NEWSLETTER DE IP-IT – Febrero 2017

CONTENIDOS

1. Primeras directrices para la aplicación del Reglamento Europeo de Protección de Datos: Figura del DPO y derecho a la portabilidad.

El Grupo del Artículo 29, integrado por las Autoridades de Protección de Datos de los Estados miembro de la Unión Europea (en adelante, "**WP29**"), ha publicado las primeras directrices para la implementación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "**RGPD**"). Dichas guías tiene el propósito de facilitar la comprensión así como introducir sugerencias o aclaraciones con relación al RGPD que entrará en vigor a partir del 25 de Mayo de 2018.

En esta primera oportunidad, se han publicado tres directrices relativas a:

i. Delegado de Protección de Datos (por sus siglas en inglés "**DPO**");
ii. Derecho de portabilidad;
iii. Autoridad de control principal.

Teniendo en cuenta su incidencia en la configuración de la política de privacidad de responsables y

encargado del tratamiento, nos centraremos en analizar las Directrices sobre el DPO y el derecho de portabilidad.

Delegado de Protección de Datos
El objetivo de las Directrices sobre el DPO es aclarar las disposiciones relevantes que se recogen en los artículos 37 a 39 del RGPD, para así ayudar y orientar a los responsables y encargados del tratamiento y también para asistir al DPO en el cumplimiento de sus funciones.

El WP29 procede a analizar una a una las circunstancias que condicionan el desempeño de las funciones del DPO. A continuación procedemos a sintetizar los aspectos más relevantes:

- Si bien en el artículo 37.1 del RGPD se enuncian las circunstancias que hacen obligatoria la designación de un DPO, uno de los argumentos que más se reiteran a lo largo del documento es que en cualquier escenario la designación de un DPO se considera una buena práctica muy recomendable para responsables y encargados del tratamiento.
- Se procede a aclarar y a interpretar una serie de conceptos esenciales para determinar la obligatoriedad de designar al DPO por los responsables o los encargados del tratamiento. A tales efectos, se determina lo que debe ser entendido como "autoridad u organismo público"; "tratamiento de datos a gran escala"; "observación regular y sistemática" de datos personales; o "actividades principales" del responsable o encargado del tratamiento. En todo caso, se recomienda dejar constancia del análisis realizado por los sujetos pasivos de la norma para determinar si se encuentran o no obligados a designar un DPO.
- Se reitera la necesidad de dotar de medios al DPO para el buen desempeño de sus funciones y se analiza su carácter independiente. Así, para el WP29 es necesario que el DPO sea conocido por todos los miembros de la organización del responsable o encargado del tratamiento; dependa orgánicamente del *management* de la compañía; cuente con acceso a la información necesaria y sea dotado de medios necesarios para cumplir debidamente con sus obligaciones.
- Se destaca la necesaria autonomía e independencia en sus criterios, no pudiendo ser apartado de su posición por tales circunstancias, citándose además posiciones dentro de las organizaciones en las que el cargo de DPO sería incompatible (e.g: responsable de RRHH o de IT); reiterándose el hecho de que el DPO puede ser externalizado por las organizaciones.

Finalmente, además de destacar la ausencia de responsabilidad personal del DPO, el WP29 insiste que el deber de implementar las medidas necesarias para cumplir con lo dispuesto en el RGPD es responsabilidad de los responsables y encargados del tratamiento. La labor del DPO será orientativa y aclaratoria, y en caso de no ser seguida o atendida por el responsable o encargado del tratamiento, tal circunstancia deberá ser debidamente justificada.

Derecho a la portabilidad de datos
En las Directrices sobre el derecho a la portabilidad de datos se analizan las implicaciones del derecho de portabilidad reconocido en el artículo 20 del RGPD. A través de este documento, el WP29 tiene el propósito de ayudar a los responsables del tratamiento a entender sus obligaciones y recomendaciones para las mejores prácticas y para el desarrollo de herramientas y soportes que permitan garantizar el derecho a la portabilidad de datos.

En línea con lo anterior, el WP29 procede a analizar los elementos que componen la definición del derecho a la portabilidad, de acuerdo a lo señalado en el artículo 20.1 del RGPD, así como las implicaciones técnicas que deben ser observadas para garantizar un libre ejercicio del derecho por parte de los titulares de los datos personales.

Recuerda el WP29 que este derecho debe basarse en tratamientos de datos que (i) se traten de forma automatizada en base al consentimiento del interesado o para la ejecución de un contrato del que el interesado sea parte, y (ii) se refieran al interesado y se haya facilitado por éste (esto incluye los datos

que genere su actividad, pero no el análisis que se pueda realizar de su comportamiento).

