CLAVES PRÁCTICAS
FRANCIS LEFEBVRE

Kit de herramientas para el delegado de protección de datos

Fecha de edición: 5 de febrero de 2020

Esta monografía de la Colección
CLAVES PRÁCTICAS
es una obra editada por iniciativa y bajo
la coordinación de
Francis Lefebvre

MIGUEL RECIO GAYO
Profesor asociado de la Universidad CEU San Pablo de Madrid.
Abogado de CMS Albiñana & Suárez de Lezo

Lefebvre-El Derecho, S. A.
Monasterios de Suso y Yuso, 34. 28049 Madrid. Teléfono: 91 210 80 00.
Fax: 91 210 80 01
www.efl.es
Precio: 30,16 € (IVA incluido)

ISBN: 978-84-17985-63-9
Depósito legal: M-5429-2020

Impreso en España por Printing'94
C/ Orense, 4 (2ª planta) – 28020 Madrid

Plan general

Abreviaturas

AEPD	Agencia Española de Protección de Datos
art.	artículo
CCN	Centro Criptológico Nacional
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CEPD	Comité Europeo de Protección de Datos
CERT	Equipo de Respuesta ante Emergencias Informáticas *(Computer Emergency Response Team)*
CNMC	Comisión Nacional de los Mercados y la Competencia
Dict	Dictamen
Dir	Directiva
DNI	Documento Nacional de Identidad
DPD	Delegado/a de Protección de Datos
EEE	Espacio Económico Europeo
EIPD	Evaluación de Impacto relativa a la Protección de Datos
ENAC	Entidad Nacional de Acreditación
ENS	Esquema Nacional de Seguridad
GT29	Grupo de Trabajo del artículo 29
INCIBE	Instituto Nacional de Ciberseguridad
ISO	Organización Internacional de Normalización *(International Organization for Standardization)*
ITU	Unión Internacional de Comunicaciones *(International Telecommunications Union)*
L	Ley
LCSP	Ley de contratos del sector público (L 9/2017)
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LO 3/2018)
LPH	Ley de propiedad horizontal (L 49/1960)
LSSI	Ley de servicios de la sociedad de la información y de comercio electrónico (L 34/2002)
PYME	Pequeña y Mediana Empresa
RD	Real Decreto
RDL	Real Decreto-ley
Rgto	Reglamento
RGPD	Reglamento del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Dir 95/46/CE (Rgto UE/2016/679)
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
UIP	Unidad de Información sobre los pasajeros

Capítulo 1. Tratamiento de datos personales

1. Derecho fundamental a la protección de datos y cumplimiento

50

60

Modelo europeo actual de protección de datos El nuevo modelo de protección de datos personales al que da lugar el Rgto UE/2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Dir 95/46/CE (en adelante, también RGPD o el Reglamento) supone un **cambio relevante** con respecto a esta Directiva (la primera a nivel europeo en materia de protección de datos personales, vigente durante veinte años).

La Exposición de Motivos de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD), indica que se produce un cambio o evolución de un modelo basado, fundamentalmente, en el **control del cumplimiento**, a otro que descansa en el principio de responsabilidad proactiva (***accountability***), lo que exige una **previa valoración** tanto por el responsable como por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas técnicas y organizativas adecuadas para minimizar el riesgo.

65 Superada la que podría denominarse primera etapa europea del derecho fundamental a la protección de datos (que tenía como objetivos específicos armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con el tratamiento de los datos personales), el RGPD tiene el objetivo específico de establecer un **marco más sólido y coherente** en la materia (RGPD considerando 7).

Es también la primera vez que la normativa europea menciona expresa y específicamente:

– la Carta de los Derechos Fundamentales de la Unión Europea art.8 (en adelante, CDFUE);

– el Tratado de Funcionamiento de la Unión Europea art.16 (en adelante, TFUE).

Se entra en una **nueva etapa** marcada, en particular, por el hecho de que el RGPD es directamente aplicable reservando a la ley nacional únicamente, como ha indicado la Comisión Europea, la oportunidad de precisar las normas de protección de datos en **sectores específicos** (COM(2018) 43); en concreto:

- sector público;
- empleo y seguridad social;
- medicina preventiva y medicina laboral;
- sanidad pública;
- archivo con fines de interés público;
- investigación científica o histórica o con fines estadísticos;
- número nacional de identificación;
- acceso público a los documentos oficiales, y
- obligaciones de secreto.

Además, los Estados miembros pueden mantener o introducir **condiciones adicionales o limitaciones** en el caso de datos:

– genéticos;
– biométricos, y
– relativos a la salud.

75 **Ámbito competencial** Con el RGPD se produce también una **delimitación** del ámbito competencial del:

– legislador y juez europeo y,
– legislador y jueces nacionales.

