Novedades que introduce el Reglamento general de protección de datos

6 mayo de 2016

Tras una larga tramitación, ha sido publicado el Reglamento general de protección de datos –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–, que será directamente aplicable en todo el territorio de la Unión Europea y de obligado cumplimiento a partir de mayo de 2018

Introducción

Después de varios años de debate en el seno de las instituciones de la Unión Europea, el Reglamento General de Protección de Datos ha sido publicado finalmente en el Diario Oficial de la Unión Europea el día 4 de mayo de 2016. Desde esa fecha, la norma se conocerá como 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. Este nuevo Reglamento deroga la Directiva 95/46/CE, transpuesta en España mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, que la desarrolla; e introduce una serie de novedades que deberán ser observadas por todas las entidades que realicen actos de tratamiento de datos de carácter personal.

La Unión Europea ha promovido esta reforma con un doble objetivo. Por un lado, persigue adaptar la normativa a los avances tecnológicos y al entorno digital, que permiten la recogida y tratamiento de datos a gran escala. Por otro, trata de homogeneizar la regulación en todo el ámbito de la Unión Europea, para lo que utiliza la figura del reglamento que, a diferencia de la directiva, es directamente aplicable en todos los Estados Miembros. De esta manera se intenta poner fin a la fragmentación que existe actualmente entre los Estados Miembros.

El Reglamento general de protección de datos entrará en vigor a los veinte días de su publicación, pero no será de obligado cumplimiento hasta 2018. El regulador europeo, consciente de las muchas novedades que introduce la norma y de la relevancia de las mismas, concede un periodo de dos años para que las entidades que traten datos personales puedan adaptar su actividad de manera adecuada.

La normativa vigente en la actualidad no será derogada, sino que dejará de aplicarse en todo lo que contradiga al nuevo Reglamento general de protección de datos.

Novedades

- **Ámbito de aplicación territorial.**
    - Responsables o Encargados radicados o con establecimientos en la Unión Europea.
    - Responsables o Encargados radicados fuera de la Unión Europea que ofrezcan bienes o servicios a residentes europeos o analicen su comportamiento.

- **Principios *privacy by design* y *privacy by default*.** El Responsable deberá aplicar las medidas de seguridad adecuadas para el tratamiento de los datos desde el momento inicial. Además, deberá tratar, por defecto, solamente los datos estrictamente necesarios para la finalidad deseada y durante el plazo mínimo.

- **Principio de responsabilidad proactiva o *accountability*.** Las entidades que traten datos personales no estarán obligadas a cumplir unas medidas de seguridad determinadas, salvo algunas excepciones. En general, gozan de libertad para determinar las vías de prevención más adecuadas. Se viene a establecer una obligación de resultado: la posibilidad de demostrar el respeto a los principios de protección de datos y la seguridad de los datos personales, sin importar los medios utilizados para conseguirlo. No obstante, sí serán obligatorios la implementación del principio *Privacy by design*, el cumplimiento de ciertas obligaciones documentales y, en algunos casos, la realización de Evaluaciones de Impacto (PIA) o la designación de un Delegado de Protección de Datos (DPO).

- **Consentimiento.** El consentimiento deberá otorgarse mediante una acción activa, no bastando el silencio o la inacción.

- **Nuevos derechos.**
    - Derecho al Olvido. Los interesados podrán solicitar al Responsable la eliminación de sus datos personales.
    - Derecho a la Portabilidad de datos. Los interesados tendrán derecho a recibir los datos que les afecten que estén en poder de un proveedor para utilizar los servicios de otro.

- **Datos genéticos y biométricos.** Estas clases de datos se consideran datos especialmente protegidos junto a los datos de origen étnico o racial, datos relativos a preferencias políticas, religiosas o filosóficas, afiliación sindical, datos de salud y datos relativos a la vida sexual de las personas.

- **Delegado de Protección de Datos (DPO).** Será obligatorio designar un Delegado de Protección de Datos (empleado o externo) en los siguientes casos:
    - Tratamientos realizados por organismos públicos, excepto tribunales.
    - Actividades que supongan el tratamiento de datos a gran escala.
    - Tratamiento a gran escala de datos especialmente protegidos.

  El DPO deberá ser experto desde las perspectivas jurídica y técnica. Se encargará de lidiar con todas las cuestiones relacionadas con protección de datos que afecten a la entidad y tendrá plena autonomía, reportando únicamente al órgano directivo. Además, actuará como nexo en las relaciones y reclamaciones entre la entidad y los interesados.

  El Responsable deberá notificar la identidad del DPO a la autoridad de control.

  Se recomienda disponer de un DPO en muchos supuestos adicionales, ya que contribuye a dar cumplimiento al principio de *accountability*.

