Persevera

AL ALCANCE DE QUIEN ESTUDIA

BLOQUE II · ORGANIZACIÓN DE OFICINAS PÚBLICAS

Tema 4

Protección de datos y derechos digitales

Cuerpo General Administrativo de la Administración del Estado

INGRESO LIBRE · EDICIÓN 2026

perseveraoposiciones.com

AL ALCANCE DE QUIEN ESTUDIA

Estudiar una oposición ya cuesta bastante. Dinero, tiempo, esfuerzo. Lo que se ofrece habitualmente añade fricción: temarios caros y no redistribuibles, academias con horarios fijos y mensualidades que no todos pueden pagar.

Persevera publica los temarios enteros, en abierto. Lees, copias, imprimes y compartes con quien quieras.

Esta es la primera entrega. Los siguientes cuerpos los decidiremos contigo: nos cuentas qué oposición te interesa.

El temario es un producto vivo: hay erratas, hay matices que pueden afinarse, hay decisiones de redacción que pueden discutirse. Si encuentras algo que pueda mejorar, escríbenos. Lo leemos todo y publicamos las correcciones.

ÍNDICE

TEMA 4

Epígrafe 1 — La protección de datos personales y su régimen jurídico

1. Fundamento constitucional y europeo

La protección de datos personales tiene una **triple base normativa de rango superior**: la Constitución Española (art. 18.4 CE), la Carta de los Derechos Fundamentales de la Unión Europea (art. 8 CDFUE) y el Tratado de Funcionamiento de la Unión Europea (art. 16 TFUE). En el ordenamiento español está conectada con el derecho al honor, a la intimidad personal y familiar y a la propia imagen del art. 18.1 CE, pero ha sido perfilada por la jurisprudencia constitucional como **derecho fundamental autónomo** —el llamado *derecho a la autodeterminación informativa*— vid. STC 292/2000.

Artículo 18 CE · Honor, intimidad, imagen, domicilio, comunicaciones y limitación de la informática

> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

El **art. 18.4 CE** es un **mandato constitucional al legislador** para que limite el uso de la informática en garantía del honor, la intimidad y los demás derechos fundamentales. La

ley a la que remite el 18.4 ha tenido tres versiones sucesivas en el ordenamiento español: la **LO 5/1992 LORTAD**, la **LO 15/1999 LOPD** y, hoy, la **LO 3/2018 LOPDGDD**, que se complementa con el RGPD europeo de aplicación directa.

Artículo 8 CDFUE · Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Artículo 16 TFUE · Protección de datos en el Derecho de la Unión

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

> Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

El art. 8 CDFUE eleva la protección de datos a la categoría de derecho fundamental de la Unión, **distinto del derecho al respeto de la vida privada y familiar del art. 7 CDFUE**. El art. 16 TFUE habilita al legislador europeo (Parlamento Europeo + Consejo, procedimiento legislativo ordinario) para adoptar las normas de desarrollo y exige el control por autoridades independientes —habilitación de la que nace, precisamente, el RGPD.

> **RECUERDA**
>
> **Triple base del derecho fundamental a la protección de datos**: art. 18.4 CE (autonomía constitucional · mandato al legislador) · art. 8 CDFUE (derecho fundamental de la Unión) · art. 16 TFUE (habilitación legislativa europea + control por autoridades independientes).

2. Las dos normas de cabecera del régimen jurídico

El régimen jurídico vigente se asienta sobre dos instrumentos de rango y naturaleza distintos que operan de manera **complementaria, no alternativa**:

Norma	Naturaleza jurídica	Publicación / aplicación	Objeto
Reglamento (UE) 2016/679 – RGPD	Reglamento de la Unión Europea (art. 288 TFUE)	DOUE L 119/1 de **4/05/2016** · entrada en vigor el 25/05/2016 (a los 20 días) · **aplicable desde el 25/05/2018** (a los dos años, art. 99 RGPD)	Protección de las personas físicas respecto al tratamiento de sus datos personales y libre circulación de esos datos
Ley Orgánica 3/2018, de 5 de diciembre – LOPDGDD	Ley orgánica española (con partes ordinarias, ver más abajo)	BOE núm. 294 de **6/12/2018** · entrada en vigor el **7/12/2018** (disp. final 16.ª: «día	Adaptar el ordenamiento español al RGPD, completar sus disposiciones y garan-

		siguiente al de su publicación en el Boletín Oficial del Estado»)	tizar los derechos digitales (mandato del art. 18.4 CE)

El RGPD es **directamente aplicable** sin necesidad de transposición (art. 288, párrafo segundo, TFUE: «el reglamento […] será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro»); los Estados miembros conservan, no obstante, un margen normativo para concretar los aspectos que el propio Reglamento les remite expresamente. La LOPDGDD ejercita ese margen: no es una norma de transposición —los reglamentos UE no se transponen—, sino una norma de **adaptación y desarrollo** del RGPD en el ordenamiento español que, además, incorpora un Título X dedicado a los **derechos digitales** que excede la materia armonizada europea.

La **disposición final 1.ª LOPDGDD** desglosa la naturaleza jurídica de la ley con detalle: la regla general es el carácter orgánico, pero tienen carácter de **ley ordinaria** el Título IV; el Título VII (salvo arts. 52 y 53); el Título VIII; el Título IX; los arts. 79, 80, 81, 82, 88, 95, 96 y 97 del Título X; las disposiciones adicionales (salvo la 2.ª y la 17.ª); las disposiciones transitorias; y las disposiciones finales (salvo la 1.ª, 2.ª, 3.ª, 4.ª, 8.ª, 10.ª y 16.ª).

MATIZ

No toda la LOPDGDD es ley orgánica. Conforme a la disp. final 1.ª, tienen carácter **ordinario** los Títulos IV, VIII y IX, la mayor parte del VII (salvo arts. 52-53) y buena parte del Título X (arts. 79-82, 88, 95-97), además de casi todas las disposiciones adicionales, transitorias y finales. La fórmula es habitual en leyes orgánicas con contenido mixto: solo el núcleo materialmente reservado a ley orgánica conserva esa naturaleza.

MATIZ

Tres fechas de la LOPDGDD que se confunden: firma del Rey el **5 de diciembre de 2018**, publicación en el BOE el **6 de diciembre** y entrada en vigor el **7 de diciembre** («día siguiente al de su publicación»). El RGPD, en cambio, distingue **entrada en vigor** (25-5-2016, a los 20 días de su publicación en el DOUE) y **aplicación** (25-5-2018, a los dos años): en el periodo intermedio el Reglamento ya estaba vigente, pero todavía no era exigible.

MATIZ

Tres leyes orgánicas sucesivas han desarrollado el art. 18.4 CE: **LO 5/1992 LORTAD** (Regulación del Tratamiento Automatizado de Datos, derogada por la LO 15/1999) · **LO 15/1999 LOPD** (Protección de Datos de Carácter Personal, derogada por la LO 3/2018) · **LO 3/2018 LOPDGDD** (vigente). Cualquier referencia normativa actual a la LOPD o a la LORTAD remite a normas derogadas.

3. Conceptos clave del RGPD — art. 4

El art. 4 RGPD contiene veintiséis definiciones. Las quince primeras son las que vertebran toda la materia y se reproducen literalmente del DOUE L 119:

Artículo 4 RGPD · Definiciones (nº 1-15)

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o

uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros,

determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

nº	Concepto	Idea-fuerza
1	Dato personal	Información sobre persona física identificada o **identificable** («interesado»). Identificable = puede determinarse directa o indirectamente
2	Tratamiento	Cualquier operación sobre datos, automatizada o no (recogida, registro, conservación, comunicación, supresión…)
3	Limitación del tratamiento	Marcado de los datos para limitar su tratamiento futuro
4	Elaboración de perfiles	Tratamiento automatizado para evaluar aspectos personales (rendimiento, salud, preferencias, comportamiento, ubicación, movimientos)
5	Seudonimización	Datos que ya no pueden atribuirse a un interesado sin información adicional separada y protegida

6	Fichero	Conjunto estructurado de datos accesibles con arreglo a criterios determinados
7	Responsable	Quien determina **fines y medios** del tratamiento (solo o junto con otros)
8	Encargado	Quien trata datos **por cuenta del responsable**
9	Destinatario	A quien se comunican datos (sea o no tercero); **excepción**: autoridades públicas en investigación concreta
10	Tercero	Persona distinta del interesado, responsable, encargado y de quienes actúan bajo su autoridad directa
11	Consentimiento	Manifestación libre, específica, informada e inequívoca + declaración o clara acción afirmativa
12	Violación de la seguridad	Destrucción, pérdida o alteración accidental o ilícita; o comunicación/acceso no autorizados
13	Datos genéticos	Características genéticas heredadas o adquiridas; análisis de muestra biológica
14	Datos biométricos	Características físicas, fisiológicas o conductuales que permitan la identificación única (imagen facial, datos dactiloscópicos)
15	Datos relativos a la salud	Salud física o mental, incluida la prestación de servicios sanitarios

RECUERDA

Responsable vs. encargado. Responsable = «**Para qué + Cómo**» (determina fines y medios). Encargado = «**Por cuenta de**» (trata datos por cuenta del responsable). El responsable puede serlo solo o conjuntamente con otros (corresponsabilidad, art. 26 RGPD); el encargado nunca actúa por sí mismo, siempre por cuenta del responsable.