En este sentido, en relación a los datos que pueden ser objeto de este derecho, sintetiza dos condiciones relevantes, esto es:

- El alcance del ejercicio del derecho será el marcado por la solicitud, es decir, solo se incluirán aquellos datos personales que estén dentro del alcance de una solicitud.
- Los datos personales contemplados en este derecho son aquellos facilitados por el propio titular. Ahora bien, el responsable del tratamiento también deberá incluir aquellos datos personales que se han generado a partir de los datos facilitados por su titular. Así, las siguientes categorías pueden ser calificadas como "datos suministrados por el titular de los datos": (i) datos claramente suministrados por el titular de los datos (e-mail, nombre de usuario, edad, etc.); (ii) datos suministrados por el titular en función del uso de dispositivos o de la prestación de servicios (dispositivos de seguimientos a la actividad física).

Otra de las recomendaciones incluidas por el WP29 es que el responsable del tratamiento incluya siempre información sobre el derecho a la portabilidad de datos antes de cerrar una cuenta. Esto permitirá al usuario obtener sus datos y transmitirlos fácilmente a sus propios dispositivos o a otro proveedor con el que contrate el servicio.

Finalmente, el WP29 hace un llamamiento para impulsar sistemas interoperables y compatibles. Para ello, animan a la cooperación entre las empresas y asociaciones para trabajar en un objetivo común que permita contar con formatos y dispositivos que reúnan unas condiciones de interoperabilidad estándar.

• • •

2. Consulta pública sobre la adaptación al Reglamento General de Protección de Datos.

El Ministerio de Justicia ha abierto un proceso de consulta pública sobre la adaptación de la normativa nacional al contenido del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE.

En particular, los temas sobre los que se solicita opinión son (i) los problemas que se pretenden solucionar con la iniciativa, (ii) la necesidad y oportunidad de su aprobación, (iii) los objetivos de la norma y (iv) las posibles soluciones alternativas regulatorias y no regulatorias.

De conformidad con lo anterior, los ciudadanos, organizaciones y asociaciones que así lo consideren, pueden hacer llegar sus opiniones sobre los aspectos planteados en el siguiente enlace hasta el día 28 de febrero de 2017, a través de la dirección de correo electrónico sg_politica.legislativa@mjusticia.es.

• • •

3. Adaptación al nuevo Reglamento General de Protección de Datos (RGPD).

La Agencia Española de Protección de Datos ha publicado varios documentos para facilitar a las empresas la adaptación al nuevo Reglamento General de Protección de Datos (**RGPD**), que será de aplicación a partir del 25 de mayo de 2018.

El principal texto es la Guía del Reglamento General de Protección de Datos para responsables de tratamiento, en la que repasa los principios y obligaciones establecidos por el RGPD, identificando las diferencias respecto de la actual normativa. Esta Guía incluye una lista de verificación simplificada, que pretende facilitar a los responsables y encargados del tratamiento que realicen un número limitado de tratamientos la revisión de su grado de cumplimiento y la identificación de los aspectos de mejora.

Adicionalmente, la Agencia ha publicado una Guía para el cumplimiento del deber de informar, con recomendaciones sobre la información que debe proporcionarse y el modo en el que podrá cumplirse esta obligación; y unas Directrices para la elaboración de contratos entre responsables y encargados de tratamiento, encaminadas a facilitar que dichos contratos incluyan el contenido mínimo exigido por el RGPD.

Aunque estos documentos están dirigidos a pequeñas y medianas empresas, los criterios y recomendaciones de la Agencia son útiles para cualquier empresa que trate datos personales, independientemente de su tamaño y, por tanto, son una buena herramienta para iniciar la adecuación al RGPD.

• • •

4. Sentencia del Tribunal de Justicia de la Unión Europea de 19 de octubre de 2016. Consideración de la dirección IP dinámica como dato de carácter personal.

El Tribunal de Justicia de la Unión Europea (**TJUE**) ha publicado una sentencia en la que concluye que la dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta realizada por una persona de un sitio de Internet que dicho proveedor hace accesible al público, constituye dato de carácter personal respecto a dicho proveedor.

La expresada sentencia trae causa de una cuestión prejudicial planteada por el *Bundesgerichtshof* (Tribunal Supremo Civil y Penal de Alemania) que tiene por objeto la interpretación del artículo 2, letra a) y del artículo 7, letra f), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

En la cuestión prejudicial se solicita al TJUE que se dilucide si el artículo 2, letra a), debe interpretarse en el sentido de que una dirección IP dinámica registrada por un proveedor en línea constituye un dato de carácter personal cuando la información adicional para identificar al titular de dicha dirección IP está únicamente en posesión de un tercero (en este caso, el proveedor de acceso a Internet).

