REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS y Proyecto LOPD

PRINCIPIOS Y GARANTÍAS PARA RESPONSABLES Y ENCARGADOS

Jesús Acevedo
@jesacevedo

Normativa española

- Constitución Española de 27 de diciembre de 1978
- Directiva 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. **(LOPD)**
- Real Decreto 1720/2007 de 21 de diciembre por el que de desarrolla la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. **(RD 1720)**
- Instrucciones de la Agencia Española de Protección de Datos
- RGPD Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, exigible a partir del 25 de Mayo de 2018.
- PLOPD

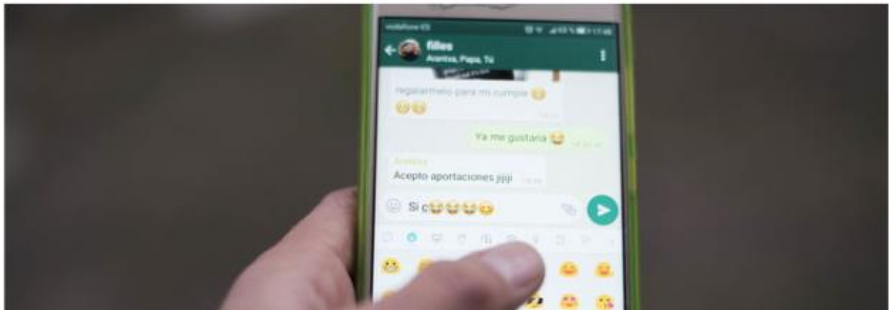
#RGPD Penalties Everywhere

Diario de Sevilla SOCIEDAD

ENTRA EN VIGOR EN MAYO

Incumplir la ley de Protección de Datos se sancionará con hasta 20 millones de euros

- Las empresas, autónomos y administraciones públicas, como encargados del tratamiento de los datos, tienen cuatro meses para aplicar medidas que garanticen y demuestren que cumplen la nueva normativa.



RGPD

A través del RGPD se consigue armonizar en todos los Estados miembros de la UE la dispersión normativa existente hasta entonces en materia de protección de datos. El RGPD por tanto es una norma única de aplicación directa a todos los Estados cuyo objetivo principal es otorgar un mayor control a los ciudadanos europeos sobre su información privada, y permitir una aplicación uniforme en toda la Unión Europea con el objetivo de alcanzar un nivel de protección de datos razonable en todo el territorio de la UE que evite la aplicación las diferentes normativas de cada Estado miembro.

La entrada en vigor del Reglamento, ¿supone que ya no se aplica la Ley Orgánica de Protección de Datos española?

- No. El Reglamento ha entrado en vigor el 25 de mayo de 2016 pero no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018. Hasta entonces, tanto la Directiva 95/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

PRINCIPIOS RGPD (art. 5)

Los datos han de ser tratados de manera lícita, leal y transparente en relación con el interesado :

(«Licitud, Lealtad y Transparencia»)

- **Principio de limitación de la finalidad:** se rectifiquen o supriman los datos personales de forma que sean inexactos.
- **Principio de adecuación y minimización de datos:** deben ser objeto de tratamiento los datos estrictamente necesarios atendiendo a los fines del tratamiento.
- **Principio de exactitud de los datos:** se rectifiquen o supriman los datos personales de forma que sean inexactos.
- **Principio de limitación del plazo de conservación**: la vinculación entre los datos y su titular tiene que ser el estrictamente necesario en función del tratamiento para el cual se ha recabado el consentimiento del afectado.
- **Integridad y confidencialidad:** garantizar una seguridad adecuada con medidas adecuadas.

Principio de Accountability

¿Qué implica la responsabilidad activa recogida en el Reglamento?

Las empresas deben **adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD establece**.

El Reglamento entiende que *actuar* ***sólo cuando ya se ha producido una infracción es insuficiente como estrategia***, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Todo tratamiento de datos personales exige una base jurídica que lo legitime, a saber (artículo 6 RGPD):

- Consentimiento de afectado.
- Existencia de una relación contractual.
- Existencia de un interés legítimo prevalente del responsable o de terceros a los que se ceden o comunican los datos personales.
- Justificado en una necesidad vital del interesado.
- Cuando resulte una obligación legal para el responsable del tratamiento.
- Exista un interés público o se derive del ejercicio de poderes públicos.

Principio de Accountability

¿Qué implica la responsabilidad activa?

- Mantenimiento de un registro de tratamientos.

- Realización de evaluaciones de impacto sobre la protección de datos

- Medidas de seguridad según el riesgo de cada tratamiento.

Principio de Accountability

¿Qué implica la responsabilidad activa?

- Protección de datos desde el diseño.

- Protección de datos por defecto.

Principio de Accountability

¿Qué implica la responsabilidad activa recogida en el Reglamento?

-- Notificación de violaciones de la seguridad de los datos.

-- Promoción de códigos de conducta y esquemas de certificación.

Principio de Accountability

-- Mediación con los afectados por los tratamientos.

-- Comunicación activa con las autoridades de Control.

Principio de Accountability

Enfoque basado en el riesgo

El DPD deberá «considerar debidamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento».

Análisis de riesgos

¿Cuáles pueden ser los factores de riesgo?

- los tipos de tratamientos,
- la naturaleza de los datos,
- el número de interesados afectados,
- la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Registro de tratamientos

El mantenimiento de los registros

Es el responsable o el encargado del tratamiento, no el DPD, quien

- está obligado a «mantener un registro de las operaciones de tratamiento de las que es responsable» o
- «mantener un registro de todas las categorías de actividades de tratamiento llevadas a cabo en nombre de un responsable del tratamiento».

Encargado de tratamiento

- El RGPD exige en su artículo 28 y el PLOPD en su art. 33, que las relaciones responsable/encargado del tratamiento se regulen en un contrato, o en un acto jurídico.

- Se regula, por otra parte, de una forma minuciosa, el contenido mínimo de los contratos de encargo con acceso a datos por cuenta de terceros.

- Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

Encargado de tratamiento

- **El nuevo RGPD no realiza la tradicional distinción entre los niveles de seguridad (BASICO-MEDIO-ALTO).**

- **En el artículo 32.2, se dispone que al evaluar la adecuación del nivel de seguridad se tendrán en cuenta los riesgos que presente el tratamiento de datos , en particular:**

- como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma,

- la comunicación o acceso no autorizados a dichos datos.

- **Es decir, para evaluar el nivel de seguridad debe analizarse el caso concreto, atendiendo a los concretos riesgos que presente el tratamiento de datos personales.**

Con independencia del nivel de aplicación, **deben ser aplicadas tanto por el responsable del fichero como por el encargado del tratamiento.**

Obligatoriedad del DPD - RGPD

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) 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.

Obligatoriedad del DPD - RGPD

Obligatoriedad del DPD - PLOPD

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión.

i) Los distribuidores y comercializadores de energía eléctrica, y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Obligatoriedad del DPD - PLOPD

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a lo dispuesto en la Ley 3/2011, de 27 de mayo, de regulación del juego.

ñ) Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Perfil del DPD

El RGPD establece que **el DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos** y a su capacidad para desempeñar sus funciones.

En su artículo 37.6, el RGPD dice:

"El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios."

Perfil del DPD

1) **Formación y Competencia Profesional**
2) **Independencia**
3) **Ausencia conflicto de intereses.**
4) **Habilidades de Negociación.**
5) **Trabajo en equipo.**
6) **Liderazgo.**
7) **Comunicación.**

Cumplimiento real y no formal.

Gracias

CEA
Confederación de
Empresarios de Andalucía

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA Y CONOCIMIENTO