RECUERDA

Seudonimización ≠ anonimización. Los datos seudonimizados **siguen siendo datos personales** porque la reidentificación es posible con la información adicional separada. Los datos anonimizados quedan fuera del ámbito del RGPD porque la reidentificación es imposible.

MATIZ

«Destinatario» NO equivale a «tercero». Un encargado del tratamiento, una persona bajo autoridad directa del responsable o el propio interesado pueden ser destinatarios de una comunicación de datos sin ser terceros. Y al revés: las autoridades públicas que reciben datos en el marco de una investigación concreta no se consideran destinatarios pese a recibir la comunicación.

4. Datos de las personas fallecidas — art. 3 LOPDGDD

El RGPD ampara únicamente a las personas físicas vivas: los fallecidos no son «interesados» a efectos del Reglamento. La LOPDGDD reconoce, no obstante, en su art. 3 —ubicado en el **Título I (Disposiciones generales)**, no en el Título III de derechos del interesado — un régimen específico de **acceso, rectificación o supresión** de los datos personales del causante por parte de determinados legitimados.

Artículo 3 LOPDGDD · Datos de las personas fallecidas

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo,

si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Apartado	Legitimados	Régimen específico
3.1	Personas vinculadas por razones familiares o de hecho · Herederos	Acceso, rectificación o supresión. **Excepción doble**: prohibición expresa del fallecido o ley en contrario. **Subexcepción**: la prohibición no afecta al derecho de los herederos a los datos de carácter patrimonial del causante
3.2	Personas o instituciones designadas expresamente por el fallecido	Acceso, rectificación o supresión, con arreglo a las instrucciones recibidas. Real decreto regulará la acreditación de validez/vigencia y el registro de mandatos
3.3	Menores fallecidos: representantes legales y Ministerio Fiscal · Personas con discapacidad fallecidas: designados para funciones de apoyo	El MF puede actuar de oficio o a instancia de cualquier persona interesada. Los designados para apoyo solo cuando las facultades estén comprendidas en las medidas de apoyo prestadas

MATIZ

La prohibición expresa del fallecido bloquea el acceso a sus datos, salvo que una ley disponga lo contrario. Pero esa prohibición **NO afecta** al derecho de los herederos a acceder a los **datos de carácter patrimonial** del causante (necesarios, por ejemplo, para la sucesión).

MATIZ

El art. 3 está en el Título I (Disposiciones generales), no en el Título III (derechos del interesado, arts. 11-18). El fallecido **no es «interesado»** a efectos del RGPD: el régimen del art. 3 LOPDGDD solo cubre acceso, rectificación y supresión —no portabilidad, oposición, limitación ni decisiones automatizadas —.

TEMA 4

Epígrafe 2 — Principios

Los principios que rigen el tratamiento de datos personales se enumeran en el **art. 5 RGPD** y se desarrollan en el **Título II de la LOPDGDD (arts. 4-10)**, con normas específicas sobre exactitud, confidencialidad, consentimiento, consentimiento de menores, bases distintas del consentimiento, categorías especiales y datos de naturaleza penal.

1. Los seis principios del art. 5 RGPD y la responsabilidad proactiva

Artículo 5 RGPD · Principios relativos al tratamiento

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Letra	Etiqueta literal del art. 5.1 RGPD	Idea-fuerza
a	Licitud, lealtad y transparencia	Los datos se tratan de manera lícita, leal y transparente en relación con el interesado
b	Limitación de la finalidad	Recogida con fines determinados, explícitos y legítimos; el tratamiento ulterior con fines de archivo en interés público, investigación científica o histórica o estadísticos **no se considera incompatible** con los fines iniciales (art. 89.1 RGPD)

c	Minimización de datos	Adecuados, pertinentes y limitados a lo necesario para los fines
d	Exactitud	Exactos y, si fuera necesario, actualizados; supresión o rectificación sin dilación de los inexactos
e	Limitación del plazo de conservación	No más tiempo del necesario para los fines; conservación más larga solo para fines de archivo, investigación o estadísticos con medidas técnicas y organizativas apropiadas
f	Integridad y confidencialidad	Seguridad adecuada frente a tratamiento no autorizado, pérdida, destrucción o daño accidental, mediante medidas técnicas u organizativas apropiadas
(5.2)	Responsabilidad proactiva	El responsable es responsable del cumplimiento de los seis principios **y capaz de demostrarlo**

RECUERDA

Esquema mental de los seis principios (orden BOE a-f): **3 limitaciones** de los datos —de la **finalidad** (b), de la **minimización** (c) y del **plazo de conservación** (e)—

1. 3 cualidades

de los datos —**licitud-lealtad-transparencia** (a), **exactitud** (d) e **integridad y confidencialidad** (f)—

1. responsabilidad proactiva

del responsable (art. 5.2).

MATIZ

Responsabilidad proactiva ≠ responsabilidad civil del art. 82 RGPD. La proactiva del art. 5.2 RGPD obliga al responsable a **acreditar** documentalmente el cumplimiento de los principios (registro de actividades, EIPD, políticas internas, formación). La civil del art. 82 RGPD obliga a **indemnizar** los daños y perjuicios causados por una infracción del Reglamento. El régimen sancionador administrativo de los arts. 83 RGPD y 70-78 LOPDGDD es una tercera dimensión distinta.

2. Las seis bases jurídicas del tratamiento — art. 6 RGPD

El art. 5.1.a RGPD impone que el tratamiento sea **lícito**. El art. 6 RGPD concreta esa licitud exigiendo que concurra **al menos una** de **seis bases jurídicas** o «condiciones de licitud», ninguna superior a las demás:

Artículo 6.1 RGPD · Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
>
> f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
>
> Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Letra	Base jurídica	Idea-fuerza
a	**Consentimiento** del interesado	Manifestación libre, específica, informada e inequívoca + declaración o clara acción afirmativa (art. 4.11 RGPD + art. 6 LOPDGDD)
b	**Contrato**	Ejecución del contrato del que el interesado es parte o medidas precontractuales a petición del interesado
c	**Obligación legal** del responsable	Solo si lo prevé norma de Derecho UE o norma con rango de ley (art. 8.1 LOPDGDD)
d	**Interés vital** del interesado u otra persona física	Excepcional; el interesado no esté capacitado física o jurídicamente para consentir
e	**Misión de interés público o poderes públicos**	Solo si deriva de competencia atribuida por norma con rango de ley (art. 8.2 LOPDGDD)
f	**Interés legítimo** del responsable o tercero	Ponderación con los derechos del interesado; **excluido** para autoridades públicas en el ejercicio de sus funciones

MATIZ

El interés legítimo del 6.1.f no está al alcance de las autoridades públicas en el ejercicio de sus funciones. El propio art. 6.1 RGPD lo excluye en su párrafo final. Las AAPP que actúan en su esfera pública han de ampararse en los apartados c) (obligación legal) o e) (misión de interés público / poderes públicos), no en el f).

MATIZ

Las seis bases del art. 6.1 RGPD son alternativas, no jerárquicas. Basta con que concurra una. El consentimiento del 6.1.a no es la regla general ni la base preferente —es una más entre seis—. En la práctica, el sector público se ampara casi siempre en c) o e).

3. Desarrollo nacional de bases distintas del consentimiento — art. 8 LOPDGDD

Artículo 8 LOPDGDD · Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al trata-

miento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

El art. 8 LOPDGDD desarrolla en el ordenamiento español las bases del **6.1.c y 6.1.e RGPD**, exigiendo en ambos casos que el fundamento esté en **norma con rango de ley** (Derecho de la Unión o ley nacional). No basta una norma reglamentaria.

RECUERDA

Reserva de ley para las bases públicas del tratamiento. Las bases del 6.1.c (obligación legal) y 6.1.e (misión de interés público / poderes públicos) requieren norma de Derecho UE o **norma con rango de ley** (no sirve un reglamento). El art. 8 LOPDGDD añade, además, que la norma de cobertura **puede** —no debe — determinar condiciones generales del tratamiento, tipos de datos, cesiones y medidas adicionales de seguridad.

