Data Centric

www.DataCentric.es

RGPD

TODO LO QUE NECESITAS SABER PARA NO "LIARLA"

Introducción

Los "datos" son ya un aspecto de importancia pública suficiente como para que su recopilación, uso y seguridad estén en el punto de mira del legislativo.

Sin embargo, la reactividad inherente a los gobiernos y la mayor celeridad del sector privado para comprender e implementar las nuevas tecnologías han hecho que, hasta ahora, el control sobre la gestión de la información sea aún tierra de nadie debido a que coexisten:

1. **Normativas redactadas en una etapa temprana del uso comercial de los datos.**
2. **Empresas que hacen un uso intensivo de los datos pero desconocen el alcance de la ley que lo regula.**
3. **Una relativa permisividad o carencia legal fruto de la "juventud" de estas leyes y la falta de medios de muchas empresas para un cumplimiento riguroso.**

Pero todo eso cambiará con el nuevo RGPD (Reglamento General de Protección de Datos) en 2018. Una directiva Europea mucho más madura, fruto de un estudio más concienzudo de las TIC, el uso comercial de la información, las repercusiones del mismo y las peticiones de los ciudadanos.

Fruto también de observar las carencias de las diferentes leyes de cada país en materia de protección de datos; carencias evidenciadas en los diferentes juicios que los principales "players" de los datos han enfrentado en Europa: Facebook, Google y muchas otras tecnológicas cuyo negocio nace y se cimenta en la información de los usuarios de sus plataformas.

1 La LOPD hasta ahora

La LOPD en España observa ciertas recomendaciones europeas en materia de protección de datos, pero mantenía cierta holgura. Ahora, la Unión Europea tomará las riendas de la privacidad de datos.

Por el mero hecho de pertenecer a la Unión Europea, España cuenta con medidas mucho más restrictivas que otros países como Estados Unidos o la práctica totalidad de Asia. Aún así, la LOPD está muy lejos de haber sido una de las leyes más "fuertes". Islandia, Suiza, Noruega o Rumanía, por ejemplo, son países con normativas mucho más protectoras de los datos personales.

En España, la Agencia Española de Protección de Datos es el organismo encargado de supervisar el cumplimiento de la LOPD. La ley, por su parte, establecía hasta ahora sanciones en 3 tramos:

Leves: *de 900 € a 40.000 €*
Graves: *de 40.001 € a 300.000 €*
Muy graves: *de 300.001 a 600.000 €*

Estas multas podían (y pueden, hasta mayo de 2018) venir motivadas por el incumplimiento de las empresas de las siguientes obligaciones:

- **Deber de información: la empresa debe comunicar al usuario al que pide sus datos todos los aspectos relacionados con ellos (uso al que dará, derechos, consecuencias).**
- **Consentimiento: el usuario debe aceptar la recopilación de sus datos.**
- **Acceso a los datos por terceros: los casos y responsabilidades vienen muy definidos en la LOPD.**

EN EL 2013, LA AEPD MULTÓ A GOOGLE CON 900.000€ POR INCUMPLIR 3 ARTÍCULOS DE LA LOPD.

2 El nuevo RDPG: qué cambia

El "nuevo" Reglamento General de Protección de datos fue aprobado el 27 de abril de 2016 por el Parlamento Europeo. Desde el 25 de mayo de 2018, los 28 Estados miembros deberán acatar las nuevas directrices pero, como casi toda ordenanza Europea, el RGPD es más una serie de vías a perfilar por cada país miembro dentro de su territorio.

Lo que sí está claro es que el remodelado de la Ley parte de una premisa clara: asegurar la privacidad y proteger la capacidad de decisión de compra de los consumidores. Dicho de otro modo, el foco del RGPD está en:

1 Que las empresas **solo puedan recabar datos de los usuarios previo consentimiento** y únicamente si disponen de una estructura tecnológica y de procedimiento que garantice su seguridad.

2 En el caso de querer elaborar un perfilado de usuarios mediante el tratamiento automatizado de sus datos, **debe garantizarse la protección de derechos, libertades e intereses de los usuarios.**

Con esta nueva medida de seguridad se pretende evitar que los encargados del tratamiento de datos evalúen aspectos sensibles y personales de los individuos, sin conocimiento ni aceptación de estos, para condicionar la oferta comercial que reciban.

Existirán, además, 3 casos en los que las empresas no pueden realizar una recopilación y tratamiento de datos de los usuarios con fines comerciales:

- **Evaluar la situación económica o de salud del usuario sin conocimiento o consentimiento de este, para definir una oferta comercial de créditos o seguros.**
- **Discriminar a candidatos para un empleo según su orientación sexual, opiniones políticas, estado de salud, u otros criterios de preferencia o intereses personales.**
- **Adaptar los precios de una página web en base al perfil del usuario.**

Si esto ocurre, el interesado tiene el derecho de pronunciarse y solicitar que no se apliquen a sus datos personales las operaciones de tratamiento automatizado (Derecho de limitación de tratamiento).

