1. APLICACIÓN DEL NUEVO REGLAMENTO

El Reglamento General de Protección de Datos **entró en vigor el día 25 de mayo de 2016**. No obstante, **no será efectivamente aplicable hasta dos años después, es decir, hasta el 25 de mayo de 2018**. Este periodo durante el cual no se aplica de manera absoluta el RGPD se ha establecido para que **los Estados de la Unión Europea, las Instituciones Europeas y las distintas entidades que tratan datos de carácter personal, mediante el estudio de la nueva normativa y de las repercusiones que tendrá, vayan preparándose y adaptándose**.

El RGPD solamente derogará las Directiva 95/46/CE, lo que significa que nuestra Ley Orgánica, así como el Reglamento que la desarrolla seguirán siendo normas plenamente válidas y aplicables. Es por ello que esa labor esencial de los Estados Miembros de elaborar normativas que armonicen el marco legal de protección de datos deberá respetar en todo momento lo dispuesto por el nuevo RGPD, pues se trata de la norma superior en este ámbito.

2. UNA NORMA MUCHO MÁS AMPLIA

El RGPD tiene como objetivo armonizar la normativa de protección de datos de los distintos Estados Miembros de la Unión Europea, lo que conlleva que su contenido sea realmente amplio. Esto afecta en gran medida a las entidades, pues su catálogo de obligaciones se vuelve mucho más extenso de lo que ha sido típicamente. Además, las obligaciones impuestas a las entidades no se encuentran realmente concretadas, por lo que la labor de interpretación jurídica es más importante que nunca, para no incumplir la nueva ley de manera grave.

El Reglamento pretende que el ciudadano sea el eje central del ámbito de la protección de datos. Para ello, **el sistema pasará a ser preventivo y no sancionador**, esto es, las distintas entidades tendrán un gran número de obligaciones para que los derechos de los ciudadanos se respeten en todo momento. **Sin embargo, las sanciones son ahora mucho más cuantiosas, llegando a los 20 millones de euros o al 4 % del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía** de entre las dos cantidades. De esta manera, las entidades deben conocer con perfecta claridad sus obligaciones si no quieren hacer frente a este tipo de sanciones.

Para ello, el RGPD recoge lo que se denomina como **responsabilidad activa: las entidades están obligadas a adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece**. Ésta es precisamente la justificación del gran incremento en la cuantía de las sanciones, ya que las mismas se imponen de no haber respetado de manera alguna los derechos de los ciudadanos a los que protege esta normativa de protección de datos de carácter personal. Las sanciones no son válidas como estrategia para proteger los derechos del ciudadano, pues su imposición supone que tales derechos se han violado. Es por ello que la prevención es la razón de ser del RGPD, pues así se obliga a las entidades a proteger los derechos propios de los ciudadanos.

Es necesario cambiar el punto de vista con el que se contemplaba este ámbito hasta ahora para cumplir con la nueva normativa. **No se trata ya de respetar determinados artículos de una ley, sino que se pretende que las entidades gestionen los datos asesorados por profesionales del sector, para que de esa forma se consiga el fin último de la ley: salvaguardar los derechos fundamentales de los ciudadanos europeos**.

El listado de las más importantes obligaciones que el RGPD impone a las entidades puede condensarse de la siguiente manera:

- Protección de datos desde el diseño

- Protección de datos por defecto

- Medidas de seguridad

- Mantenimiento de un registro de tratamientos

- Realización de evaluaciones de impacto sobre la protección de datos

- Nombramiento de un delegado de protección de datos

- Notificación de violaciones de la seguridad de los datos

2.1. Protección de datos desde el diseño

La privacidad desde el diseño pretende el cumplimiento de la normativa de protección de datos en todos los productos y servicios desde sus primeros estadios de desarrollo. El RGPD afirma que **el responsable del tratamiento está obligado a aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, que den como resultado la aplicación de forma efectiva de los principios de protección de datos**.

Para entender este concepto, es realmente gráfico el ejemplo dado por la "*Office of the Information and Privacy Commissioner of Ontario*". La privacidad desde el diseño sería un diario personal, en el que una persona apunta sus pensamientos más íntimos, que cuenta con un candado desde que se fabricó. De no existir el candado, cualquiera podría acceder a lo escrito en el diario, por lo que se deberían tomar medidas para proteger su contenido de manera posterior, como meter el diario en un cajón o esconderlo. Sin embargo, ese candado del diario que simboliza la *privacy by design*, supone la consideración de privacidad desde el principio, siendo el sujeto de manera posterior el que decidiría a quién mostrar la información.

