RESUMEN DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Este Reglamento es el resultado de varios años de debate entre los diferentes organismos, instituciones y actores --gobiernos, las autoridades de protección de datos europeas y las empresas debido al **incesante avance de las nuevas tecnologías** en las últimas décadas, regulando con más detalle, aspectos que se derivan de dicha evolución tecnológica, como son la privacidad y la protección de datos.

En la actualidad, la popularización del uso de Internet y las redes sociales, el análisis avanzado de datos o el auge del Internet de las Cosas, entre otros factores, han cambiado totalmente la manera en la que usuarios y empresas se comunican entre ellos. En consecuencia, el nuevo Reglamento Europeo de Protección de Datos quiere **sentar las bases de una normativa de privacidad que se adecúe a la tecnología hoy presente**.

IMPACTO DEL NUEVO REGLAMENTO EUROPEO

La entrada en vigor del reglamento supone la derogación de la Directiva 95/46/CE, hasta ahora vigente, dicha derogación tiene efecto a partir del 25 de mayo de 2018, para permitir la plena adecuación de Estados, Administraciones públicas y empresas.

En España, en cuanto a la ley nacional aprobada por la LO 15/1999 de 13 de diciembre y su reglamento de desarrollo, aprobado por el Real Decreto 1720/2007 de 21 de diciembre, el Reglamento no los deroga ni puede derogarlos, pues dicha atribución corresponde al Estado Español.

El **Reglamento Europeo de Protección de Datos (RGPD)** tiene aplicabilidad directa en todos los Estados miembros a partir del **25 de mayo de 2018**, es decir, dos años después de su publicación. Además el 10 de noviembre de 2017 el Consejo de Ministros aprobó la remisión a las Cortes Generales del **Proyecto de Ley Orgánica de Protección de Datos**, que tiene por objeto adaptar la legislación española a las disposiciones del RGPD.

El RGPD **cambia radicalmente la forma actual de regular la protección de datos**, obligando a empresas, organismos, instituciones y administraciones a cambios y esfuerzos significativos de carácter organizativo, técnico, económico y humano al imponer nuevas obligaciones y requerimientos.

Figura fundamental en este nuevo marco regulador, es la del **Delegado de Protección de Datos (DPO)**, con el que, a partir de la entrada en vigor del Reglamento, deberán contar un gran número de empresas y organizaciones. La regulación específica del conocido como **Derecho al olvido**, el **registro de las actividades de tratamiento**, la **notificación a los interesados de las violaciones de**

seguridad, la **responsabilidad proactiva del responsable del tratamiento de los datos** o el principio de **portabilidad** de los mismos, son algunas de las novedades que nos trae el nuevo Reglamento.

RESUMEN DE LA AEPDATOS SOBRE LA ENTRADA EN VIGOR DEL REGLAMENTO EUROPEO.

Nuevos principios . El art. 5 del GDPR contiene la lista de principios a tener en cuenta en el tratamiento de datos personales. Algunos de ellos ya estaban previstos en la LOPD, pero se añaden otros nuevos.

Principio de Transparencia (5.1.a)

"Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado".

Este principio se centra en facilitar las relaciones entre el responsable de los datos y el interesado, así como entre el responsable de los datos y las autoridades de control.

Su materialización conlleva un importante cambio, ya que **desaparece la obligación de notificar y registrar los ficheros** que contienen datos personales ante la autoridad de control. En España, esta autoridad es la Agencia Española de Protección de Datos.

En el nuevo GDPR se ha definido un **"Registro de actividades de tratamiento"**. Este registro se llevará a cabo de forma interna y contendrá, entre otros, los siguientes datos:

- nombre y datos de contacto del responsable del tratamiento
- nombre y datos del Delegado de Protección de Datos
- finalidad del tratamiento
- descripción de categorías del interesado
- descripción de categorías de datos tratados
- las transferencias internacionales de datos

- **Principio de limitación de la finalidad (5.1.b)**

"Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (...) Los fines deben definirse en el momento de la recogida de Datos.

Minimización de datos (5.1.c)

"Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

En la edad de oro del Big Data este principio obliga a aplicar las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, **solo sean objeto de**

tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento (Artículo 25.2).

Nuevos derechos de los ciudadanos

La Ley Orgánica de Protección de Datos establecía 4 derechos para los interesados: Acceso, Rectificación, Cancelación y Oposición (conocidos en España como derechos ARCO).Pues bien, con el nuevo Reglamento Europeo de Protección de Datos, esta lista se amplía. Además de los derechos ARCO, se contemplan también los siguientes derechos:

- Derecho a la transparencia de la información, (art. 12)
- Derecho de supresión (derecho al olvido), (art. 17)
- Derecho de limitación, (art. 18)
- Derecho de portabilidad, (art. 20)

Por sus importantes consecuencias prácticas analizamos con más detalle el derecho al olvido y el derecho a la portabilidad:

- DERECHO AL OLVIDO. El nuevo GDPR establece que cualquier persona tendrá derecho a que su información personal sea eliminada de los proveedores de servicios de Internet cuando lo desee, siempre y cuando quien posea esos datos no tenga razones legítimas para retenerlos.

