*) se ha incrementado un 33% con respecto al año anterior.

La implicación de la AEPD en tareas de sensibilización y orientación y de apoyo a la implementación de la RGPD ha sido enorme y se han publicado varias herramientas y directrices de apoyo.

Ha habido pocas sanciones específicas desde que el RGPD devino exigible; la AEPD se ha centrado más bien en el análisis de las infracciones y el envío de apercibimientos a las respectivas empresas responsables. Destaca la sanción anunciada a "La Liga", por importe de 250.000 euros, por una aplicación que informa de los resultados de los partidos de fútbol que usan millones de usuarios, aplicación que usa el micrófono del móvil del particular para luchar contra la piratería del fútbol; una suerte de app "espía" que usa para ello, además, la geolocalización del usuario sin la debida transparencia para el usuario y sin que éste tenga ocasión de revocar el consentimiento, a juicio de la AEPD. La Liga ha anunciado que recurrirá la sanción.



En cuanto a los apercibimientos que ha realizado la AEPD, destaca el caso de dos resoluciones diferentes similares, pero no idénticas, relativas a dos colegios y a los datos personales y las fotos de los alumnos, en las que la AEPD tuvo en cuenta los esfuerzos desplegados por ambas escuelas en las medidas de protección de datos adoptadas tanto antes como después de que se produjera la infracción de protección de datos. Es de esperar, no obstante, que se harán públicas en las próximas semanas o meses más sanciones. Así lo ha declarado públicamente en varios medios la directora de la propia Agencia.

Alemania

Desde la entrada en vigor del RGPD en mayo de 2018, las autoridades alemanas de protección de datos han impuesto 75 multas relacionadas con el RGPD. El importe total de las multas ascenderá a 449.000 euros.

La multa más elevada en un solo caso en Alemania fue de 80.000 euros y se impuso debido a la filtración de datos sanitarios por la inadecuación de los mecanismos de control interno. En otro caso, la autoridad de protección de datos de Berlín impuso una multa de 50.000 euros a un banco que había tratado datos no autorizados de antiguos clientes. Una red social alemana tuvo que pagar una multa de 20.000 euros por almacenar datos de usuario no encriptados en servidores antiguos.

Sin embargo, en general las multas se han mantenido dentro de unos límites razonables. Por otra parte, cabe suponer que a lo largo de 2019 se impondrán algunas sanciones más. Algunas autoridades alemanas de protección de datos ya han dejado claro que realizarán inspecciones sin previo aviso y que aumentarán el número de empleados.

En consecuencia, se puede resumir que el conocimiento sobre la protección de datos ha aumentado considerablemente en Alemania. Las empresas han "ordenado" sus bases de datos, han obtenido una visión general de sus procesos de protección de datos y han ajustado sus procesos para cumplir con los requisitos de RGPD.

Sin embargo, las pequeñas empresas y asociaciones alemanas se quejan del alto nivel de burocracia que implica, en particular en lo que se refiere a las obligaciones de información y documentación. Incluso el Comisionario Federal de Protección de Datos de Alemania considera en su informe anual reducir los gastos burocráticos de las pequeñas empresas y asociaciones.

Austria

Desde la entrada en vigor de la RGPD en Austria se han producido cambios notables, aunque todavía no han sido dramáticos. En cuanto a los cambios, el número de reclamaciones aumentó rápidamente entre 2017 y 2018 (el número al menos se triplicó). Sin embargo, la sanción más alta, de 4.800 euros, que se ha impuesto en Austria es bastante moderada.

Pero atención, ojo, a pesar de que estas sanciones todavía son manejables, se observa un cambio en la jurisdicción de la Autoridad de Protección de Datos (APD). Los requisitos de la APD para con los responsables de tratamiento han aumentado notablemente, especialmente en lo que respecta a las medidas de seguridad (especialmente en el sector de la asistencia sanitaria), así como a los requisitos de información y a los requisitos formales de consentimiento y de grabación de vídeo. En la práctica,

cientos de consentimientos inválidos pueden ser comercialmente más dolorosos que una multa, ya que los datos pertinentes ya no pueden utilizarse legalmente y pueden producirse reclamaciones por daños y perjuicios. Según lo que muestran las decisiones actuales, no se debería confiar en la hasta ahora práctica de "consulta en lugar de sanción" prometida inicialmente por los políticos en Austria. Al menos ahora, todo el mundo debería cumplir con el RGPD.