4. El consentimiento del afectado — art. 6 LOPDGDD

El consentimiento es la primera base jurídica del art. 6.1 RGPD y es la única que el propio Reglamento define en su art. 4.11. La LOPDGDD reproduce esa definición en su art. 6 y añade dos reglas específicas sobre **pluralidad de finalidades** y **prohibición de la supeditación contractual**.

Artículo 6 LOPDGDD · Tratamiento basado en el consentimiento del afectado

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.
3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

RECUERDA

Mnemotécnico LEII + acción afirmativa del consentimiento (art. 4.11 RGPD y art. 6.1 LOPDGDD): **L**ibre · **E**specífica · **I**nformada · **I**nequívoca + declaración o clara acción afirmativa. Las cuatro cualidades de la voluntad y el modo de manifestarla.

MATIZ

No existe el consentimiento tácito ni el consentimiento por omisión. El RGPD y la LOPDGDD exigen siempre **declaración** o **clara acción afirmativa**. Las casillas marcadas por defecto, el silencio o la inacción del interesado no son consentimiento válido (vid. STJUE de 1-10-2019, asunto C-673/17, *Planet49*).

MATIZ

Pluralidad de finalidades = consentimiento específico para cada una. No vale un consentimiento global y genérico para «cualesquiera finalidades»: el art. 6.2 LOPDGDD exige que conste de manera específica e inequívoca que se otorga para **todas** las finalidades (granularidad).

MATIZ

No supeditación contractual (art. 6.3 LOPDGDD). No se puede condicionar la ejecución del contrato a que el afectado consienta el tratamiento de datos para finalidades **no relacionadas** con el mantenimiento, desarrollo o control de la relación contractual (la triple coletilla del BOE — más amplia que «la prestación del servicio»).

5. El consentimiento de los menores de edad — art. 7 LOPDGDD + art. 8 RGPD

Artículo 7 LOPDGDD · Consentimiento de los menores de edad

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad

> o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8.1 RGPD · Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

> 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
>
> Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

Edad	Régimen aplicable en España
≥ 14 años	Pueden prestar consentimiento por sí mismos. **Excepción**: cuando la ley exija asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento
< 14 años	El tratamiento solo es lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen

MATIZ

Tres edades en juego para el consentimiento del menor: **16 años** = techo del RGPD por defecto (art. 8.1 RGPD, ámbito limitado a servicios de la sociedad de la información); **13 años** = suelo absoluto que los Estados miembros no pueden rebajar (mismo art. 8.1 RGPD, párrafo segundo); **14 años** = la edad fijada por España en el art. 7 LOPDGDD para cualquier tratamiento basado en consentimiento.

MATIZ

El art. 8 RGPD se aplica únicamente a servicios de la sociedad de la información ofrecidos directamente a niños. El art. 7 LOPDGDD generaliza el régimen a **cualquier** tratamiento de datos del menor basado en consentimiento (no solo SSI). Por tanto, en España la edad de 14 años opera tanto para apps, redes sociales y plataformas digitales como para cualquier otro tratamiento que se ampare en el consentimiento del 6.1.a RGPD.

6. La exactitud — art. 4 LOPDGDD

El art. 4 LOPDGDD desarrolla el principio de **exactitud** del art. 5.1.d RGPD aclarando cuándo la inexactitud **no es imputable** al responsable: cuando los datos inexactos se obtuvieron de cuatro fuentes específicas y el responsable adoptó todas las medidas razonables para suprimirlos o rectificarlos sin dilación.

Artículo 4 LOPDGDD · Exactitud de los datos

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.
2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que

este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

RECUERDA

Cuatro fuentes que excluyen la imputación al responsable (art. 4.2 LOPDGDD), siempre que el responsable haya adoptado todas las medidas razonables para suprimir o rectificar sin dilación: **a)** del propio afectado · **b)** de un mediador o intermediario sectorial · **c)** de otro responsable por ejercicio de la portabilidad · **d)** de un registro público. La carga de responsabilidad por la inexactitud se desplaza, en su caso, al mediador o intermediario que entregó los datos.

7. El deber de confidencialidad — art. 5 LOPDGDD

Artículo 5 LOPDGDD · Deber de confidencialidad

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.
2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

El art. 5 LOPDGDD desarrolla el principio de **integridad y confidencialidad** del art. 5.1.f RGPD añadiendo dos reglas específicas: (i) el deber es **complementario** —no sustitutivo— de los deberes de secreto profesional aplicables (médico, abogado, sacerdote, periodista, funcionarial…), y (ii) **se mantiene tras la extinción** de la relación del obligado con el responsable o encargado.

MATIZ

El deber de confidencialidad NO cesa al terminar la relación laboral o contractual. Es una obligación permanente que pervive más allá de la extinción del vínculo del obligado con el responsable o encargado. La exempleada que conoció datos personales durante su trabajo sigue obligada a la confidencialidad indefinidamente.

MATIZ

Confidencialidad del art. 5 LOPDGDD ≠ secreto profesional. El deber del art. 5 es una obligación general de protección de datos. Los deberes de secreto profesional (médico, abogado, periodista, sacerdote…) tienen su régimen propio en su normativa sectorial y conviven con el del art. 5 LOPDGDD: cuando proceda, se aplican **acumulativamente** (apartado 2: «será complementaria»).

8. Categorías especiales de datos — art. 9 RGPD + art. 9 LOPDGDD

El art. 9 RGPD parte de una **prohibición general** del tratamiento de las categorías especiales y enumera **diez excepciones** a esa prohibición (apartado 2, letras a-j). El art. 9 LOPDGDD añade un matiz nacional a la excepción del consentimiento (9.2.a) y exige norma con rango de ley para tres de las excepciones (9.2.g, h, i).

Artículo 9.1 RGPD · Prohibición de tratamiento de categorías especiales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

nº	Categoría especial del art. 9.1 RGPD
1	Origen étnico o racial
2	Opiniones políticas
3	Convicciones religiosas o filosóficas
4	Afiliación sindical
5	Datos genéticos

6	Datos biométricos dirigidos a identificar de manera unívoca a una persona física
7	Datos relativos a la salud
8	Datos relativos a la vida sexual o la orientación sexual

Excepciones a la prohibición · a-j (art. 9.2 RGPD)

Letra	Excepción
a	Consentimiento explícito del interesado para fines especificados (salvo que el Derecho UE/EM lo prohíba)
b	Cumplimiento de obligaciones y ejercicio de derechos en el ámbito laboral y de seguridad social, autorizado por norma o convenio colectivo
c	Intereses vitales del interesado o de otra persona física, cuando el interesado no esté capacitado para consentir
d	Tratamiento por fundación, asociación u organismo sin ánimo de lucro de finalidad política, filosófica, religiosa o sindical, sobre miembros o personas en contacto regular
e	Datos manifiestamente públicos por el propio interesado
f	Formulación, ejercicio o defensa de reclamaciones; o tribunales en ejercicio de su función judicial
g	Interés público esencial sobre la base del Derecho UE/EM proporcional al objetivo
h	Medicina preventiva o laboral, evaluación de capacidad laboral, diagnóstico médico, asistencia sanitaria o social, gestión de sistemas de salud
i	Interés público en el ámbito de la salud pública (amenazas transfronterizas, calidad de la asistencia sanitaria)
j	Fines de archivo en interés público, investigación científica o histórica o estadísticos (art. 89.1 RGPD)

Artículo 9 LOPDGDD · Categorías especiales de datos

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

MATIZ

El solo consentimiento NO basta para tratar datos cuya finalidad principal sea identificar **ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico** (art. 9.1 LOPDGDD). Pero esos datos sí pueden tratarse al amparo de **cualquier otra excepción** del art. 9.2 RGPD (b a j) cuando concurra (segundo párrafo del 9.1 LOPDGDD). La regla no es una prohibición absoluta, sino una restricción del peso del consentimiento como base única.

MATIZ

Tres excepciones del 9.2 RGPD requieren norma con rango de ley en España: la **g)** (interés público esencial), la **h)** (medicina, asistencia sanitaria y social) y la **i)** (salud pública). El art. 9.2 LOPDGDD así lo dispone — no basta una norma reglamentaria.

MATIZ

Las categorías del art. 9.1 RGPD son ocho, no siete. El literal del DOUE en español contiene una incongruencia gramatical («las orientación sexuales» en lugar de «la orientación sexual»); la cita se mantiene tal como aparece en el texto oficial. La enumeración material es: origen étnico o racial · opiniones políticas · convicciones religiosas o filosóficas · afiliación sindical · datos genéticos · datos biométricos para identificar unívocamente · datos de salud · datos relativos a la vida sexual o la orientación sexual.