En este sentido, es necesario considerar que:

1. El CDFUE art.8, que reconoce y consagra el derecho fundamental a la protección de datos personales de manera independiente a otros derechos fundamentales, constituye ahora la **norma que guía** al legislador nacional en la regulación de este derecho.

2. Si bien los tribunales nacionales pueden interpretar el derecho europeo de protección de datos personales, es el Tribunal de Justicia de la Unión Europea (TJUE) en última instancia quien lo haga en virtud del planteamiento de una **cuestión prejudicial** dirigida a que este se pronuncie, con carácter **vinculante** tanto para el órgano jurisdiccional nacional que la haya planteado como para el resto de los órganos jurisdiccionales nacionales de la Unión Europea, sobre la interpretación o validez del Derecho de la Unión Europea.

2. Significado de los datos personales

90 Aunque la cuestión relativa a qué son los datos personales podría considerarse como una cuestión sin mayor trascendencia dado que el concepto de datos personales parece suficientemente asentado, no es así. Buena muestra de lo anterior es el hecho de que el Grupo de Trabajo del art.29 (en adelante, GT29), que fue creado en virtud del citado artículo de la Dir 95/46/CE y que actualmente está incorporado en el Comité Europeo de Protección de Datos (en adelante, CEPD), dedicase uno de sus dictámenes al concepto de datos personales.

El GT29, consciente entonces de la necesidad de llevar a cabo un profundo análisis del concepto de datos personales, trató este asunto en el Dict 4/2007 sobre el concepto de datos personales, WP 136, que fue adoptado el 20 de junio. Y a pesar de que se trata de un documento adoptado hace más de una década, sigue siendo relevante ya que, entre otras cuestiones, incluye algunas **claves** para entender el **alcance de la normativa** sobre protección de datos personales.

Es así que atendiendo al citado dictamen y al RGPD, las claves a considerar en relación con el concepto de protección de datos personales se refieren a:

- la **proporcionalidad** en la aplicación de la normativa en la materia (nº 110 s.), y
- que esta normativa cuenta con **excepciones** (nº 180).

PRECISIONES Por último, la Comisión Europea (2019) ha indicado que el hecho de que «la definición de datos personales sea tan amplia es intencional, manteniéndose prácticamente sin cambios en el Reglamento general de protección de datos, en comparación con la legislación anterior».

a. Proporcionalidad en la aplicación de la normativa

110 En el siguiente epígrafe se analiza el significado y alcance de la proporcionalidad (nº 115), las categorías de interesados y de datos personales (nº 120), la aplicación de la normativa sobre protección de datos personales (nº 130), la proporcionalidad en la aplicación del derecho a la protección de datos (nº 135), la existencia de fuentes accesibles al público (nº 140) y la cuestión acerca de los datos personales obtenidos de fuentes de acceso público y hechos manifiestamente públicos (nº 150).

115 **Significado y alcance** Es importante tener en cuenta que la normativa sobre protección de datos es aplicable cuando exista un **tratamiento de datos personales**, salvo que concurra alguna excepción.

Esto implica que el hecho de estar ante datos personales no implica que de manera automática, se aplique la normativa sobre protección de datos personales. No obstante, es importante reparar en el hecho de que el **concepto de tratamiento** es también muy amplio.

En este sentido, puede plantearse de manera gráfica en los siguientes términos:

120 Categorías de interesados y de datos personales Es importante identificar:

– **de quién** se tratan los datos personales y
– **qué** datos personales se tratan.

Esta información puede ser necesaria para, entre otras obligaciones:

