REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Reflexiones tras los primeros meses de la entrada en vigor

Elaborado para la AEC por IBM

Octubre de 2018

Índice

Monte Esquinza, 34 2ºB- 28010 Madrid
Telf: 91 308 01 61
www.consultoras.org

Recordemos qué es el RGPD

Aunque todos deberíamos conocer qué es el **Reglamento General de Protección de Datos**, merece la pena recordarlo como punto de partida de este documento. El **RGPD** (GDPR en inglés) regula la protección de las personas físicas en lo que respecta al tratamiento de **datos personales** y a la libre circulación de estos datos. Este reglamento entró en vigor el 25 de mayo de 2016 y fue de aplicación el **25 de mayo de 2018**.

El tiempo pasa rápido y hace ya más de un trimestre que el RGPD es de aplicación a nivel europeo. Ello implica, por tanto, que cualquier empresa europea que maneje información personal de cualquier tipo deberá cumplir el reglamento. Cabe destacar que esta normativa también aplica a toda empresa (sea o no europea) que tenga negocios en la UE.

Esta reglamentación más restrictiva se concibió para proporcionar a los individuos un mejor **control sobre sus datos personales** y establecer un conjunto único de reglas de protección de datos de ciudadanos de la UE. Por tanto, el objetivo que se persigue es disponer de un marco legal armonizado para la protección de los datos en todo el territorio de la UE.

¿Qué datos se tienen que proteger y cómo?

El concepto de Dato Personal puede dar lugar a equívocos, por lo que es pertinente clarificar el concepto. La definición exacta es la siguiente: **Dato Personal** es cualquier información que **identifique o pueda identificar a un individuo**, sin distinción entre datos privados, públicos o profesionales. Por tanto, cualquier dato que identifique o pueda identificar a un ciudadano de la UE será considerado como dato personal.

Dicho esto, una parte clave de la normativa es que cómo se deben proteger dichos datos. Para que una organización, entidad o empresa pueda gestionar datos personales, los individuos tienen que proporcionar a dichas organizaciones el consentimiento a que sus datos sean tratados, manejados o procesados. Y, aún más, dichas organizaciones deberán tener la evidencia del **consentimiento**. Asimismo, los datos proporcionados tienen que ser tratados para un propósito específico, explícito y legítimo, pudiendo los individuos solicitar la cancelación del consentimiento en cualquier momento, teniendo el derecho a que sus datos se borren cuando el propósito para el que se recopilaron ya no aplica.

Cuando las organizaciones obtienen datos personales de un individuo, éste debe tener conocimiento expreso de:

- La identidad y datos de contacto de la organización que gestiona / posee sus datos personales.
- El propósito o razón por la que se recopilan los datos y cómo y con qué fin serán utilizados.
- Si los datos serán transferidos internacionalmente.
- El período durante el cual se almacenarán los datos.
- El derecho del individuo para el acceso, rectificación o borrado de los datos.
- El derecho del individuo para retirar en cualquier momento el consentimiento de acceso o tratamiento de los datos.
- El derecho del individuo a presentar una queja.

En cuanto a la seguridad, las compañías tienen que reportar cualquier **brecha de seguridad** en la gestión de los datos personales a la Autoridad Supervisora competente. Esto se tiene que realizar sin retraso, y antes de las **72 horas** de haberse identificado el incidente (salvo riesgo improbable de que se produzca la brecha).

Roles de las organizaciones

En cuanto a los roles, también conviene tratar el papel de las organizaciones o empresas en lo relativo a la gestión de los Datos Personales, más aun en un entorno de consultoría donde compañías de este sector prestan sus servicios. Así, en cuanto al tratamiento de Información Personal, el RGPD distingue las figuras de Controlador y Procesador.

El **Controlador** es aquella organización que **controla el propósito y el uso del dato** y es el principal responsable del cumplimento y compromisos que conlleva la normativa.

El Controlador puede, además, contratar un **Procesador** que **ayuda en el procesamiento del dato** de acuerdo con sus instrucciones.

Si bien el Controlador es quien ostenta la principal responsabilidad en el cumplimiento de la normativa y, por tanto, el que está expuesto a las multas más altas en caso de incumplimiento, el RGPD también extiende alguna de las obligaciones y compromisos al Procesador de datos.