9. Datos de naturaleza penal — art. 10 RGPD + art. 10 LOPDGDD

Artículo 10 RGPD · Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 10 LOPDGDD · Tratamiento de datos de naturaleza penal

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.
2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.
3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Apartado	Supuesto	Régimen
10.1	Tratamiento de datos penales para **fines distintos** a los penales (no prevención / investigación / enjuiciamiento / ejecución)	Solo si lo ampara norma de Derecho UE, la propia LOPDGDD u otra norma de rango legal
10.2	**Registro completo** de los datos del art. 10 RGPD	Conforme a la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia

10.3	Fuera de los apartados 1 y 2	Solo abogados y procuradores, para recoger información facilitada por sus clientes en el ejercicio de sus funciones

MATIZ

Reserva legal para el tratamiento de datos penales fuera de fines penales (art. 10.1 LOPDGDD): cualquier tratamiento de datos sobre condenas, infracciones, procedimientos y medidas cautelares con un propósito **no penal** (estadístico, periodístico, de transparencia…) requiere norma con rango de ley. La excepción residual del 10.3 deja la puerta abierta solo a abogados y procuradores en el ejercicio de su función procesal.

MATIZ

Registro completo de condenas → control público (art. 10 RGPD in fine + art. 10.2 LOPDGDD): no caben registros completos de antecedentes penales en manos privadas. El sistema español encomienda esa función al Registro Central de Penados (Ministerio de Justicia), dentro del Sistema de registros administrativos de apoyo a la Administración de Justicia.

TEMA 4

Epígrafe 3 — Derechos

Los derechos del interesado están regulados en el **Capítulo III del RGPD (arts. 12-22)** y desarrollados en el **Título III de la LOPDGDD (arts. 11-18)**, con dos planos diferenciados: la **transparencia y modalidades de ejercicio** (arts. 11-12 LOPDGDD + art. 12 RGPD + arts. 13-14 RGPD), y los **seis derechos sustantivos** del catálogo —acceso, rectificación, supresión, limitación, portabilidad y oposición— a los que se añade un séptimo derecho separado: el **derecho a no ser objeto de decisiones individuales automatizadas** del art. 22 RGPD.

1. Información por capas — art. 11 LOPDGDD + arts. 13 y 14 RGPD

El RGPD obliga al responsable a facilitar al interesado, en el momento en que se obtengan sus datos, una **información extensa y detallada** sobre el tratamiento (identidad del responsable, fines, base jurídica, plazos de conservación, derechos del interesado, decisiones automatizadas, transferencias a terceros países…). Por la complejidad de esa información, la LOPDGDD habilita un sistema de **información por capas**: el responsable puede facilitar primero una **información básica** y enlazar con un medio sencillo y accesible al resto.

Artículo 11 LOPDGDD · Transparencia e información al afectado

> 1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de las que procedieran los datos.

Origen de los datos	Norma RGPD	Información básica del art. 11 LOPDGDD

Del propio afectado	Art. 13 RGPD (deber de información en el momento de la obtención)	a) identidad del responsable y representante · b) finalidad · c) derechos de los arts. 15-22 RGPD · (+ elaboración de perfiles y derecho a oponerse a decisiones automatizadas, en su caso)
No del afectado (terceros, registros, redes…)	Art. 14 RGPD (información en plazo razonable, máximo 1 mes)	La información básica anterior **+** a) categorías de datos · b) fuentes de las que proceden

RECUERDA

Información «por capas»: la primera capa (información básica del art. 11 LOPDGDD) cumple el deber de información si se enlaza con un medio sencillo y accesible al resto (segunda capa). La información completa de los arts. 13/14 RGPD es siempre exigible; la LOPDGDD solo permite **fraccionarla** en dos capas para no saturar al afectado en el momento de la recogida.

MATIZ

Tres letras a/b/c en la información básica cuando los datos vienen del afectado (art. 11.2 LOPDGDD); **cinco letras** cuando los datos no vienen del afectado (las tres anteriores **+** categorías + fuentes — art. 11.3 LOPDGDD). Si la finalidad incluye elaboración de perfiles, **se añade siempre** la mención del derecho a oponerse a decisiones automatizadas.

MATIZ

Plazo del art. 14.3 RGPD para informar cuando los datos no son del afectado: **plazo razonable**, a más tardar **un mes**, salvo que se vayan a utilizar antes para comunicarse con el interesado (en cuyo caso, en la primera comunicación) o se vayan a comunicar a otro destinatario (en la primera comunicación). El art. 14.5 RGPD enumera **cuatro excepciones** al deber de información (interesado ya dispone · imposible o esfuerzo desproporcionado · obtención prevista por norma con garantías · obligación de secreto profesional regulada por ley).

2. Disposiciones generales sobre ejercicio de los derechos — art. 12 LOPDGDD + art. 12 RGPD

Artículo 12 LOPDGDD · Disposiciones generales sobre ejercicio de los derechos

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.
2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.
3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.
5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.
6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.
7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 12 RGPD · Transparencia y modalidades de ejercicio (apartados 3, 5 y 6)

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará

por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

Aspecto	Regla literal
Plazo general de respuesta	**1 mes** desde la recepción de la solicitud (art. 12.3 RGPD)
Prórroga máxima	**2 meses adicionales** en función de complejidad o número de solicitudes; informar al interesado en el primer mes con motivos. **Total máximo: 3 meses**
Forma de respuesta	Por escrito o medios electrónicos; verbalmente solo a petición del interesado y previa identificación

Gratuidad	Regla general; **excepción**: solicitudes manifiestamente infundadas o excesivas (especialmente repetitivas) → canon razonable o negativa a actuar (carga de la prueba al responsable)
Identificación	Si el responsable tiene dudas razonables, puede pedir información adicional para confirmar la identidad
Representación	Directa o por representante legal o voluntario (art. 12.1 LOPDGDD); titulares de patria potestad por menores de 14 años (art. 12.6 LOPDGDD)
Carga de la prueba del cumplimiento	Sobre el responsable (art. 12.4 LOPDGDD)
Encargado	Puede tramitar por cuenta del responsable si así se pactó en el contrato o acto jurídico (art. 12.3 LOPDGDD)

RECUERDA

Plazos de respuesta del art. 12.3 RGPD: 1 + 2 = 3 meses como máximo. Un mes desde la recepción de la solicitud, prorrogable otros dos meses por complejidad o número, **comunicando la prórroga al interesado dentro del primer mes** y motivándola.

MATIZ

Gratuidad como regla, no como derecho absoluto. Solo cabe cobrar canon o negarse cuando la solicitud sea **manifiestamente infundada o excesiva**, especialmente por su **carácter repetitivo** (art. 12.5 RGPD). La carga de demostrar ese carácter recae sobre el responsable, no sobre el interesado.

MATIZ

El art. 12.6 LOPDGDD usa el término «cancelación» —terminología de la antigua LOPD 1999— al enumerar los derechos que los titulares de la patria potestad pueden ejercer en nombre de menores de 14 años. Bajo el régimen vigente del RGPD ese término equivale al **derecho de supresión** (art. 17 RGPD).

3. Acceso — art. 15 RGPD + art. 13 LOPDGDD

Artículo 15 RGPD · Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.
3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Artículo 13 LOPDGDD · Derecho de acceso

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.
4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

RECUERDA

Sistema de acceso remoto, directo y seguro (art. 13.2 LOPDGDD): la mera comunicación al afectado del modo de acceso al sistema **basta** para tener atendida la solicitud. Es la fórmula legal de despachar el derecho de acceso mediante un portal de área privada del interesado, sin tramitar solicitudes individuales.

MATIZ

Seis meses = plazo a partir del cual puede considerarse repetitivo el ejercicio del derecho de acceso (art. 13.3 LOPDGDD), a menos que exista **causa legítima**. La cláusula de salvaguardia es importante: la mera reiteración no convierte automáticamente la solicitud en abusiva si hay causa legítima.

MATIZ

El acceso del art. 15 RGPD incluye más que «los datos»: incluye también la información (a-h) sobre fines, categorías, destinatarios, plazos, derechos, origen y decisiones automatizadas, **más** una **copia** de los datos objeto de tratamiento (art. 15.3). La primera copia es gratuita; copias adicionales pueden devengar canon razonable basado en costes administrativos.

4. Rectificación — art. 16 RGPD + art. 14 LOPDGDD

Artículo 16 RGPD · Derecho de rectificación

> El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 14 LOPDGDD · Derecho de rectificación

> Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar,

cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

RECUERDA

Doble alcance del art. 16 RGPD: rectificación de datos **inexactos** + integración de datos **incompletos** mediante declaración adicional, teniendo en cuenta los fines del tratamiento. El art. 14 LOPDGDD precisa la carga formal del afectado: indicar los datos a corregir y aportar documentación justificativa cuando proceda.