1. Analizar el riesgo que implica el tratamiento.

2. Cumplimentar el registro de actividades del tratamiento.

3. Llevar a cabo la evaluación de impacto relativa la protección de datos.

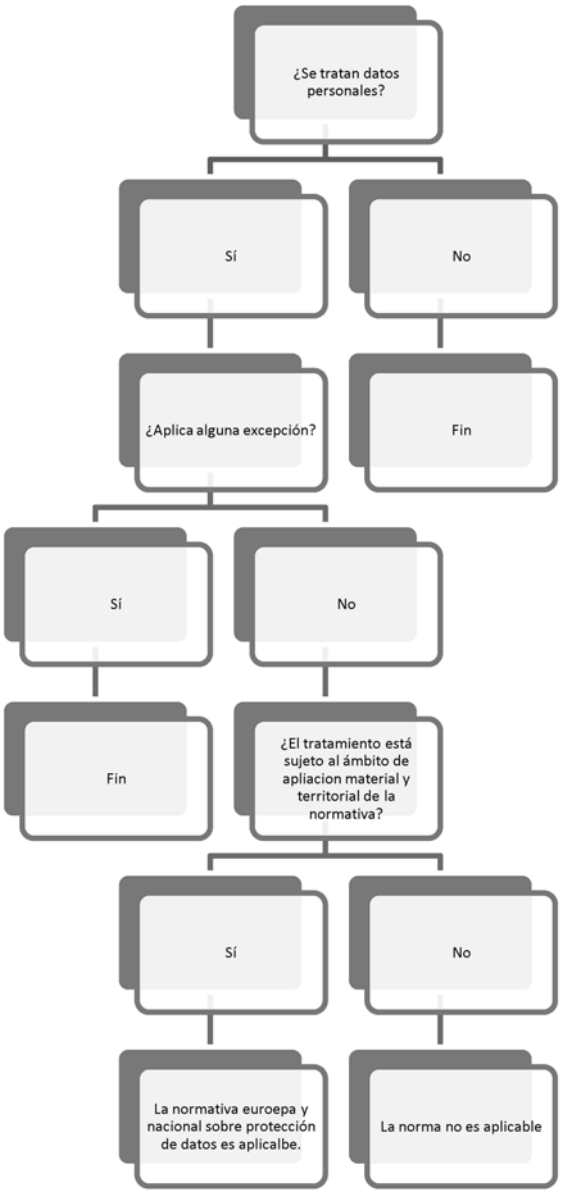
A continuación se incluye un listado que no tiene carácter exhaustivo pero que puede resultar de ayuda en la identificación de las categorías de interesados y de datos personales tratados: **125**

Categorías de	Listado
Interesados	Clientes Pre-clientes Interesado (ámbito administrativo) Representante del interesado (ámbito administrativo) Asociados Empleados Antiguos empleados Candidatos a un puesto de trabajo Becarios Colaboradores Proveedores Empresario individual Persona de contacto en una empresa Profesores Investigadores Alumnos Usuarios Deudor Denunciante (sistema de denuncias internas) Denunciante (infracciones del Derecho de la UE) Denunciado (sistema de denuncias internas o infracciones del Derecho de la UE) Infractor Imputado Condenado Cargos públicos Ciudadanos Residentes Contribuyentes Pacientes Propietarios Visitantes Padres o tutores Representantes legales Signatarios de un contrato

Categorías de	Listado
Datos personales	Datos identificativos Características personales Circunstancias sociales Datos de autenticación del usuario Números únicos de identificación de la persona y firma Identificadores seudonimizados Información biométrica Datos de contacto Datos de gestión de personal Datos de transacciones Datos bancarios, financieros y de seguros Datos laborales o de empleo Datos profesionales Datos de salud Otras categorías especiales de datos Datos de imagen/voz Datos sobre el cliente (*know your customer*, KYC) y diligencia debida Datos relativos a los ciudadanos (Administraciones Públicas) Datos relativos a antecedentes penales Datos relativos a infracciones y sanciones penales Datos relativos a medidas cautelares Datos relativos a infracciones y sanciones administrativas Datos relativos a educación o formación académica Datos relativos a beneficios que recibe el interesado Datos relativos a comunicaciones Datos de servicios recibidos por los clientes Datos relativos a actividad del usuario Datos relativos a contenido Datos de localización o geolocalización Datos relativos a dispositivos del usuario Perfil del interesado

130 Aplicación de la normativa sobre protección de datos personales

En definitiva, el responsable o encargado del tratamiento y, en particular el **Delegado de Protección de Datos** (en adelante, DPD), cuando informa o asesora a los anteriores, debe tener en cuenta que determinar si la normativa sobre protección de datos personales es aplicable o no pasa por **aplicar el siguiente esquema** en cuanto a si aquella aplica o no:



Proporcionalidad en la aplicación del derecho a la protección de datos Implica que cuando se tratan datos personales debe tenerse en cuenta su interrelación con otros derechos fundamentales, ya que no es un derecho absoluto. **135**

En este sentido: «el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la

sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad» (RGPD considerando 4).

140 ¿Existen las fuentes accesibles al público? Sí, aunque la aplicación del RGPD requiere analizar específicamente la base de legitimación del tratamiento.

En relación con esta cuestión, la **Agencia Española de Protección de Datos** (en delante, AEPD) ya indicó, en respuesta a una consulta en la 10ª sesión anual abierta, que con el RGPD no puede hablarse de un concepto legal de «fuentes accesibles al público» como el que existía en la derogada LO 15/1999, ni tampoco de que los datos que aparezcan en este tipo de fuentes legitime sin más el tratamiento.

En concreto, explica en relación con esto último que, aunque un dato personal pueda ser **accesible por cualquiera**, lo que puede ser tenido en cuenta para realizar la ponderación del interés legítimo, esto no implica que el tratamiento de los datos personales sea lícito, siendo necesario respetar los principios del tratamiento de los datos personales, entre los que se encuentra la necesidad de tener una **base de legitimación** del tratamiento (nº 1500 s.).