  Además obliga a los responsables de los datos que han difundido la información a terceros a comunicarles la obligación de suprimir cualquier enlace a los datos publicados, así como a eliminar cualquier copia o réplica de dichos datos. Su objetivo es conseguir eliminar de la red y de los buscadores cualquier rastro que haya de los datos de la persona que quiere ser “olvidada” de manera definitiva.

  DERECHO A LA PORTABILIDAD. En el nuevo GDPR se prevé la posibilidad de transmitir los datos de un responsable a otro, de forma que el interesado tendrá derecho a que los datos personales se transmitan directamente cuando sea técnicamente posible.

  Un ejemplo habitual es cuando un particular quiere cambiar de operadora de telecomunicaciones o de compañía de electricidad: la portabilidad permite que los datos personales del particular se transfieran directamente a la nueva compañía escogida, de forma ágil y sencilla para el usuario final.

  Además de incorporar estos nuevos derechos, el GDPR también exige que se creen **procedimientos visibles, accesibles y con un lenguaje sencillo** para facilitar al interesado el ejercicio de sus derechos. Además tendrá que ser posible a través de **medios electrónicos** como indica el Considerando 59.

Ampliación del deber de información

Nuestra legislación actual establece que a la hora de recoger el consentimiento de los interesados se les debía informar de la persona responsable del fichero, de la existencia de los ficheros inscritos en el Registro General de Protección de Datos, de la finalidad de la recogida de los datos y de la posibilidad de ejercitar los Derechos ARCO.

Desde mayo de 2108, además de estos datos, el Reglamento exige la obligación de informar sobre nuevos aspectos, se tiene que explicar la base legal para el tratamiento de los datos:

- se debe informar acerca del periodo de conservación
- se debe informar acerca de la posibilidad de hacer reclamaciones
- se debe informar de los demás derechos que incorpora el nuevo RGDP

Es por tanto conveniente revisar las **cláusulas informativas** que se hayan incorporado en los procesos de recogida de datos e incluir los nuevos apartados para cumplir así con las exigencias del GDPR.

Obtención del consentimiento para el tratamiento de datos

La actual LOPD exige el consentimiento inequívoco de los interesados para el tratamiento de sus datos.

No obstante, si los datos recabados no son especialmente sensibles (como por ejemplo los datos biométricos), se admite que dicho consentimiento pueda ser tácito.

El GDPR mantendrá los mismos principios del consentimiento que establece la LOPD, exigiendo un consentimiento libre, informado, específico e inequívoco. Sin embargo, como novedad respecto de la LOPD, el nuevo GDPR indica que para poder considerar que el consentimiento es inequívoco, deberá existir **una declaración del interesado o una acción positiva que manifieste su conformidad**.

El silencio, las casillas ya marcadas o la inacción no constituirán prueba de consentimiento (Considerando 32 del GDPR).

El tratamiento de datos de menores en el nuevo Reglamento Europeo de Protección de Datos.

Respecto al tratamiento de datos de menores en el nuevo GDPR, se dispone de una regla homogénea que establece que la edad en la que los menores pueden prestar por sí mismos su propio **consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información** (por ejemplo, redes sociales o aplicaciones móviles) es de 16 años.

Sin embargo, esa edad se puede rebajar y cada Estado miembro puede establecer la suya propia, fijando un límite no inferior en ningún caso a los 13 años.

Por ejemplo, **el límite en España se ha dispuesto en los 14 años.** Si se es menor de esa edad, es necesario que padres o tutores den su consentimiento a la empresa u organización que quiera tratar los datos personales del menor.

¿Hay que obtener el consentimiento explícito de clientes ya existentes según el nuevo GDPR?

Uno de los aspectos que está provocando mayor debate es **la forma en que se van a regular los consentimientos de clientes o usuarios** obtenidos con anterioridad a la entrada en vigor del nuevo Reglamento Europeo de Protección de Datos.

En este sentido, el nuevo GDPR es tajante: si el consentimiento no se encontraba claramente identificado o se basó en formas tácitas o por omisión, **deberá volverse a solicitar.**

Habrá que tenerlo muy en cuenta, porque el tratamiento de datos sin el consentimiento de los usuarios se entiende como una infracción muy grave según el nuevo reglamento.

Establecer acciones y medidas de seguridad

Actualmente el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD) establece la obligación de aplicar diferentes medidas en función del nivel de seguridad - básico, medio o alto - de los datos tratados.

El nuevo GDPR no distingue entre los niveles de los ficheros, sino que especifica que se apliquen medidas de seguridad teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas. (Artículo 25 Protección de datos desde el diseño y por defecto).

El nuevo Reglamento europeo de protección de Datos habla de medidas para garantizar un nivel de seguridad adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse.

El GDPR, bajo el **principio de responsabilidad proactiva (Artículo 5.2),** exige al responsable del tratamiento que aplique las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. El GDPR propone como mecanismos efectivos de verificación del cumplimiento la adhesión a códigos de conducta o a mecanismos de certificación (artículo 42.3 del GDPR).