5. Supresión — art. 17 RGPD + art. 15 LOPDGDD

El art. 17 RGPD se denomina formalmente **«derecho de supresión (el derecho al olvido)»**. Tiene una doble proyección: la supresión clásica (apartado 1) y la **obligación adicional del responsable** que haya hecho públicos los datos de comunicar la solicitud de supresión a otros responsables que estén tratando enlaces, copias o réplicas (apartado 2 — la verdadera proyección «de olvido digital»).

Artículo 17 RGPD · Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 15 LOPDGDD · Derecho de supresión

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.
2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Apartado art. 17 RGPD	Contenido
17.1	**Seis supuestos a-f** que dan derecho a la supresión: a) datos ya no necesarios · b) retirada del consentimiento sin otra base · c) oposición ex art. 21.1 sin motivos legítimos prevalentes o ex 21.2 (marketing) · d) tratamiento ilícito · e) obligación legal de supresión · f) datos obtenidos en SSI ofrecidos a niños (art. 8.1 RGPD)
17.2	**Proyección «al olvido»**: si el responsable hizo públicos los datos, debe adoptar medidas razonables para informar a otros responsables que traten enlaces, copias o réplicas de la solicitud de supresión
17.3	**Cinco excepciones a-e** al derecho de supresión: a) libertad de expresión e información · b) obliga-

	ción legal o misión de interés público · c) interés público en salud pública · d) fines de archivo, investigación o estadísticos · e) formulación, ejercicio o defensa de reclamaciones

RECUERDA

Conservación de datos identificativos para impedir marketing futuro (art. 15.2 LOPDGDD): cuando la supresión derive de la oposición a marketing directo (art. 21.2 RGPD), el responsable puede **conservar** los datos identificativos mínimos para garantizar que no se vuelvan a usar con esos fines (lista de exclusión).

MATIZ

«Derecho al olvido» ≠ supresión a secas. El art. 17 RGPD utiliza el paréntesis «(el derecho al olvido)» en el título, pero la verdadera proyección «de olvido» en sentido digital es el **apartado 17.2**: la obligación del responsable que ha hecho públicos los datos de informar a otros responsables que traten enlaces, copias o réplicas. La doctrina identifica el derecho al olvido en sentido propio con esa propagación de la supresión, no con la supresión clásica del 17.1.

6. Limitación del tratamiento — art. 18 RGPD + art. 16 LOPDGDD

Artículo 18 RGPD · Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.
3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 16 LOPDGDD · Derecho a la limitación del tratamiento

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.
2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Apartado art. 18 RGPD	Supuesto / régimen
18.1.a	El interesado **impugna la exactitud** → limitación durante el plazo de verificación
18.1.b	Tratamiento **ilícito** y el interesado **se opone a la supresión** y prefiere la limitación
18.1.c	El responsable **ya no necesita los datos** pero el interesado los necesita para reclamaciones
18.1.d	Oposición ex 21.1 mientras se verifica si prevalecen los motivos legítimos del responsable
18.2	**Régimen de los datos limitados**: solo conservación; tratamiento adicional solo con consentimiento, para reclamaciones, para proteger derechos de otra persona o por interés público importante
18.3	**Comunicación previa al levantamiento**: el responsable debe informar al interesado antes de levantar la limitación

RECUERDA

La limitación debe constar claramente en los sistemas de información del responsable (art. 16.2 LOPDGDD). No basta con desactivar el procesamiento: hace falta una marca técnica visible que impida usos ulteriores no permitidos.

MATIZ

La limitación NO es una supresión. Los datos siguen existiendo y pueden volver a tratarse cuando se levante la limitación. Por eso el art. 18.3 RGPD impone al responsable comunicar el levantamiento al interesado antes de aplicarlo: el interesado tiene derecho a saber cuándo deja de protegerle la limitación.

Artículo 19 RGPD · Notificación de rectificación, supresión o limitación

> El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

MATIZ

Obligación adicional del art. 19 RGPD: cuando se rectifiquen, supriman o limiten datos previamente comunicados a otros destinatarios, el responsable **debe** notificarles la actuación, salvo imposibilidad o esfuerzo desproporcionado. Y debe informar al interesado de quiénes son esos destinatarios si este lo pide. No es una notificación al interesado, sino a la red de destinatarios anteriores.

7. Portabilidad — art. 20 RGPD + art. 17 LOPDGDD

Artículo 20 RGPD · Derecho a la portabilidad de los datos

> 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Artículo 17 LOPDGDD · Derecho a la portabilidad

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

MATIZ

Doble requisito acumulativo del art. 20.1 RGPD: el tratamiento debe estar basado en **consentimiento o contrato** (no vale interés legítimo, ni obligación legal, ni interés público ni interés vital) **Y** efectuarse por **medios automatizados**. La portabilidad no aplica a tratamientos en papel.

MATIZ

La portabilidad NO se aplica al sector público que actúe en interés público o en ejercicio de poderes públicos (art. 20.3 RGPD). Las AAPP que tratan datos amparándose en el 6.1.e RGPD están exentas de portar los datos a otro responsable. Por eso es un derecho prácticamente irrelevante en el contexto de la Administración pública.

MATIZ

Portabilidad ≠ acceso. El acceso del art. 15 RGPD obliga a entregar copia de los datos al interesado en formato electrónico de uso común. La portabilidad del art. 20 RGPD obliga, además, a usar **formato estructurado, de uso común y lectura mecánica**, y a permitir la **transmisión directa de responsable a responsable** cuando sea técnicamente posible.

8. Oposición y decisiones individuales automatizadas — arts. 21 y 22 RGPD + art. 18 LOPDGDD

Artículo 21 RGPD · Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los

derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22 RGPD · Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Artículo 18 LOPDGDD · Derecho de oposición

> El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

Modalidad de oposición (art. 21 RGPD)	Régimen
21.1 – Oposición general	Por motivos relacionados con la **situación particular** del interesado, frente a tratamientos basados en el 6.1.e (interés público / poderes públicos) o 6.1.f (interés legítimo). El responsable cesa, salvo que acredite motivos legítimos **imperiosos** prevalentes o necesidad para reclamaciones
21.2 – Oposición a marketing directo	**Sin necesidad de motivos**, en cualquier momento. El responsable cesa **inmediatamente** el tratamiento para esos fines (21.3)
21.4 – Información explícita	El derecho debe mencionarse explícitamente al interesado, claramente y al margen, **a más tardar en la primera comunicación**
21.5 – SSI	En servicios de la sociedad de la información cabe oposición por medios automatizados con especificaciones técnicas
21.6 – Investigación / estadística	Oposición por situación particular, salvo que el tratamiento sea necesario para una misión de interés público

Aspecto del art. 22 RGPD	Regla
Regla general (22.1)	Derecho a NO ser objeto de **decisión basada únicamente** en tratamiento automatizado (incluido perfilado) que produzca **efectos jurídicos** o afecte **significativamente** de modo similar
Excepciones (22.2 a-c)	a) decisión necesaria para celebración/ejecución de contrato · b) autorizada por norma UE/EM con garantías · c) consentimiento explícito
Garantías mínimas (22.3)	En los supuestos a) y c): derecho a **intervención humana** + a **expresar el punto de vista** + a **impugnar** la decisión

Restricción (22.4)	Las decisiones del 22.2 no pueden basarse en categorías especiales del art. 9.1 RGPD, **salvo** que se aplique el 9.2.a (consentimiento explícito) o 9.2.g (interés público esencial) **y** se hayan tomado medidas adecuadas

9. El catálogo ARSLIPO + el séptimo derecho

Derecho	Art. RGPD	Art. LOPDGDD	Especialidad LOPDGDD
Acceso	15	13	Sistema de acceso remoto, directo y seguro = derecho atendido. Repetitivo a partir de >1 vez en 6 meses (salvo causa legítima). Coste desproporcionado del medio elegido por el afectado → exceso a su cargo
Rectificación	16	14	El afectado debe indicar los datos y la corrección, y aportar documentación justificativa cuando proceda
Supresión («olvido»)	17	15	Si la supresión deriva de oposición a marketing (21.2), el responsable puede conservar datos identificativos mínimos para impedir tratamientos futuros con esos fines
Limitación	18	16	Debe constar claramente en los sistemas de información del responsable
portab**I**lidad	20	17	Remisión al art. 20 RGPD; **excluida** para misiones de interés

			público y poderes públicos
Oposición	21	18	Remisión al art. 21 RGPD; el art. 18 LOPDGDD agrupa en una sola remisión la oposición y las decisiones automatizadas del art. 22 RGPD

RECUERDA

Mnemotécnico ARSLIPO (orden RGPD): **A**cceso (15) · **R**ectificación (16) · **S**upresión (17) · **L**imitación (18) · portab**I**lidad (20) · **O**posición (21). Son **6 derechos sustantivos** del Capítulo III RGPD, todos ellos remitidos por el Título III LOPDGDD.