Es decir, si se tratan datos personales obtenidos de una fuente de acceso público será necesaria una base de legitimación del tratamiento de los datos personales.

150 ¿Son lo mismo los datos personales obtenidos de fuentes de acceso público que hechos manifiestamente públicos? (RGPD art.9) No.

Aunque no exista actualmente un concepto legal de fuente de acceso público, resulta claro que se trataría de datos personales **accesibles por cualquiera**, en los términos ya expresados, mientras que los datos personales hechos manifiestamente públicos son aquellos que la persona **ha decidido revelar**.

Al respecto, el Consejo de Estado, en su dictamen sobre el Anteproyecto de Ley Orgánica de Protección de Datos Personales, indicó que podría resultar lógico entender que quien publica manifiestamente sus propios datos personales debe asumir las **consecuencias** de su actuación, y a ello se añade que el propio RGPD permite, como excepción a la regla general prohibitiva, el tratamiento de los datos «sensibles» enumerados en el art.9.1 cuando el interesado los haya hecho manifiestamente públicos (RGPD art.9.2.e). Parece lógico concluir que, si el RGPD permite el tratamiento en el caso de los datos sensibles hechos manifiestamente públicos, debería hacerlo también en relación con los que no tienen esta característica y son, por tanto, merecedores de un **grado de protección inferior**.

155 Hay que tener en cuenta que establece expresamente, en relación con el tratamiento de estos datos sensibles, que «además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento» (RGPD considerando 51).

De lo anterior podría deducirse que (aunque en este punto la interpretación del Reglamento tampoco es clara), sin perjuicio de la concurrencia de uno de los supuestos de excepción a la prohibición general de tratamiento del RGPD art.9.2, el tratamiento ha de ser **lícito** al amparo de una de las circunstancias de su art.6.1, lo que en ocasiones puede dar lugar a exigencias redundantes, pero en casos como el contemplado en la letra e), podría interpretarse que el tratamiento de los datos sensibles hechos manifiestamente públicos por el interesado solo será lícito si:

– responde, por ejemplo, a una **obligación legal**, o
– si el afectado ha dado su **consentimiento expreso**.

En otro caso, habría que entender que el Reglamento presenta una grave incoherencia interna, excepcionando precisamente para el tratamiento de datos sensibles la exigencia general de que el consentimiento del afectado, cuando sea base del tratamiento, sea expreso.

b. Excepciones a la aplicación del RGPD y de la LOPD

180

Es decir, quedarían excluidos de la aplicación de la normativa sobre protección de datos los tratamientos de datos:

1. **Excluidos** del ámbito de aplicación del Derecho de la UE.

2. Llevados a cabo por los Estados miembros en el ámbito de aplicación del TUE título V capítulo 2: **política exterior y de seguridad común**.

3. Por **autoridades competentes** con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención:

– En este caso es aplicable la Dir UE/2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

4. De **personas fallecidas**, salvo por lo que se refiere al acceso, rectificación o supresión de personas fallecida en virtud de la LOPD art.3.

5. Sometidos a la normativa sobre protección de **materias clasificadas**.

190 En el caso de la **LOPD**, debe tenerse en cuenta que en los casos que se indican a continuación, si bien aquella no es aplicable, se remite a la normativa específica:

Tratamientos de datos relativos a	Previsión
Actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea	«se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles».
Tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial	«se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables».

195 Por lo tanto, es necesario considerar si aplica alguna de las excepciones anteriores, ya que esto supondrá que no sean aplicables ni el RGPD ni la LOPD, sin perjuicio de que los tratamientos que se llevasen a cabo, en los casos relativos a las actividades no comprendidas en el ámbito de aplicación del Derecho de la UE y en la tramitación por los órganos judiciales de los procesos de los que sean competentes, es decir, en el ejercicio de sus funciones jurisdiccionales, así como el realizado dentro de la gestión de la Oficina Judicial, queden sujetos a la normativa específica que sea aplicable en su caso.

3. Categorías de datos personales

210 A continuación se analiza una clasificación de los datos personales (nº 215), así como la posibilidad de encontrar otro tipo de categorías (nº 220).

215 **Clasificación** Atendiendo a la normativa sobre protección de datos personales cabe distinguir tres categorías de datos personales, que son:

Esta clasificación, que atiende a la naturaleza de los datos personales tratados, es una decisión del legislador europeo, al que sigue el legislador nacional.

En cualquier caso, es importante tener en cuenta que el legislador podría modificar el listado de categorías especiales de datos y de hecho a nivel nacional