Procesador es un término muy amplio que abarca, por ejemplo, el almacenamiento de la información. Por tanto, todo Procesador tiene que tomar las medidas necesarias para mantener su servicio bajo las exigencias del cumplimiento de la normativa: eso supone revisar contratos, sistemas y procesos, e incluso su relación con subprocesadores si existieran. El papel de Procesador es el que suele aplicar a las **empresas de consultoría cuando éstas prestan sus servicios a clientes**, de ahí la importancia para el cumplimiento del RGPD cuando el papel jugado es el de Procesador.

Consecuencias de incumplimiento

El incumplimiento del RGPD puede tener unas consecuencias muy importantes para las organizaciones. Las sanciones pueden ascender hasta **10 millones de euros** o, en caso de que se trate de un importe mayor, hasta el **2% de la facturación total anual** del contrato. Se trata, por tanto, de penalizaciones importantes en caso de brecha en el mantenimiento de los datos, seguridad o notificación y, en definitiva, cualquier violación en la gestión de datos personales de individuos de la UE.

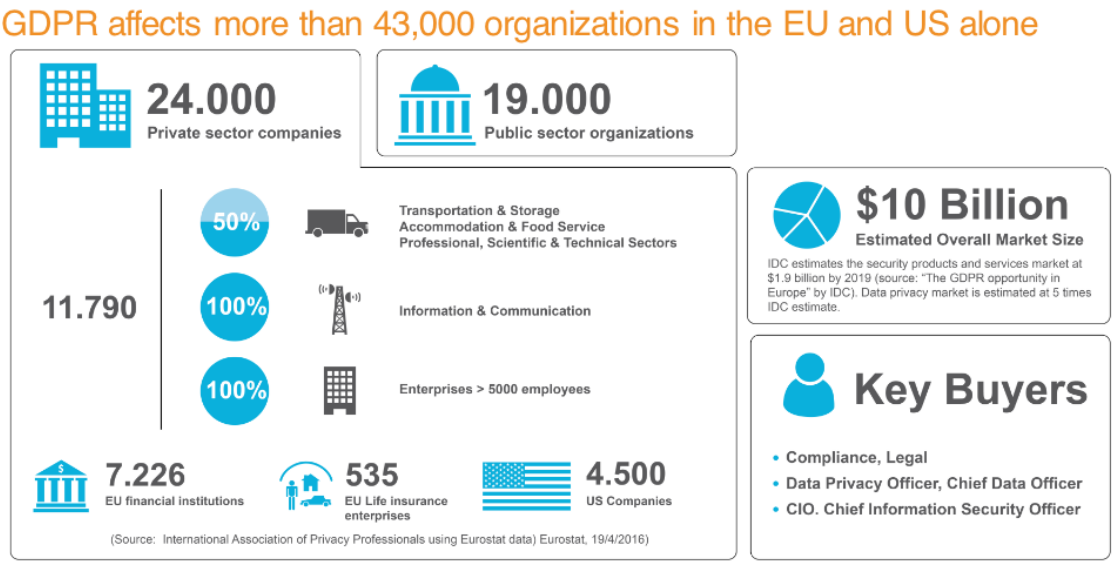
Cabe destacar, que **las sanciones se podrían duplicar** en caso de violaciones relacionadas con justificaciones Legales en lo relativo al procesamiento de datos, falta de consentimiento, derechos del individuo y transferencia de datos internacionales.

Por tanto, las posibles sanciones son, entre otras, una de las causas más que justificada para considerar la protección de Datos Personales en el 'top' de prioridades de cualquier empresa y, con ello, las oportunidades de mercado para las consultoras están a la orden del día.

Mercado

En el mundo actual las reglas de **privacidad** suponen un desafío para cualquier negocio y organización.

El RGPD requiere que muchas organizaciones implementen grandes **cambios en sus sistemas y procesos**, principalmente en aquéllas organizaciones que están inmersas en proyectos de Transformación Digital, tanto internos como externos para sus clientes.