MATIZ

El art. 22 RGPD añade un séptimo derecho que NO entra en el ARSLIPO: el derecho a no ser objeto de decisiones individuales automatizadas con efectos jurídicos o significativos. El art. 18 LOPDGDD lo agrupa con la oposición en una sola remisión, pero técnicamente es un derecho distinto al de oposición y con régimen propio (excepciones 22.2 + garantías mínimas del 22.3 + restricción del 22.4 sobre categorías especiales).

MATIZ

El art. 19 RGPD (notificación a destinatarios) no es un derecho del interesado, sino una **obligación correlativa del responsable**. Cuando se rectifica, suprime o limita un dato comunicado a terceros, el responsable debe notificárselo a esos destinatarios (salvo imposibilidad o esfuerzo desproporcionado) y, si el interesado lo pide, decirle quiénes son esos destinatarios.

TEMA 4

Epígrafe 4 — Responsable y encargado del tratamiento

El responsable y el encargado del tratamiento están regulados en el **Capítulo IV del RGPD (arts. 24-43)** y desarrollados en el **Título V de la LOPDGDD (arts. 28-37)**, este último dividido en tres capítulos: Capítulo I — Obligaciones generales (arts. 28-32), Capítulo II — Encargado del tratamiento (art. 33) y Capítulo III — Delegado de protección de datos (arts. 34-37, materia del Ep. 5). El tratamiento de datos crediticios y de morosos del **art. 20 LOPDGDD** —que el programa BOE no encuadra explícitamente, pero que materialmente es un régimen de obligaciones del responsable—, se integra en este epígrafe en la sub-sección final.

1. La responsabilidad activa (accountability) — art. 24 RGPD + art. 28 LOPDGDD

El RGPD sustituye el modelo previo de cumplimiento formal por un modelo de **responsabilidad activa** (*accountability*): el responsable y el encargado deben **valorar el riesgo** del tratamiento y adoptar **medidas técnicas y organizativas apropiadas**, sin esperar a la intervención de la autoridad de control. La responsabilidad proactiva del art. 5.2 RGPD (acreditar el cumplimiento de los principios) se complementa aquí con la responsabilidad activa de los arts. 24 RGPD y 28 LOPDGDD (adoptar medidas conforme al riesgo).

Artículo 24 RGPD · Responsabilidad del responsable del tratamiento

> 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará 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.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.
3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 28 LOPDGDD · Obligaciones generales del responsable y encargado del tratamiento

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.
2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

> h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Letra	Supuesto del art. 28.2 LOPDGDD que exige especial atención al riesgo
a	Tratamientos que generen riesgo de discriminación, usurpación, fraude, pérdidas financieras, daño reputacional, pérdida de confidencialidad de datos sujetos a secreto profesional, reversión no autorizada de la seudonimización, otro perjuicio económico, moral o social significativo
b	Tratamientos que priven a los afectados de sus derechos y libertades o impidan el control sobre sus datos
c	Tratamiento no meramente incidental de **categorías especiales** (arts. 9 y 10 RGPD/LOPDGDD) o de datos sobre infracciones administrativas
d	Elaboración de **perfiles** (rendimiento, salud, preferencias, fiabilidad, comportamiento, solvencia, localización, movimientos)
e	Datos de **grupos vulnerables**: menores y personas con discapacidad
f	Tratamiento **masivo** (gran número de afectados o gran cantidad de datos)
g	**Transferencias habituales** a terceros Estados u organizaciones internacionales sin nivel de protección adecuado
h	Cualesquiera otros relevantes a juicio del responsable o del encargado, en particular los previstos en códigos de conducta y esquemas de certificación

RECUERDA

Ocho supuestos a-h del art. 28.2 LOPDGDD que exigen especial atención al riesgo. La letra **g)** sobre transferencias internacionales habituales sin nivel de protección adecuado es la que más suele olvidarse en los listados sintéticos.

MATIZ

Responsabilidad activa ≠ responsabilidad proactiva ≠ responsabilidad civil ≠ responsabilidad sancionadora. La activa (art. 24 RGPD + 28 LOPDGDD) obliga a **adoptar medidas conforme al riesgo** la proactiva (art. 5.2 RGPD) obliga a **acreditar** el cumplimiento de los principios; la civil (art. 82 RGPD) obliga a **indemnizar** la sancionadora (arts. 83 RGPD + 70-78 LOPDGDD) impone **sanciones administrativas**. Son cuatro dimensiones complementarias del régimen de responsabilidad.

2. Protección desde el diseño y por defecto — art. 25 RGPD

Artículo 25 RGPD · Protección de datos desde el diseño y por defecto (apartados 1 y 2)

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de

cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. 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. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

RECUERDA

Privacy by design + privacy by default. El art. 25 RGPD impone dos obligaciones distintas: (i) **desde el diseño** (apartado 1) — integrar las garantías y la minimización en el momento de **determinar los medios** y en el del tratamiento, no a posteriori; (ii) **por defecto** (apartado 2) — la configuración predeterminada solo trata los datos necesarios para cada fin, con accesibilidad limitada. La fórmula técnica pivota sobre **seudonimización + minimización + accesibilidad restringida**.

3. Corresponsables del tratamiento — art. 26 RGPD + art. 29 LOPDGDD

Artículo 26 RGPD · Corresponsables del tratamiento

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.
2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.
3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 29 LOPDGDD · Supuestos de corresponsabilidad en el tratamiento

> La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

MATIZ

Frente a cada uno y contra cada uno (art. 26.3 RGPD): el interesado puede ejercer **todos** sus derechos frente a **cualquiera** de los corresponsables, **independientemente** del reparto interno de responsabilidades. El acuerdo entre corresponsables vincula a estos entre sí, no al interesado.

4. Representantes de responsables/encargados no establecidos en la UE — art. 27 RGPD + art. 30 LOPDGDD

Artículo 27 RGPD · Representantes de responsables o encargados del tratamiento no establecidos en la Unión (apartados 1 y 2)

> 1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.
> 2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:
>
> a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y

libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

Artículo 30 LOPDGDD · Representantes de responsables o encargados no establecidos en la UE

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

MATIZ

Doble régimen de solidaridad del representante en España (art. 30 LOPDGDD): (i) la AEPD/auton. puede imponer al representante **solidariamente con el responsable/encargado** las medidas del RGPD; (ii) en la responsabilidad civil del art. 82 RGPD, responsable, encargado y representante responden **solidariamente** por los daños. El representante conserva acción de repetición frente a quien proceda.

5. El encargado del tratamiento — art. 28 RGPD + art. 33 LOPDGDD

Artículo 28 RGPD · Encargado del tratamiento (apartados 1, 2, 3 y 10)

1. 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 apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.
2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del

responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, inclusive inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado del tratamiento informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 33 LOPDGDD · Encargado del tratamiento

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.
2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos

de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.
5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

MATIZ

El acceso del encargado a los datos NO es comunicación de datos (art. 33.1 LOPDGDD), siempre que se cumplan el RGPD, la LOPDGDD y sus normas de desarrollo. Esto evita que el encargo de tratamiento active el régimen de cesión de datos a terceros y simplifica las relaciones entre responsable y encargado.

MATIZ

Dos formas de convertirse de encargado en responsable (art. 33.2 LOPDGDD): (i) actuar **en nombre propio sin que conste que se hace por cuenta del responsable** ante los afectados —salvo en encargos del sector público con cobertura legal—; (ii) **utilizar los datos para finalidades propias** del encargado, no del responsable. La conversión es automática: el RGPD se le aplica como si siempre hubiera sido responsable. La regla del 28.10 RGPD complementa: si el encargado infringe el RGPD al determinar fines y medios, se le considera responsable.

MATIZ

Subencargado solo con autorización previa por escrito (art. 28.2 RGPD), específica o general. En el caso de autorización general, el encargado debe informar al responsable de cualquier cambio en la incorporación o sustitución de subencargados, **dando al responsable la oportunidad de oponerse**. Si el subencargado incumple, el encargado inicial **sigue siendo plenamente responsable** ante el responsable (art. 28.4 RGPD).

RECUERDA

Ocho cláusulas mínimas a-h del contrato del 28.3 RGPD: a) instrucciones documentadas · b) confidencialidad de las personas autorizadas · c) medidas de seguridad del 32 · d) condiciones para recurrir a otro encargado · e) asistencia al responsable para responder a derechos de los interesados (Cap. III) · f) ayuda al responsable para arts. 32-36 (seguridad, violaciones, EIPD, consulta previa) · g) suprimir o devolver datos al final · h) facilitar información para demostrar cumplimiento + auditorías.