El asesoramiento, por tanto, es esencial para el cumplimiento de este nuevo concepto, pues para aplicarlo se han de tener en cuenta circunstancias tales como:

- El estado de la técnica.
- El coste de la aplicación efectiva de tales medidas.
- La naturaleza, ámbito, contexto y fines del tratamiento.
- Los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas

2.2. Protección de datos por defecto

La privacidad por defecto se encuentra recogida en el art. 25.2 RGPD, el cual afirma que **el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento**.

Lo que significa la privacidad por defecto, básicamente, es que las medidas más restrictivas en cuanto a la normativa de protección de datos son las que han de aplicarse automáticamente en el momento en que un usuario adquiere un nuevo producto. Sin embargo, el asesoramiento es esencial tanto para el cumplimiento de este nuevo concepto, como para el cumplimiento de la privacidad desde el diseño, pues **se trata de nuevos conceptos jurídicos indeterminados cuya aplicación práctica por parte de los empresarios es especialmente complicada**.

Para aplicarla se han de tener en cuenta circunstancias tales como:

- La cantidad de datos personales recogidos.
- La extensión de su tratamiento.
- Su plazo de conservación.
- Su accesibilidad.

2.3. Medidas de seguridad

Tanto el responsable como el encargado del tratamiento deberán aplicar las medidas necesarias para garantizar un nivel de seguridad adecuado al riesgo. Las medidas mínimas de seguridad establecidas por el RGPD son las siguientes:

- La **seudonimización** y el **cifrado de datos personales**.
- La capacidad de garantizar la **confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento**.
- **La capacidad de restaurar la disponibilidad y el acceso a los datos personales** de forma rápida en caso de incidente físico o técnico.
- **Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas** técnicas y organizativas para garantizar la seguridad del tratamiento.

Para conocer con exactitud las medidas de seguridad que deben implantarse en el sistema de tratamiento de datos se han de tener en cuenta las denominadas **evaluaciones de impacto**, que posteriormente se detallan y que se convertirán en esenciales cuando la nueva normativa se comience a aplicar.

2.4. Mantenimiento de un registro de tratamientos

Este registro constará **por escrito, inclusive en formato electrónico** (art. 30.3 RGPD). El encargado del tratamiento y, en su caso, el representante del responsable deberá poner el registro a disposición de la autoridad de control si así lo solicitase, como bien dicta el art. 30.4 RGPD.

El registro de actividades de tratamiento debe contener los siguientes puntos:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- En su caso, las transferencias de datos personales a un tercer país u Organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

2.5. Realización de evaluaciones de impacto sobre la protección de datos

El RGPD determina que, cuando sea probable que un tipo de tratamiento suponga un riesgo para los derechos y libertades de las personas, **el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales**. Si dentro de la entidad se hace uso de las nuevas tecnologías, el RGPD hace hincapié en la especial necesidad de utilización de estas evaluaciones de impacto, y ello por el riesgo que supone la utilización de estos medios en el ámbito de la protección de datos de carácter personal. Según lo dispuesto en el RGPD, las evaluaciones de impacto deberán incluir lo siguiente:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

- Una evaluación de los riesgos para los derechos y libertades de los interesados.

- Las medidas previstas para afrontar tales riesgos, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

2.6. Nombramiento de un delegado de protección de datos

El Delegado de Protección de Datos es una nueva figura creada por el RGPD que pretende el asesoramiento jurídico especializado en materia de protección de datos de carácter personal.

El responsable o el encargado del tratamiento deberán nombrar un Delegado de Protección de Datos en los casos en que la normativa, tanto europea como española, así lo determine. **De momento, y a falta de desarrollo normativo por parte de nuestras autoridades nacionales, el RGPD determina que se deberá designar un delegado de protección de datos siempre que**:

- El tratamiento lo lleve a cabo una autoridad u organismo público.

- El tratamiento, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.

- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

El Delegado de Protección de Datos, como bien determina el art. 37.5 RGPD, deberá ser nombrado atendiendo a sus conocimientos en Derecho y, más en concreto, teniéndose en cuenta su especialización en protección de datos. Las funciones que esta figura deberá desempeñar son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados de sus obligaciones respecto a la protección de datos.

- Supervisar el cumplimiento de la normativa de protección de datos de carácter personal.

- Asignar responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y la realización de las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicite acerca de las distintas evaluaciones de impacto que se desarrollen dentro de la entidad.

- Cooperar con las autoridades de control, así como actuar como punto de contacto con ella.

2.7. Notificación de violaciones de la seguridad de los datos

El art. 33 RGPD determina que **las brechas en la seguridad de los datos de carácter personal deberán ser notificadas por el responsable del tratamiento a la autoridad de control** en el plazo máximo de 72 horas. De esta manera, la autoridad de control pasará a comprobar si la entidad cuya seguridad ha sido violada cumple con lo estipulado por la normativa de protección de datos.