Como consecuencia de todos estos cambios digitales y las relevantes políticas de privacidad ya vigentes, se podría decir que nos encontramos en una 'batalla' entre el cumplimiento de las normativas de **Privacidad frente a** los objetivos de **Innovación Digital**. En general, los clientes quieren sentirse protegidos y, entre tanto, existe el peligro de que el negocio se pueda resentir por las propias restricciones que supone la nueva regulación.

A modo de ejemplo, cabe destacar que la seguridad de una organización / empresa está más comprometida cuanto mayor es la base de clientes y, en consecuencia, muchos negocios pueden sentirse penalizados en su capacidad para crecer.

De la misma forma, el propio mercado demanda más y más experiencias personalizadas. Las áreas de negocio siguen planificando y/o ejecutando su agenda de **transformación digital** para satisfacer las necesidades internas y externas. En contraposición, **seguridad y privacidad cobran relevancia** modelando comportamientos que, junto con la regulación vigente, son cada vez más exigentes. Según Gartner, *"Technology strategic planners will see new spending driven by regulations and continued spending as organizations" (Gartner Forecast Analysis: Information Security, Worldwide, 1Q18).*

Así, las agendas digitales y de transformación de todos los negocios se están revisando teniendo en cuenta el RGPD. Tanto es así, que se puede decir que el éxito de los **proyectos de transformación digital** depende, en gran medida, de la habilidad de diseñar y asegurar como se

están procesando los datos de acuerdo con los nuevos requerimientos de seguridad y privacidad.

Algunas menciones de Gartner al respecto:

" […] poor CRM will lead to a privacy violation and a maximum GDPR sanction" (Gartner Predicts 2018: CRM and Customer Experience).

"CRM systems typically contain vast amounts of sensitive personal data and are kept for a considerable amount of time, making them a more likely sources of noncompliance with the EU General Data Protection Regulation (GDPR) than other applications" (Gartner Predicts 2018: CRM and Customer Experience).

De todo ello se deduce que ya existe mercado que demanda servicios y soluciones relacionados con el RGPD. Asimismo, se prevé un incremento importante de la demanda de servicios y soluciones para asegurar el cumplimiento de la normativa.

Las posibilidades de negocio son diversas y se pueden aplicar a cualquiera de las facetas que conlleva un proyecto de transformación de envergadura, cobrando especial importancia la evaluación, diseño e implantación de **medidas organizativas y técnicas de seguridad**.

Otros aspectos a tener en cuenta son:

- El almacenamiento de datos.
- Las certificaciones, como por ejemplo en los desarrollos.
- La implantación de las nuevas exigencias regulatorias.
- La identificación y mitigación de riesgos.

Por tanto, todo ello ofrece importantes **oportunidades** por explorar. No nos cabe duda de que las **soluciones y servicios para el cumplimiento e implementación del RGPD** en las organizaciones y empresas Europeas será una de las **palancas de crecimiento del mercado** en los próximos años.

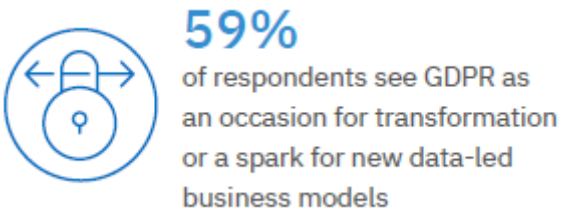
Impacto directo en las empresas

Como ya se ha anticipado, la nueva regulación RGPD trae consigo impactos a las organizaciones que necesitan afrontar este reto de forma extensa, si bien con un **criterio de proporcionalidad** (coste – beneficio), para evitar que se convierta en uno de sus puntos débiles.

De la misma forma, se estima indispensable un **cambio de mentalidad organizativa**, donde la privacidad ya forma parte del acervo cultural de cualquier empresa. Todo ello proporciona las bases que permitirán aprovechar la privacidad como elemento impulsor de la "experiencia de usuario" en cualquier servicio.

Se debe tener en cuenta que la normativa da especial relevancia a la responsabilidad, tanto en la faceta de ser responsable en el cumplimiento de las obligaciones del RGPD, como también en ser capaz de demostrar y evidenciar este cumplimiento. La adaptación a la nueva normativa, sin lugar a dudas, supone un esfuerzo muy importante para las compañías que tratan con datos personales de ciudadanos europeos.