Polonia

Desde que el RGPD entró en vigor, podemos ver una intensificación de los esfuerzos de la Autoridad de Supervisión Polaca. A lo largo de este período, la Autoridad (PUODO) ha proporcionado una amplia orientación y ha anunciado un plan de inspecciones para 2019. El plan involucra principalmente a entidades públicas, el sector financiero y empresas dedicadas al telemarketing. La Autoridad de Supervisión ha declarado prestar especial atención a la videovigilancia y a la contratación de personal.

Hasta ahora se han impuesto dos multas administrativas en Polonia. La primera, de casi 1 millón de PLN (unos 230.000 euros), se impuso a una empresa que utilizaba datos personales de empresarios polacos en su actividad empresarial. Los datos fueron recogidos y presentados en la página web de la empresa, sin que los interesados hubieran sido informados de ello en la forma exigida por el artículo 14 del RGPD. El otro caso se refería a una asociación regional de fútbol que publicó en su sitio web los nombres, direcciones y números de identificación personal de 585 árbitros autorizados. La multa fue de 55.000 PLN (unos 13.000 euros) y se redujo gracias a la buena cooperación, al cumplimiento de las instrucciones de PUODO y al hecho de que ninguno de los árbitros sufrió daños. Estas no fueron las únicas infracciones detectadas por el órgano de vigilancia, pero las demás infracciones no fueron sancionadas.

El RGPD suscitó gran preocupación entre los empresarios polacos en mayo de 2018. Sin embargo, también aumentó considerablemente la concienciación sobre las cuestiones relativas a la protección de datos personales. Además, el RGPD influyó positivamente en algunas PYMEs polacas, que ahora realizan tratamiento de datos con mayor cuidado y se esfuerzan por garantizar su cumplimiento a este respecto.

El RGPD tiene algunos efectos secundarios en Polonia, siendo uno de ellos el llamado "troleo RGPD", según el cual algunos avispados envían spam a empresas polacas con solicitudes de datos personales, con la esperanza de descubrir alguna infracción para poder así reclamar daños y perjuicios. Hasta ahora, que nosotros sepamos, estos intentos han resultado inútiles.

Italia

En Italia podemos decir que han pasado pocos días desde el comienzo de la plena aplicación del nuevo régimen de sanciones previsto por R.G.P.D.

Aunque la RGPD entró en vigor el 25 de mayo de 2018, Italia estableció un "período de gracia", mediante el artículo 22, apartado 13, del Decreto Legislativo 101/2018, según el cual durante los primeros ocho meses, a partir de septiembre de 2018, la Autoridad Italiana de Protección de Datos no imponía ninguna sanción relacionada con el RGPD. Este "período de gracia" finalizó el 19 de mayo.

Durante 2018, la Autoridad Italiana de Protección de Datos se centró en cuestiones relacionadas con el software malicioso, aspectos del derecho laboral, la ciberseguridad, la asistencia sanitaria, la facturación electrónica y el telemarketing, como subrayó el presidente de la Autoridad durante el informe de actividad de 2018.

Hungría

Desde la entrada en vigor del RGPD, la autoridad húngara de protección de datos (NAIH) ha impuesto multas administrativas de entre 500.000 y 1.000.000 HUF (unos 1.500 y 3.000 euros); en una ocasión, impuso una multa de 11.000.000 HUF (unos 34.000 euros).