Además, **el responsable del tratamiento deberá informar a los interesados de las violaciones de seguridad** que se hayan producido con respecto a sus datos, pues de ello se puede derivar un perjuicio grave.

A esta cadena de notificaciones se une **el encargado del tratamiento, pues éste deberá informar al responsable del tratamiento de las violaciones de seguridad que se produzcan**.

En este sentido, el objetivo del RGPD es doble: **por un lado**, las autoridades de control pueden desarrollar su actividad, en el sentido de que pueden controlar de qué manera las distintas entidades llevan a cabo el tratamiento de datos de carácter personal; **por otro lado**, se responsabiliza a las entidades, debiendo las mismas rendir cuentas a los interesados en caso de que una determinada brecha en la seguridad suponga un perjuicio para sus derechos y libertades.

2.8. Responsabilidad proactiva

El art. 24 RGPD establece que, atendiendo a la naturaleza, al ámbito, al contexto y los fines del tratamiento y a los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y **poder demostrar** que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Por ello, y como bien se ha encargado de recordar la Agencia Española de Protección de Datos, la obligación documental para los responsables y encargados será mucho mayor, pues es necesario dejar constancia de todo los protocolos y actuaciones desarrollados para con la información de carácter personal.

3. REPERCUSIONES SOBRE EL COLEGIO

Lo que significa la aprobación del nuevo Reglamento es el **cambio en la manera de gestionar datos por parte del Colegio Profesional**. El RGPD pretende que estas entidades, en su actividad cotidiana, respeten el derecho fundamental a la protección de datos, lo que significa que ya no se trata de cumplir con ciertas obligaciones, sino de **incluir en el normal funcionamiento de la entidad actividades encaminadas a respetar los derechos de las personas físicas en este ámbito**.

Y ello queda demostrado con la nueva figura que determinadas entidades deben nombrar: el Delegado de Protección de Datos. Este nuevo sujeto, que se une a los ya existente (responsable del tratamiento y encargado del tratamiento), será el garante de que se cumple con lo dispuesto por la nueva normativa.

Además, las evaluaciones de impacto están destinadas a cambiar el funcionamiento actual, pues suponen que la entidad debe, en cierto modo, organizar su propio sistema de protección de datos en base a los análisis llevados a cabo por especialistas, y que deben encaminarse a cumplir con el contenido del RGPD.

Asimismo, se ha querido ampliar el alcance de la norma. El RGPD se aplica a responsables y encargados establecidos en la UE, pero **también se aplica a responsables o encargados que se encuentren fuera del territorio europeo** siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

Esta ampliación de la norma supone que **las garantías que hay que salvaguardar con respecto a los ciudadanos se amplían considerablemente. Y más si tenemos en cuenta que cambian los derechos de los ciudadanos**. Los derechos ARCO dejan paso a los siguientes, establecidos por el RGPD: **Transparencia, Información, Acceso, Rectificación, Supresión (o Derecho al Olvido), Limitación del Tratamiento, Portabilidad de Datos y Oposición**. Esto requiere, por consiguiente, una mayor carga para las entidades en cuanto a obligaciones para cumplir con la legalidad en sus relaciones con los clientes.

Como bien ha interpretado la AEPD, **el nuevo Reglamento tiene como objetivo que cada entidad, según sus características propias, desarrolle un tratamiento de datos distinto adaptado a las necesidades específicas de cada caso, pero respetando siempre los límites y las máximas que las normas establecen y contando con el asesoramiento de las nuevas figuras que el Reglamento crea y que deben contar con amplia experiencia dentro del sector**.

Incluso el consentimiento otorgado por el particular para el tratamiento de sus datos con una determinada finalidad cambia. **Ya no es válido el consentimiento tácito**, siendo necesario el denominado

consentimiento explícito, por lo que las cláusulas y contratos que pretenden la recogida y el tratamiento de datos deben cambiarse para ser acordes con la nueva normativa europea.

Las políticas de privacidad y de cookies también deben cambiar para adaptarse a la legalidad. Dado que los cambios que se producen son sustanciales, las políticas de privacidad deben cambiar también, debiendo estar escritas en los términos de transparencia, accesibilidad y sencillez marcados por el Reglamento.

El RGPD pretende, por tanto, que los responsables y encargados se conciencien y responsabilicen con la normativa de protección de datos, estableciendo para ello sanciones de gran calibre para el caso de que la protección de este derecho fundamental sea insuficiente. Este aumento en las sanciones, que llegan hasta los 20 millones de euros o el 4% del volumen de negocio anual (se optará por la de mayor cuantía), tiene por objetivo castigar severamente a las entidades que no se adapten en la forma requerida a la nueva normativa. **Ya no se trata de cumplir con determinados principios de protección de datos, sino de conformar y desarrollar un correcto y adecuado sistema que respete lo que el nuevo Reglamento General de Protección de Datos dispone**.