A este respecto el TJUE establece que, si bien una dirección IP dinámica no revela directamente la identidad de una persona física, del tenor del artículo 2, letra a) se desprende que se considera identificable a la persona que puede ser identificada no sólo directamente sino también indirectamente. Así el uso por parte del legislador del término indirectamente muestra que, para calificar una información de dato de carácter personal, no es necesario (i) que dicha información permita, por sí sola, identificar al interesado ni, (ii) que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona.

Más información en el siguiente enlace.

• • •

5. Sentencia del Tribunal de Justicia de la Unión Europea de 15 de septiembre de 2016. Responsabilidad del titular de una red Wi-Fi por la infracción de derechos de autor cometida por un usuario de la misma.

El Tribunal de Justicia de la Unión Europea (**TJUE**) ha publicado una sentencia en la que analiza la responsabilidad del titular de una red Wi-Fi por la infracción de derechos de autor cometida por un usuario de la misma.

La sentencia está relacionada con una petición de decisión prejudicial que el *Landgericht München I* (Tribunal Regional Civil y Penal de Munich I, Alemania) remitió al TJUE en el marco de un litigio entre el Sr. Tobias Mc Fadden y Sony Music Entertainment Germany Gmbh en relación con la eventual responsabilidad del primero por el uso, por parte de un tercero, de la red local inalámbrica que gestiona, con la finalidad de poner a disposición del público, sin autorización, un fonograma producido por Sony Music.

La Sentencia determina que los prestadores que facilitan un servicio de acceso a una red de telecomunicaciones no son responsables de los datos que les hayan sido transmitidos por los destinatarios de este servicio siempre que se cumplan tres requisitos (i) que no hayan originado ellos mismos la transmisión, (ii) que no hayan seleccionado al destinatario de la transmisión y, (iii) que no hayan seleccionado ni modificado los datos transmitidos.

De esta manera, el TJUE establece que, cuando se cumplen los requisitos arriba indicados, queda excluido en todo caso que el titular de derechos de autor pueda solicitar a ese prestador de servicios una indemnización debido a que la conexión a dicha red ha sido utilizada por terceros para infringir sus derechos.

Acceso a la Sentencia completa en el siguiente enlace.

• • •

6. Informe Jurídico 2016-0172 de la Agencia Española de Protección de Datos. Publicación individualizada de transferencias de valor. Interés legítimo.

La Agencia Española de Protección de Datos (**AEPD**) ha publicado un Informe Jurídico en el que analiza la conformidad a lo dispuesto en la Ley 15/1999, de 13 de diciembre. De Protección de Datos de Carácter Personal, de la publicación en sitios web de las informaciones individualizadas relacionadas con las transferencias de valor sin recabar previamente el consentimiento de los interesados.

La obligación de publicar las transferencias de valor está establecida en el artículo 18 del Código de Buenas Prácticas de la Industria Farmacéutica (**Código**), siendo las disposiciones contenidas en dicho Código de obligado cumplimiento para todas las empresas adheridas al mismo.

La AEPD indica en su Informe que la publicación de las informaciones individualizadas relacionadas con las transferencias de valor se encuentra amparada por el artículo 7 f) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, no siendo preciso el consentimiento de los interesados para que se lleve a cabo dicha publicación.

Sin perjuicio de lo anterior, la AEPD recomienda la adopción de medidas que impidan un tratamiento posterior de los datos que son publicados que pueda alejarse de la finalidad pretendida como, por ejemplo, (i) la aplicación de protocolos en los sitios web en los que se lleven a cabo las publicaciones que eviten la indexación de la información a través de motores de búsqueda o, (ii) la indicación en el propio sitio web de que la finalidad de la publicación es dar cumplimiento de la obligación del artículo 18 del Código.

Se puede consultar el Informe completo en el siguiente enlace.

• • •

7. Propuesta de Reglamento ePrivacy – Protección reforzada de la privacidad en las comunicaciones electrónicas.

Uno de los principales retos que debe superar el mercado único digital, es consolidar la confianza de los ciudadanos en la seguridad de los servicios digitales (mensajería instantánea, servicios de voz por Internet, entre otros). La incertidumbre respecto de la garantía de su vida privada, la confidencialidad de las comunicaciones y la protección de los datos personales, son zonas grises que afectan al sector de las comunicaciones electrónicas.