LA FILOSOFÍA DEL RGPD ES "DISEÑADO PARA LA PRIVACIDAD", Y PONE LA RESPONSABILIDAD EN LA PREVENCIÓN. UNA EMPRESA SERÁ CULPABLE, NO CUANDO SUS DATOS SEAN ROBADOS, SINO CUANDO NO HAYA PUESTO LOS MEDIOS INDICADOS EN CADA CASO PARA IMPEDIRLO.

3 nuevos principios de obligada observación

El RGPD nace de tres premisas que guiarán todas las obligaciones de la empresa y su violación puede suponer las sanciones más graves. Estos son:

- **Responsabilidad.** Las empresas deberán poder acreditar que cumplen todas las responsabilidades exigidas de ellas (seguridad, tratamiento, control, etc.).
- **Prevención.** Se exige de las empresas que garanticen la seguridad de los datos en función de la sensibilidad de los mismos y según las medidas aprobadas.
- **Transparencia.** Debe informarse inequívocamente al usuario de toda recopilación y uso de sus datos y, estos, ser aceptados por dicho usuario.

Cookies más claras, mayor transparencia y opt-in más visible

Uno de los primeros puntos de la nueva normativa es pedir al usuario su permiso expreso para recopilar sus datos. En España es algo que ya contempla la LOPD y el requerimiento solicita de la empresa que:

- **Informe al usuario** de que sus datos de navegación están siendo recopilados.
- **Pida al usuario la realización de una acción consciente** como pulsar un botón de "Acepto" para proceder a la recopilación de datos.
- **Permita al usuario modificar los permisos y borrar cookies** sin necesidad de aceptarlos con cada visita.

El Reglamento General de Protección de Datos hace especial hincapié en las personas y el consentimiento de datos. En este aspecto debes de saber que:

Las empresas tienen la obligación de ofrecer a los interesados información más amplia, de fácil acceso y transparente, sobre el tratamiento de sus datos y las consecuencias que conlleva.

El nuevo reglamento establece que el consentimiento de los interesados debe ser ***libre, inequívoco y específico.*** Lo que significa que el interesado debe afirmar y consentir de forma explícita el tratamiento de los datos personales.

3 Incumplirlo, qué conlleva

El aspecto que más se recrudece en el RGPD son las sanciones. ¡Y vaya si se recrudecen! Las nuevas cuantías que se prevén por incumplir la nueva normativa pueden ir directamente contra el volumen de negocio de las compañías que quiebren la Ley.

En los siguientes capítulos veremos en detalle las obligaciones concretas de las empresas. En función de cuál de ellos se haya descuidado, existirán dos nuevos bloques de sanciones (en lugar de los tres que establece la LOPD).

1. Primer tramo

Sanción: *hasta 10.000.000 € o un 2% de los ingresos anuales declarados el último año fiscal.*

Condiciones:

- *Se han recabado datos de menores sin su consentimiento o el de sus tutores legales.*
- *No se ha cumplido con las obligaciones técnicas del RGPD.*
- *No se ha registrado el tratamiento de los datos.*
- *No se ha realizado la Evaluación de Impacto.*
- *No se ha designado un DPO (Delegado de Protección de Datos).*

2. Segundo tramo

Sanción: *hasta 20.000.000 € o un 4% de los ingresos anuales declarados el último año fiscal.*

Condiciones:

- *Se han incumplido los principios del RGPD.*
- *Se violan los derechos de privacidad de los ciudadanos.*
- *No se cumplen los requisitos para transferencias internacionales de datos.*
- *Se incumple la resolución de la Autoridad de Control (o la AEPD en España).*

4 Tratamiento de los datos y organización de la empresa

La principal premisa en las obligaciones corporativas es que no todas las empresas tratan los mismos datos. Por tanto, ¿por qué deberían implementar todas las mismas medidas?

Es la propia empresa la que deberá decidir qué nivel de seguridad aplicar puesto que sobre ella recaerá la responsabilidad de salvaguardarlos.

Las empresas de menos de 250 empleados estarán exentas de estos requisitos, salvo que los datos que gestionen sean de alta sensibilidad (como sanitarios o penales).

Para discernir de qué nivel de protección deben dotar a sus sistemas y procesos de tratamiento de los datos, las medidas aprobadas en el RGPD establecen una serie de pasos y condiciones concretas que las empresas deberán dar y cumplir.