Las multas más pequeñas estaban relacionadas con la violación de diversos requisitos de protección de datos, como el hecho de no proporcionar información suficientemente transparente a una solicitud del cliente (el cliente quería saber cómo se tratan sus datos almacenados en copias de seguridad y durante cuánto tiempo), o el hecho de que el controlador no restringiera el uso de un número de teléfono cuando el nuevo propietario del número indicaba que el número ya no pertenecía al cliente del que se había recogido originalmente. Una decisión importante afirmó que, en el contexto de un préstamo de financiación de vehículos, el uso de un número de teléfono para el cobro de deudas - que es una finalidad distinta de la que se comunicó al interesado en el momento de la recogida de los datos - es un tratamiento sobre el que el responsable del tratamiento debería haber informado al cliente, y un tratamiento que se debe justificar mediante un análisis de ponderación realizado específicamente para tal fin; no basta con una referencia general a los intereses legítimos del responsable del tratamiento (el análisis de ponderación debe realizarse con respecto a cada finalidad). El caso en el que la NAIH impuso una multa de 11.000.000 HUF (unos 34.000 euros) se refería a una infracción de protección de datos en un sitio web que afectó a 6.000 personas, cuyos datos sobre opiniones políticas se filtraron; además el responsable del tratamiento incumplió su obligación de notificar la violación a la autoridad de protección de datos.

Grecia

La autoridad griega de protección de datos ha dictado un número bastante reducido de decisiones en el marco de la RGPD. En tales decisiones, la autoridad ha sido más bien indulgente, ya que ha optado por apercibir a los responsables del tratamiento en lugar de imponer multas.

En los tres casos de incumplimiento de la obligación de notificación de la violación de datos personales, la Autoridad emitió una amonestación, teniendo en cuenta que: a) el RGPD acababa de empezar a aplicarse; b) los responsables del tratamiento reaccionaron inmediata y con rapidez y trataron eficazmente la violación de datos; c) la violación de datos se refería a un número muy limitado de personas físicas; d) el ciberataque denunciado en uno de los casos era desconocido y muy complejo.

En el único caso relativo al incumplimiento de las obligaciones relativas a comunicaciones publicitarias no solicitadas, la Autoridad optó por una amonestación ya que se trataba de una sola persona física que se quejaba de haber recibido mensajes publicitarios a través de Viber sin haber dado su consentimiento de conformidad con las disposiciones pertinentes del RGPD. Es fundamental, en opinión de la Autoridad, proporcionar suficiente información a la persona física y declarar claramente la finalidad del tratamiento, es decir, si éste se enmarca en el contexto del contrato o si es de carácter promocional.

Cabe señalar, sin embargo, que, en los casos decididos en el marco legislativo anterior, la Autoridad parece haber endurecido la imposición de multas y, en algunos casos, ha alcanzado el límite máximo de 150.000 euros.

Además, la autoridad ha anunciado que ha llevado a cabo más de 65 investigaciones a distancia autoiniciadas en las páginas web de empresas de diversos sectores de la economía, con el fin de controlar el cumplimiento de una serie de obligaciones en virtud de la RGPD. La autoridad ha enviado notificaciones a los responsables del tratamiento, ordenándoles que ajusten las operaciones de tratamiento a las disposiciones de la RGPD en un plazo determinado, en algunos casos mediante la adopción de determinadas medidas específicas propuestas por la Autoridad, y que le informen al respecto.

Además, la Autoridad ha publicado la lista de actividades de tratamiento de datos que, en su opinión, deben estar cubiertas por una evaluación del impacto de protección de los datos.

Asimismo, es interesante mencionar que la autoridad ha anunciado que ha recibido desde el 25 de mayo de 2018 hasta principios de este año más de 96.000 quejas de los titulares de los datos alegando infracción de las disposiciones de RGPD. Queda por ver qué parte de ellas está justificada y, como tal, dará lugar a la adopción de medidas sancionadoras significativas por parte de la Autoridad de Protección de Datos.

Por último, cabe señalar que Grecia todavía no ha adoptado legislación para cubrir las áreas que se dejan a la jurisdicción de los Estados miembros.