6. Registro de las actividades de tratamiento — art. 30 RGPD + art. 31 LOPDGDD

Artículo 30 RGPD · Registro de las actividades de tratamiento (apartados clave)

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una 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;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31 LOPDGDD · Registro de las actividades de tratamiento

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

RECUERDA

Registro de actividades del art. 30 RGPD: obligación general para responsables y encargados (con sus representantes en su caso). El RGPD enumera **siete contenidos a-g** del registro del responsable (a-g del 30.1) y **cuatro a-d** del registro del encargado (30.2). Debe constar por escrito (papel o electrónico) y ponerse a disposición de la autoridad de control.

MATIZ

Excepción de las menos de 250 personas (art. 30.5 RGPD), pero con triple cláusula que casi la anula: la excepción cae si el tratamiento (a) **puede entrañar riesgo** para los derechos del interesado · (b) **no sea ocasional** · (c) incluya **categorías especiales** del 9.1 o **datos penales** del 10. En la práctica, casi cualquier tratamiento empresarial ordinario activa alguna de las tres cláusulas y obliga a llevar el registro.

MATIZ

Inventario público de actividades para el sector público (art. 31.2 LOPDGDD). Los sujetos del art. 77.1 LOPDGDD (AAPP, órganos constitucionales, tribunales en su actividad no judicial, universidades públicas, Banco de España…) **deben publicar** un inventario electrónico de sus actividades con la información del 30 RGPD **y su base legal**. Es obligación adicional al registro privado y específica del sector público.

7. Seguridad del tratamiento y violaciones de seguridad — arts. 32, 33 y 34 RGPD

Artículo 32 RGPD · Seguridad del tratamiento (apartado 1)

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Artículo 33 RGPD · Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34 RGPD · Comunicación de una violación de la seguridad al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).
3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Aspecto	Regla
Plazo de notificación a la autoridad de control (art. 33.1 RGPD)	Sin dilación indebida + a más tardar **72 horas** desde que el responsable tuvo constancia. Excepción: si es improbable que constituya un riesgo. Notificación tardía → indicar motivos del retraso
Notificación encargado → responsable (art. 33.2 RGPD)	Sin dilación indebida
Comunicación al interesado (art. 34.1 RGPD)	Solo cuando sea probable que la violación entrañe **alto riesgo** para derechos y libertades. Sin dilación indebida. Lenguaje claro y sencillo
Excepciones a la comunicación al interesado (art. 34.3 RGPD)	a) datos cifrados/ininteligibles · b) medidas ulteriores que eliminen el alto riesgo · c) esfuerzo desproporcionado → comunicación pública equivalente
Documentación interna (art. 33.5 RGPD)	El responsable documentará cualquier violación, sus efectos y medidas correctivas. La autoridad de control puede verificar

RECUERDA

Plazo «72 horas» del art. 33 RGPD: es el plazo máximo para notificar a la autoridad de control desde que el responsable **tiene constancia** de la violación de seguridad, salvo improbabilidad de riesgo. Si se incumple, la notificación tardía debe motivarse.

MATIZ

Dos comunicaciones distintas tras una violación de seguridad: (i) **notificación a la autoridad de control** (art. 33 RGPD) → siempre, salvo improbabilidad de riesgo, en 72 horas; (ii) **comunicación al interesado** (art. 34 RGPD) → solo si **alto riesgo**, sin plazo numérico, con tres excepciones (cifrado, medidas ulteriores que eliminen el riesgo, esfuerzo desproporcionado → comunicación pública).

8. Evaluación de impacto (EIPD) y consulta previa — arts. 35 y 36 RGPD

Artículo 35 RGPD · Evaluación de impacto relativa a la protección de datos (apartados 1, 2, 3 y 7)

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

7. La evaluación deberá incluir como mínimo:

a) 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;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento,

teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Artículo 36 RGPD · Consulta previa (apartados 1 y 2)

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.
2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

RECUERDA

Tres supuestos en los que es obligatoria la EIPD (art. 35.3 RGPD): a) **perfilado** sistemático con decisiones de efectos jurídicos o significativos · b) tratamiento **a gran escala de categorías especiales** (art. 9.1) o de **datos penales** (art. 10) · c) **observación sistemática a gran escala de zona de acceso pública** (videovigilancia masiva). El art. 28.2 LOPDGDD añade los **8 supuestos a-h** que también obligan a valorar si procede la EIPD.

RECUERDA

Plazos del art. 36 RGPD para la consulta previa: la autoridad de control debe asesorar por escrito en **8 semanas** desde la solicitud, prorrogables **6 semanas** adicionales por complejidad (notificación de la prórroga en el plazo de un mes con motivos). Total máximo: **14 semanas**. Los plazos pueden suspenderse hasta que la autoridad obtenga la información solicitada.

MATIZ

EIPD ≠ consulta previa. La EIPD (art. 35) la realiza el **responsable** internamente, antes de iniciar el tratamiento, con el asesoramiento del DPO si lo hay. La consulta previa (art. 36) se hace **ante la autoridad de control** solo cuando la EIPD muestre alto riesgo no mitigable. La consulta previa presupone EIPD; no toda EIPD desemboca en consulta previa.

9. Bloqueo de los datos — art. 32 LOPDGDD

Artículo 32 LOPDGDD · Bloqueo de los datos

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.
2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente

elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

RECUERDA

Bloqueo del art. 32 LOPDGDD = identificación y reserva de los datos para impedir su tratamiento (incluida visualización), salvo puesta a disposición de jueces, MF y AAPP competentes (especialmente las autoridades de protección de datos) para exigir responsabilidades derivadas del tratamiento, **y solo por el plazo de prescripción** de esas responsabilidades. Transcurrido el plazo: **destrucción** de los datos.

MATIZ

Bloqueo ≠ supresión. Los datos bloqueados subsisten pero quedan inaccesibles, salvo para la única finalidad expresada (jueces/MF/AAPP/autoridades de control). No pueden tratarse para ningún otro fin (art. 32.3 LOPDGDD). Transcurrido el plazo de prescripción de las responsabilidades, los datos deben destruirse.

MATIZ

Alternativa al bloqueo del art. 32.4 LOPDGDD: si el sistema de información no permite el bloqueo o su adaptación implica esfuerzo desproporcionado, **copiado seguro** de la información con evidencia digital (o de otra naturaleza) que acredite autenticidad, fecha de bloqueo y no manipulación. Es la fórmula técnica para sistemas legacy que no admiten bloqueo nativo.

MATIZ

Excepciones a la obligación de bloqueo del art. 32.5 LOPDGDD: la AEPD y las autoridades autonómicas pueden fijar excepciones cuando la conservación bloqueada genere **riesgo elevado** para los afectados (por la naturaleza de los datos o por el número particularmente elevado de afectados) o implique **coste desproporcionado** para el responsable.

10. Sistemas de información crediticia — art. 20 LOPDGDD

Los **sistemas comunes de información crediticia** —conocidos en la práctica como **«ficheros de morosos»**— están regulados en el art. 20 LOPDGDD, que es un tratamiento concreto del Título IV LOPDGDD. Su régimen específico se incluye aquí porque encaja materialmente con las obligaciones del responsable y porque involucra una **corresponsabilidad** entre la entidad que mantiene el sistema y los acreedores que reportan la deuda.

Artículo 20 LOPDGDD · Sistemas de información crediticia

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Letra	Requisito del art. 20.1 LOPDGDD para la presunción de licitud
a	**Origen del dato**: facilitado por el acreedor o quien actúe por su cuenta o interés
b	**Calidad de la deuda**: cierta, vencida y exigible · sin reclamación administrativa o judicial pendiente del deudor · sin procedimiento alternativo de resolución vinculante en curso
c	**Información previa al deudor** (en contrato o requerimiento de pago) **+** la entidad del sistema notifica al afectado la inclusión y le informa de los derechos 15-22 RGPD dentro de los **30 días**

	siguientes a la notificación de la deuda al sistema, **permaneciendo bloqueados los datos durante ese plazo**
d	**Plazo máximo: 5 años** desde la fecha de vencimiento de la obligación, mientras persista el incumplimiento
e	**Quién puede consultar**: solo quien tenga relación contractual con el afectado o este le haya solicitado celebrar un contrato de financiación/pago aplazado/facturación periódica. Si se ha ejercitado limitación 18.1.a, el sistema informa de la existencia de la limitación, sin facilitar los datos concretos
f	**Comunicación al afectado del resultado de la consulta**: si la consulta resulta en denegación o no celebración del contrato, quien consultó debe informar al afectado

RECUERDA

Cuatro plazos y cifras del art. 20 LOPDGDD: **30 días** de notificación al afectado tras inclusión, con bloqueo durante ese plazo (20.1.c); **5 años** plazo máximo de permanencia desde el vencimiento de la obligación (20.1.d); **corresponsabilidad** del art. 26 RGPD entre entidad del sistema y acreedoras (20.2); **el acreedor responde** de la existencia y exactitud de la deuda incluida (20.2 in fine).