1. Entra en juego la auditoría de datos

El primero de estos pasos es realizar una evaluación de los riesgos que existen para la privacidad de los usuarios que hayan cedido sus datos y las medidas de protección a establecer, ponderando la naturaleza, sensibilidad y fines de los mismos. La llamada Evaluación de Impacto sobre la Privacidad

Con esta auditoría en mano, la empresa deberá acreditar con la AEPD:

- **Los datos que va a recabar** de los usuarios.
- **El uso** que va a hacer de esos datos.
- **Información de contacto del responsable** del tratamiento de los datos.
- **Programación de pruebas temporales** que aseguren la integridad del sistema.

2. Documentación de los procesos

Tras la evaluación del riesgo, la empresa deberá adecuar sus diferentes procesos de gestión de datos, de incidentes, de archivado, de conservación, de acceso a los sistemas, etc. Todo ello implementando medidas destinadas a la prevención de una violación de la privacidad de los usuarios registrados en el sistema.

3. Formación interna

El personal interno de la compañía, ligados al cumplimiento de los procesos de protección de datos de la misma por su contrato, deberán recibir formación relativa a la seguridad de los datos y su tratamiento.

4. Formulación de contratos

Los proveedores externos, por su parte, deberán firmar acuerdos de confidencialidad y presentar sus propias auditorías de riesgo antes de poder acceder a dichos datos.

5. Designación de un responsable de datos

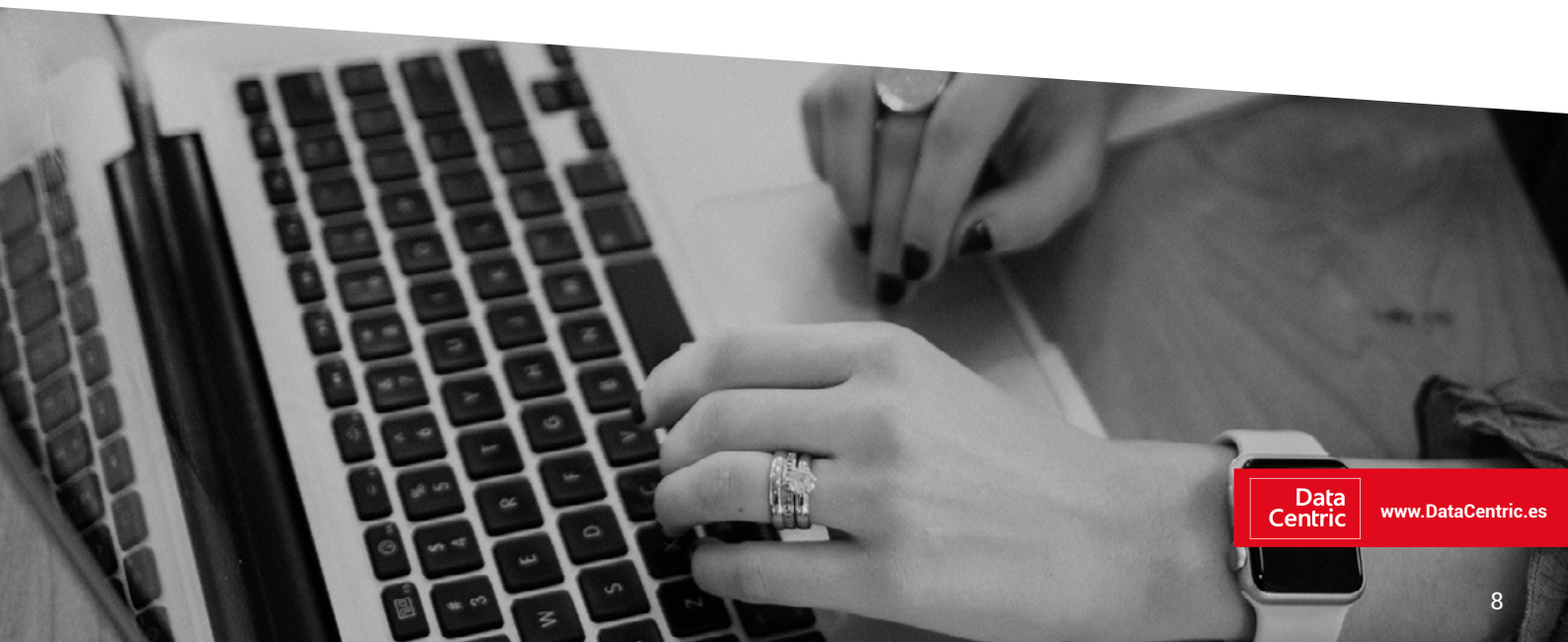
Las empresas deberán nombrar un Delegado de Protección de Datos (Data Protection Officer o DPO en inglés) que supervise todos los puntos anteriores y sirva de contacto a las administraciones necesarias. Esta figura podrá ser interna o externa.