Sin ir más lejos, la mitad de las empresas globales experimentan muchas dificultades en cumplir la normativa puesto que tienen que realizar cambios significativos en su operación, entre ellas la creación de una **Oficina de Protección de Datos** en la mayoría de los casos. Asimismo, algunas encuestas realizadas a ejecutivos de compañías destacan que el 59% de los encuestados ven el **RGPD como una oportunidad para la transformación de los nuevos modelos de negocio 'data-led'** *("The end of the beginning". IBM Institute for Business Value. Mayo 2018*).



El RGPD implica actuar no sólo en el área de tecnología, sino en cinco dimensiones de actuación dentro de cualquier empresa: **Organización, Gobierno, Procesos, Datos y Seguridad.**

- **Organización: personas, comunicación, reporting**

  · Identificación de roles, responsables, formación así como notificaciones internas/externas.
  · Roadmap de actuación, Reporting y Dashboard.

- **Gobierno**

  · Define la estrategia de privacidad de datos, políticas, estándares, guías y mejores prácticas.
  · Evaluación de la seguridad de datos, el análisis y gestión de riesgos operativos y el cumplimiento del reglamento, así como la creación de políticas y reglas de Gobierno y trazabilidad del Dato.

- **Procesos**

  · Establecer procesos de actuación, asegurando el cumplimiento de sus requerimientos en procesos operacionales y servicio.
  · Especial relevancia el proceso asociado a la Gestión del Consentimiento y la Gestión de los Derechos sobre mis Datos Personales.
  · Impacta múltiples procesos de negocio (HR, CRM, …), notificaciones de violaciones de seguridad, etc

- **Gestión de Datos**

  · Gestión completa del ciclo de vida y trazabilidad del dato personal, ya sea estructurado o no estructurado.
  · Conlleva la identificación y descubrimiento de datos personales, catálogo y gobierno (asegurando calidad de datos y linaje), almacenamiento y gestión segura de repositorios, enmascaramiento y anonimización de datos.

- **Seguridad**

  - Seguridad de Datos, Seguridad de Usuarios, Aplicaciones y Dispositivos, y Seguridad de Red.
  - Debe proteger el acceso legítimo a los datos lógicos y a los almacenados en formato físico, así como administrar y notificar infracciones de seguridad de datos dentro de un plazo establecido.
  - Responsable de prevención de fugas, gestión de vulnerabilidades, gestión de identidades y accesos, prevención de violaciones de seguridad, monitorización de seguridad y políticas de seguridad, análisis forense,...

Con todo ello, es lógico hacerse ahora la pregunta de qué medidas hay que tomar para cumplir con la normativa. Cualquier empresa tiene (ha tenido) que poner en marcha unas **medidas técnicas y organizativas** en relación con la naturaleza, alcance, contexto y propósito de la gestión y tratamiento que realice de los datos personales.

Para salvaguardar los datos, algunas de las medidas a implementar son:

- Encriptar o pseudo-anonimizar los datos.
- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.
- Restaurar la disponibilidad y acceso a los datos en tiempo y forma tras producirse un incidente físico o técnico.
- Introducir un proceso para la prueba, análisis y evaluación regular de la efectividad de los sistemas.

Últimas reflexiones

La aplicación del RGPD desde el 25 de mayo de 2018 ha supuesto y supone que muchas empresas tengan que desarrollar e implantar cambios muy relevantes en sus sistemas y procesos. Estos cambios se deben enmarcar dentro de proyectos de **Transformación Digital** que aseguren, entre otros objetivos, una protección de datos personales para sus clientes.

Por tanto, los proyectos de transformación digital ofrecen a las empresas de consultoría importantes oportunidades en nuestros clientes. Como mencionamos anteriormente, las soluciones y servicios para el cumplimiento e implementación del RGPD en las organizaciones y empresas Europeas será una de las **palancas de crecimiento del mercado** en los próximos años.

Es nuestra obligación, como empresas de consultoría, ayudar a los clientes en sus proyectos de Transformación Digital. Aprovechemos las oportunidades que se brindan en este contexto.