Rumanía

Desde la entrada en vigor del RGPD, se han producido algunos avances notables en materia de protección de datos en Rumanía. En 2018 el Parlamento rumano ha aprobado la Ley nº 190 que aborda algunos de los puntos "abiertos" del RGPD. Al mismo tiempo, las Directivas 2016/680 y 2016/1148 han sido transpuestas a la legislación nacional.

En cuanto a la legislación de segundo nivel y las guías de mejores prácticas, la participación del APD es bastante escasa. Algunas asociaciones profesionales que representan a responsables de tratamiento en sectores como la banca, las telecomunicaciones o la edición, han presentado códigos de conducta para su aprobación por parte de APD, pero, según nuestro conocimiento, ninguno de estos códigos ha sido aprobado todavía por APD. En lugar de ello, la APD ha optado por enfocarse en crear concienciación a nivel informal, participando en muchas conferencias y eventos locales dedicados al RGPD, organizados tanto por el sector público como por el privado.

Las investigaciones de la APD se centraron generalmente en la resolución de quejas sobre presuntas violaciones de la privacidad de los datos, que aumentaron significativamente desde la entrada en vigor del RGPD. En 2018, el número de reclamaciones presentadas después del 25 de mayo era 2,5 veces mayor que el número de reclamaciones presentadas antes de la entrada en vigor del RGPD. No obstante, la APD también ha abierto de oficio una serie de investigaciones sectoriales, entre otros, en el sector bancario. Además, el APD presta especial atención a las violaciones de la seguridad, sobre las que ya están investigando.

Aun así, no tenemos conocimiento de sanciones específicas aplicadas por la APD por incumplimiento del RGPD. Sin embargo, en línea con la tendencia general a nivel de la UE, se espera que las multas y otras sanciones (incluidas las medidas correctivas) por incumplimiento del RGPD se impongan más pronto que tarde.

Portugal

Una de las primeras sanciones impuestas tras la entrada en vigor del RGPD fue para el Hospital de Barreiro, uno de los hospitales públicos más poblados de la región de Lisboa. La infracción se refería al acceso indiscriminado a los datos clínicos. La sanción se basaba en las siguientes infracciones del RGPD: el principio de minimización de datos; porque el Hospital permitió el acceso indiscriminado a un conjunto excesivo de datos a profesionales que sólo podían acceder a ellos en casos previamente justificados; los principios de integridad y confidencialidad, por no aplicar medidas organizativas y técnicas destinadas a impedir el acceso ilícito a los datos personales; la incapacidad del Hospital para garantizar la integridad, confidencialidad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento y la falta de aplicación de medidas organizativas y técnicas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, en particular, un proceso para poner a prueba, evaluar y evaluar periódicamente la eficacia de las medidas de seguridad del tratamiento de los datos. La APD portuguesa (CNPD) impuso al Hospital de Barreiro una multa de 400.000 euros.

Nuestro agradecimiento especial a los autores:

- > España · [Belén Arribas](#) · belen.arribas@AndersenTaxLegal.es
- > Alemania · [Dr. Fritjof Börner](#) · fritjof.boerner@AndersenTaxLegal.de
- > Portugal · [Raquel Brízida Castro](#) · raquel.castro@AndersenTaxLegal.pt
- > Rumanía · [Bogdan Halcu](#) · bogdan.halcu@tuca.ro
- > Grecia · [Dr. Themistoklis K. Giannakopoulos](#) · themistoklis.giannakopoulos@AndersenLegal.gr
- > Italia · [Francesco Inturri](#) · francesco.inturri@andersentaxlegal.it
- > Polonia · [Magdalena Patryas](#) · magdalena.patryas@ksplegal.pl
- > Austria · [Katharina Raabe-Stuppig](#) · raabe@lansky.at
- > Hungría · [Tamás Szabó](#) · tamas.szabo@sz-k-t.hu
- > Francia · [Angélique Vibert](#) · angelique.vibert@AndersenTaxLegal.es