Por tanto, lo que el GDPR exige es que las empresas tengan una **actitud consciente, diligente y proactiva del tratamiento de los datos**, pudiendo demostrar, si llegara el caso, las medidas de seguridad aplicadas.

Evaluación de impacto del tratamiento de datos personales

Otra nueva obligación que establece el GDPR es la de realizar una **evaluación de**

impacto (Privacy Impact Assessment) para las organizaciones que realicen tratamientos de datos que puedan implicar un **alto riesgo para los derechos y libertades** de las personas físicas. Se debe evaluar el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo (Considerando 84 del GDPR).

Para facilitar esta labor, la Agencia Española de Protección de Datos publicó en 2014 **una Guía para la Evaluación de Impacto en la Protección de los Datos Personales**, en la que se establecen las bases y aspectos esenciales que deberán tener en cuenta los obligados a realizar la evaluación de impacto.

Comunicación de fallos a la autoridad de protección de datos

Otra de las novedades más importantes se trata de una nueva obligación que el GDPR impone al responsable del tratamiento: **notificar las violaciones de seguridad de los datos**. Es decir, el responsable del tratamiento de los datos deberá notificar a la autoridad competente (AEPD en España) cualquier brecha de seguridad que se haya producido en el plazo de 72 horas desde que ocurra. Además, si la brecha implica un riesgo para los interesados, también se les deberá notificar a ellos.

La Figura del Delegado de Protección de Datos

El GDPR le dedica una sección entera a una nueva figura, dada la relevancia que tiene para el futuro: el **Delegado de Protección de Datos** (Data Protección Office).

Esta persona es el **asesor de protección de datos de la empresa,** y asume competencias en materia de coordinación y control del cumplimiento de la normativa en materia de protección de datos.

Esta figura no es obligatoria para todas las organizaciones: solo tendrán que contar con un delegado **las empresas públicas**, las que tengan un tratamiento a gran escala o las que recojan datos especialmente sensibles o relativos a condenas o infracciones penales.

Entre las funciones que le serán encomendadas a un delegado de protección de datos se encuentran, entre otras, las siguientes:

- supervisar la implementación y aplicación de las políticas internas
- realizar formación al personal
- organizar y coordinar las auditorías
- gestionar la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos
- velar por la conservación de la documentación
- supervisar la realización de la evaluación de impacto
- actuar como punto de contacto para la autoridad de control

El Delegado de Protección de Datos deberá ser designado con cualidades profesionales y, en particular, con conocimiento experto de la legislación y prácticas de protección de datos y la capacidad de cumplir con las tareas impuestas por el GDPR.

El Delegado puede elegirse de entre personal existente en la organización del responsable de los Datos o cumplir las tareas a través de un contrato de servicios.

Las autoridades de protección de datos

El GDPR sigue manteniendo la existencia de los diferentes reguladores nacionales y sus funciones, pero ahora estarán coordinados por un organismo dependiente de la Comisión Europea: el **Comité Europeo de Protección de Datos**.

Para los titulares de los datos se establece un sistema de **ventanilla única**, lo que significa que en caso de que tengan que realizar una reclamación dentro de cualquiera de los Estados miembros, podrán acudir ante la autoridad de su país.

Por su parte, los responsables y encargados del tratamiento que tenga centros en diversos Estados miembros, podrán centralizar la organización de su Sistema de Gestión de la Privacidad en un único país (estableciendo una autoridad de control principal).

Sanciones más altas

Una de las cuestiones que está generando más debate y controversia es la diferencia exponencial de la **cuantía de las sanciones** que establece el nuevo GDPR.

Si hasta mayo de 2018 las sanciones pueden ir desde 900 euros hasta 600.000, a partir de entonces no se establecen cuantías mínimas y las máximas pueden alcanzar los 20 millones de euros o hasta el 4% del volumen de negocio del infractor.

RESUMEN

Las 10 novedades más destacadas de este nuevo Reglamento son:

1. Nuevos **principios**: transparencia (Registro de actividades de tratamiento), limitación de la finalidad y minimización de datos.
2. Nuevos **derechos** de los ciudadanos: derecho al olvido y derecho a la portabilidad de los datos.
3. Ampliación del deber de **información**.
4. Forma de obtención del **consentimiento**: una declaración del interesado o una acción positiva que manifieste su conformidad.
5. Establecimiento de **acciones y medidas de seguridad**.
6. Obligación de realizar **Evaluaciones de Impacto** para determinar el cumplimiento normativo.
7. Nuevas notificaciones a la Autoridad de Control: **las violaciones de seguridad de los datos.**

8. La creación de la figura del **Delegado de Protección de Datos** (DPO Data Protección Office).
9. Aplicación del concepto **"Ventanilla Única"** para que los ciudadanos interesados puedan efectuar trámites, aunque estos afecten a autoridades en la materia de otros estados miembros.
10. Incremento de la cuantía de las **sanciones**.

Madrid 9 de julio 2018