6. Notificación de violación de la seguridad

En caso de producirse un fallo en la seguridad de los datos, las empresas tendrán dos obligaciones: detectarlo y notificarlo a la autoridad competente. Detectarlo, porque se supone que el sistema debe ser seguro y estar en todo momento controlado; notificarlo, de forma que la AEPD pueda supervisar y ayudar a solventar los problemas derivados de esta brecha en la seguridad.

Te resumimos 8 claves que contienen todo lo que no se te puede escapar con esta nueva normativa:

1. La gestión de los datos **debe realizarse dentro de la UE o países que hayan recibido su aprobación**, como Argentina o Suiza.
2. La cesión de los datos por parte del usuario debe ser **consentida libremente.**
3. El usuario que consiente la cesión de los datos **debe ser mayor, como mínimo, de 13 años**, según la normativa de cada país.
4. El uso de los datos debe cumplir con los principios de **licitud, lealtad, transparencia, caducidad, proporcionalidad, integridad y confidencialidad** establecidos.
5. El uso de datos no genera **ningún tipo de discriminación.**
6. Si el interesado lo solicita, los datos deben ser **transmitidos a un tercero.**
7. **No debe realizarse un uso comercial de los datos**, si el usuario no nos ha dado su consentimiento.
8. Los datos utilizados son **exclusivamente los necesarios para los usos estipulados** ante la AEDP.



5 ¿Sabes en qué te beneficia?

Ante el reto de adaptar la empresa a una nueva normativa (y más, cuando esa normativa puede acarrear una multa por valor de hasta el 4% de nuestros ingresos), se presenta una nueva oportunidad: gestionar aún mejor la información.

Al establecer una Evaluación de Riesgo y definir los usos que la empresa esté dando de los datos, ya estamos sentando las bases de una auditoría de la información en nuestra empresa. Una auditoría que, por un poco más de esfuerzo, puede convertirse a su vez en las bases de una estrategia de Big Data.

Mientras que contar con un DPO interno puede limitar su operatividad al mero cumplimiento de la ley, confiar en un partner tecnológico como DataCentric supone la ventaja añadida de tener a tu disposición un equipo que te ayude, además de en materia de seguridad:

- **Estableciendo las bases de una estrategia de Big Data en tu empresa.**
- **Analizando, normalizando, completando y corrigiendo tus BBDD.**
- **Segmentando tus BBDD y asignando scorings a cada registro en función de su potencial de negocio.**

En resumidas cuentas, tu empresa tiene la posibilidad, no solo de cumplir con la normativa que entrará en vigor en mayo de 2018, sino de sumarse a una nueva forma de gestionar la información para obtener insights de negocio que le aporten una ventaja competitiva real.

Conclusiones

Las empresas continúan madurando en el uso de la tecnología y la gestión de los datos. Cada día, surgen nuevas formas de recopilarlos y tratarlos. A esta tendencia, ahora, se suma como "key player" el Parlamento Europeo, estableciendo unas reglas de juego comunes.

Estas nuevas reglas acarrean más obligaciones, sí, pero también la oportunidad de adaptarnos a un nuevo tablero de juego y adquirir la ventaja de la salida. También, la ventaja de reorganizar nuestros procesos de captación y gestión de datos de forma que nos aporten mucho más valor del que nos aportan actualmente.

¿Cuáles son las claves del nuevo reglamento: qué cambia?

3 premisas guían las nuevas obligaciones empresariales: Responsabilidad > Prevención > Transparencia

- **Nuevas medidas de seguridad:** requieren una protección de los datos más rigurosa.
- **Mayor responsabilidad:** obligaciones de los encargados del tratamiento automatizado de datos.
- **Nuevas obligaciones de información y consentimiento del interesado:** Se obliga a dar consentimiento expreso para la cesión de datos.

Integrar el nuevo reglamento al día a día de tu empresa implica, a grandes rasgos, desarrollar gestiones preventivas y acreditar el cumplimiento y la gestión de responsabilidades a la AEPD.

¿Qué cambios a nivel de organización puedo ir implementando en mi empresa?

- ☐ *Realiza una Evaluación de Impacto sobre la Privacidad de los datos de los usuarios.*
- ☐ *Dependiendo de los resultados obtenidos, implanta la tecnología y metodología más adecuadas para disminuir los riesgos.*
- ☐ *Da formación a tu personal interno en materia de seguridad y tratamiento de datos.*
- ☐ *Firma nuevos contratos de confidencialidad con tus proveedores externos, que además, tienen la obligación presentar sus propias Auditorías de riesgo para poder acceder a los datos.*
- ☐ *Nombra a un Delegado de Protección de datos (DPO) para supervisar que cumples con todos los requisitos.*

Data Centric

business
consumer
location
insight

¿A qué espera para dotar a tu negocio de la mayor ventaja competitiva de todas? El conocimiento de tus clientes y el mercado

www.DataCentric.es