- **Deber de información.** El Responsable que trate datos personales deberá informar de nuevas cuestiones a los interesados. Destaca, en particular, la obligación de informar del plazo en que van a conservarse los datos personales. Trascurrido el plazo indicado, el Responsable perderá su legitimación para tratar los datos personales, por lo que deberá cancelarlos.

- **Aumento de las cuantías de las sanciones.** Las sanciones que pueden derivarse de la comisión de infracciones del Reglamento podrán alcanzar los 20 millones de euros o el 4% del volumen de negocio total anual global. El Reglamento introduce cierta incertidumbre al no tasar de forma exhaustiva los criterios o supuestos de graduación de las sanciones.

- **Responsabilidad del Encargado del tratamiento.** El Encargado del tratamiento responderá solidariamente junto al Responsable de los actos de tratamiento que realice.

- **Evaluaciones de impacto (*Privacy impact assesment* - PIA).** Las evaluaciones de impacto se utilizan para determinar los riesgos que los actos de tratamiento que realiza cierta entidad suponen para los datos personales. Serán obligatorias en los siguientes supuestos:
    - Cuando sea probable que al acto de tratamiento implique un riesgo alto para el derecho a la protección de datos. Se deben tener en cuenta

factores como la utilización de las nuevas tecnologías o la naturaleza, alcance, contexto y fines del tratamiento.

- Cuando se elaboren perfiles.
- Cuando se realicen tratamientos a gran escala de datos sensibles.
- Cuando se monitoricen zonas públicas a gran escala.

En España, la AEPD podrá ampliar la lista de supuestos en los que es necesario realizar una Evaluación de impacto mediante la publicación de una lista tasada.

- **Notificación de brechas de seguridad.** Las entidades que sufran una brecha de seguridad que ponga en riesgo datos personales deberán notificar la incidencia a la AEPD o a la autoridad de control correspondiente antes de 72 horas desde su conocimiento. Además, cuando la brecha suponga un riesgo alto, ésta deberá notificarse también a los propios interesados.

- **Legitimación activa de entidades sin ánimo de lucro.** Los interesados que sufran una infracción en su derecho a la protección de datos podrán encomendar la presentación de reclamaciones a entidades sin ánimo de lucro. Con ello, el Reglamento general de protección de datos reconoce la existencia de acciones colectivas en materia de protección de datos.

- **Comité Europeo de Protección de Datos.** El Grupo de Trabajo del Artículo 29, creado por la Directiva 95/46/CE, es sustituido por el Comité Europeo de Protección de Datos, que desempeñará una función consultiva similar.

- **Obligación de documentación.** El Reglamento sustituye la obligación de notificar los ficheros de datos personales a la autoridad de control oportuna por la simple necesidad de mantener un registro interno.

- **Límites a la elaboración de perfiles.** El interesado podrá oponerse a la elaboración de perfiles psicológicos, económicos, de salud, comportamentales, de fiabilidad o de rendimiento profesional, entre otros.

- **Ventanilla única o *One Stop Shop*.** La autoridad de control competente para supervisar el tratamiento de datos de una entidad será aquella que se encuentre en el mimo Estado que el establecimiento principal del Responsable. Atenderá tanto los tratamientos que se realicen en el mismo como, en la mayoría de los casos, los que se realicen en otros Estados.

Política de actuación de la empresa

ONTIER asiste a sus clientes para que puedan adaptarse de forma íntegra a los nuevos desafíos legales que introduce el Reglamento general de protección de datos prestando, entre otros, los siguientes servicios:

- Elaboración de evaluaciones de impacto.
- Servicio de Delegado de Protección de Datos externo.
- Revisión y adaptación de la actividad de la entidad y sus políticas internas a los nuevos principios de *accountability*, *privacy by design* y *privacy by default*.
- Adaptación de la actividad de la entidad a potenciales códigos de conducta sectoriales.
- Revisión y elaboración de programas de *governance* y *compliance*.
- Asesoramiento y elaboración de políticas de mitigación y respuesta ante brechas de seguridad.
- Supervisión de la licitud del tratamiento conforme a las nuevas vías de legitimación. Adaptación a los nuevos regímenes de consentimiento e interés legítimo.
- Adaptación de los formularios informativos de obtención del consentimiento.
- Actualización de relaciones contractuales con Encargados del tratamiento.
- Asesoramiento y formación a compañías no radicadas en la Unión Europea que dirigen sus servicios a residentes.
- Asesoramiento en el desarrollo e implantación de herramientas de exportación de datos.

ONTIER

Departamento: Nuevas Tecnologías y Propiedad Intelectual
Contacto: Joaquín Muñoz - jmunoz@ontier.net