En respuesta a esta situación, el pasado 10 de enero la Comisión Europea publicó la propuesta de Reglamento para el respecto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas (**ePR**). Esta propuesta de Reglamento derogará la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.

A través del ePR se busca estandarizar la protección de la privacidad en comunicaciones electrónicas en la Unión Europea. El ePR entraría en vigor a partir del 25 de mayo de 2018.

¿Qué propone la Comisión Europea a través de la ePR?
En aquellos tratamientos que no son meramente técnicos, el consentimiento de los usuarios será una importante herramienta para garantizar una efectiva protección de la privacidad en las comunicaciones electrónicas. En síntesis, algunos de los aspectos incluidos son:

- **El tratamiento de los metadatos**, como los que se generan cuando se visita un sitio web o cuando se realiza una llamada por Internet, deberán ser eliminados o anonimizados si el usuario no ha dado su consentimiento para su tratamiento.

- Como ya se viene haciendo, será necesario aceptar el uso de *cookies* y otras tecnologías para acceder a la información almacenada en ordenadores. **La confidencialidad del comportamiento en línea de los usuarios debe ser garantizado.**

- Sin importar el tipo de tecnología usada, los usuarios deben dar su consentimiento antes de recibir **comunicaciones comerciales no solicitadas**.

- En aplicación del principio *privacy by design,* el software instalado en los dispositivos deberá informar al usuario final acerca de las herramientas de las que dispone para configurar su privacidad.

- Los prestadores de servicios de comunicaciones electrónicas deberán establecer procedimientos internos para responder las solicitudes de acceso a los datos usuarios finales de las comunicaciones electrónicas, así como informar de riesgos que puedan comprometer la seguridad de la red y de los servicios de comunicaciones electrónicas.

- La infracción de las disposiciones incluidas en el ePR podrán estar sujetas a multas de hasta 10.000.000€ o hasta el 2% de la facturación global del año anterior.

Aun cuando algunas de las medidas incluidas en el ePR ya vienen siendo aplicadas en España, será necesario integrar su aplicación junto con los cambios introducidos por el Reglamento Europeo de Protección de Datos. Según indica la Comisión Europea, el ePR complementará dicho Reglamento en lo que respecta a los datos de comunicaciones electrónicas que sean considerados datos de carácter personal.

• • •

8. El Consejo de Europa llama a los Estados miembros a prohibir los tests genéticos para fines de seguro.

El Consejo de Europa ha publicado una recomendación sobre el tratamiento de datos de salud en el ámbito asegurador.

Teniendo en cuenta el carácter sensible de la información relativa a los datos de salud objeto de tratamiento en los contratos de seguro, y los desarrollos en el campo de la genética de los últimos años que están permitiendo obtener y procesar de forma cada vez más sencilla información sobre las características genéticas de los individuos, el Consejo de Europa considera que existe un alto riesgo de que se produzcan interpretaciones incorrectas o excesivas sobre el estado de salud de los interesados,

llegando a afectar a la asegurabilidad de los mismos.

Por ello, sin negar el legítimo interés de las entidades aseguradoras en la evaluación de los niveles de riesgo, recomienda a los Estados Miembros la adopción de medidas adecuadas para garantizar el respeto de los derechos fundamentales de las personas, sin discriminación alguna. Estas medidas deberán garantizar el respeto al principio de proporcionalidad, asegurando que los datos de salud objeto de tratamiento en el marco de un contrato de seguro (genéticos o no), sean adecuados, pertinentes y no excesivos, con un alto valor predictivo de acuerdo con las normas científicas y clínicas generalmente aceptadas.

Asimismo, el Consejo de Europa considera que debe prohibirse la realización de pruebas genéticas específicamente con fines de seguro (esto es, no debería permitirse a las entidades aseguradoras imponer a los individuos el sometimiento a este tipo de pruebas genéticas como requisito para la contratación de una póliza) y, en relación con los resultados de las pruebas de esta naturaleza que puedan obrar en poder del individuo (o incluso de las aseguradoras), recomienda que su utilización sea regulado por ley.

• • •

Si desea más información sobre estos temas o cualquier otro asunto relacionado, puede ponerse en contacto con el equipo de profesionales del área de IP-IT de BROSETA.

Contactos del área de IP-IT de BROSETA

Miguel Geijo
Socio. Director del Área
mgeijo@broseta.com
Tel.: +34 91 432 31 44

Carolina Vivó
Abogada
cvivo@broseta.com
Tel.: +34 91 432 31 44

Alicia Coloma
Abogada
acoloma@broseta.com
Tel.: +34 91 432 31 44

Ángela Martínez
Abogada
angela.martinez@broseta.com
Tel.: +34 96 392 10 06