MATIZ

No existe en el art. 20 LOPDGDD una cuantía mínima de la deuda para inclusión (a diferencia de algunas formulaciones doctrinales antiguas o de manuales que mencionan «50 euros»). El BOE consolidado de la LOPDGDD no fija ninguna cifra de importe mínimo: la inclusión depende del cumplimiento de los **requisitos cualitativos a-f del 20.1** y de la corresponsabilidad del 20.2.

MATIZ

Reclamación pendiente bloquea la inclusión (art. 20.1.b LOPDGDD): si la existencia o cuantía de la deuda ha sido **impugnada** por el deudor (vía administrativa, judicial o por procedimiento alternativo de resolución vinculante), no cabe incluirla en el sistema crediticio mientras dure la impugnación. La presunción de licitud decae automáticamente.

MATIZ

Plazo de 5 años corre desde la fecha de vencimiento, no desde la inclusión en el sistema (art. 20.1.d LOPDGDD). Una deuda vencida hace 4 años e incluida hoy en el fichero solo puede mantenerse durante 1 año más, no durante 5.

MATIZ

La presunción de licitud del 20.1 NO ampara el perfilado adicional (art. 20.3 LOPDGDD): si la entidad del sistema asocia la información crediticia con datos adicionales obtenidos de otras fuentes para hacer perfilado o calificación crediticia (*credit scoring*), el régimen del 20 no cubre ese tratamiento, que necesita base jurídica propia y enfrentará las exigencias plenas de responsabilidad activa, EIPD y derechos sobre decisiones automatizadas (art. 22 RGPD).

TEMA 4

Epígrafe 5 — Delegado y autoridades de protección de datos

El delegado de protección de datos (DPO) y las autoridades de control son las dos piezas institucionales del sistema. El DPO se regula en los **arts. 37-39 RGPD** y **arts. 34-37 LOPDGDD** (Capítulo III del Título V). Las autoridades de control son: la **AEPD** (Capítulo I del Título VII LOPDGDD, arts. 44-56), las **autoridades autonómicas** (Capítulo II del Título VII, arts. 57-62) y el **Comité Europeo de Protección de Datos (CEPD)** (Capítulo VII RGPD, art. 68 ss.). El régimen sancionador (Título IX LOPDGDD, arts. 70-78 + art. 83 RGPD) y las transferencias internacionales (Título VI LOPDGDD, arts. 40-43 + Capítulo V RGPD, arts. 44-49) cierran este epígrafe como materias ordinarias del sistema institucional.

1. El delegado de protección de datos (DPO): designación obligatoria — art. 37 RGPD + art. 34 LOPDGDD

Artículo 37 RGPD · Designación del delegado de protección de datos

> 1. 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 con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.
3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de tales asociaciones y otros organismos que representen a responsables o encargados.
5. El delegado de protección de datos 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 las funciones indicadas en el artículo 39.
6. 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.
7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 34 LOPDGDD · Designación de un delegado de protección de datos

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

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 el artículo 1 de 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, reguladas por la legislación del Mercado de Valores.

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 la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

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.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

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 la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.
3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en

los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.
5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

RECUERDA

Tres supuestos del art. 37.1 RGPD que activan la designación obligatoria del DPO: a) autoridad u organismo público (salvo tribunales en función judicial) · b) observación habitual y sistemática de interesados a gran escala · c) tratamiento a gran escala de categorías especiales o datos penales. A esto, el **art. 34.1 LOPDGDD añade 16 supuestos a-o** del Derecho español (colegios profesionales, centros docentes, comunicaciones electrónicas, perfiladores SSI, entidades financieras y aseguradoras, energía, ficheros de morosos, publicidad con perfiles, centros sanitarios, informes comerciales, juego online, seguridad privada y federaciones deportivas con menores).

MATIZ

Los profesionales de la salud individuales están expresamente excluidos de la obligación de designar DPO, aunque estén legalmente obligados al mantenimiento de las historias clínicas (art. 34.1.l LOPDGDD in fine). La obligación recae sobre los **centros sanitarios**, no sobre los profesionales individuales.

MATIZ

DPO designado voluntariamente = mismo régimen que el obligatorio (art. 34.2 LOPDGDD): si una entidad no obligada decide nombrar DPO, queda sometida íntegramente al RGPD y a la LOPDGDD como si fuera obligatorio. La voluntariedad es del nombramiento, no del régimen aplicable.

MATIZ

DPO único para grupo empresarial o varias autoridades públicas: el RGPD admite un solo DPO para un grupo empresarial siempre que sea **fácilmente accesible desde cada establecimiento** (art. 37.2 RGPD), y un solo DPO para varias autoridades u organismos públicos teniendo en cuenta su estructura organizativa y tamaño (art. 37.3 RGPD). El DPO puede ser **interno** (plantilla) o **externo** (contrato de servicios) — art. 37.6 RGPD.

2. Cualificación del DPO — art. 35 LOPDGDD + art. 37.5 RGPD

Artículo 35 LOPDGDD · Cualificación del delegado de protección de datos

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios,

> a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

El art. 37.5 RGPD exige que el DPO sea 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 las funciones indicadas en el artículo 39». La LOPDGDD complementa: sea persona física o jurídica, los conocimientos pueden acreditarse por **certificación voluntaria** (esquema gestionado por la AEPD a través del **Esquema AEPD-DPD**) o por **titulación universitaria**.

MATIZ

El DPO puede ser persona jurídica (art. 35 LOPDGDD), no necesariamente persona física. Una empresa de servicios de protección de datos puede ser designada DPO por contrato de servicios (art. 37.6 RGPD). En esos casos, los conocimientos especializados deben acreditarse por la entidad mediante certificación o titulación.

3. Posición y garantías del DPO — art. 38 RGPD + art. 36 LOPDGDD

Artículo 38 RGPD · Posición del delegado de protección de datos

> 1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.
6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 36 LOPDGDD · Posición del delegado de protección de datos

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El dele-

gado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.
3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.
4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Garantía del DPO	Norma	Contenido
Participación oportuna	Art. 38.1 RGPD	En todas las cuestiones relativas a la protección de datos
Recursos suficientes	Art. 38.2 RGPD	Recursos + acceso a datos y procesos + mantenimiento de conocimientos
Sin instrucciones	Art. 38.3 RGPD	El responsable no puede instruirle sobre cómo desempeñar sus funciones
Inamovilidad	Art. 38.3 RGPD + 36.2 LOPDGDD	No puede ser destituido ni sancionado por desempe-

		ñar sus funciones; **excepción LOPDGDD: dolo o negligencia grave**
Rendición al más alto nivel	Art. 38.3 RGPD	Reporta directamente al órgano de administración/dirección
Acceso irrestricto a datos	Art. 36.3 LOPDGDD	No se le puede oponer ningún deber de confidencialidad o secreto, **incluido el del art. 5 LOPDGDD**
Confidencialidad propia	Art. 38.5 RGPD	El DPO está obligado a mantener secreto o confidencialidad
Sin conflicto de intereses	Art. 38.6 RGPD	Si desempeña otras funciones, no deben generar conflicto
Comunicación de vulneraciones	Art. 36.4 LOPDGDD	Si aprecia vulneración relevante: documentar + comunicar inmediatamente al órgano de administración/dirección

MATIZ

Inamovilidad reforzada del DPO, pero **no absoluta** (art. 36.2 LOPDGDD): el DPO no puede ser removido ni sancionado por desempeñar sus funciones, **salvo que incurra en dolo o negligencia grave** en su ejercicio. La excepción es estrecha: la mera discrepancia, opinión incómoda o resistencia inspectora del DPO no son causa de remoción.

MATIZ

Frente al DPO no cabe oponer el deber de confidencialidad del art. 5 LOPDGDD (art. 36.3 LOPDGDD). Esta prevalencia es esencial para que el DPO pueda inspeccionar los procesos internos sin verse bloqueado por cláusulas de confidencialidad o secreto profesional. El DPO tiene su propia obligación de confidencialidad (art. 38.5 RGPD).

4. Funciones del DPO — art. 39 RGPD

Artículo 39 RGPD · Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

RECUERDA

Cinco funciones a-e del DPO (art. 39.1 RGPD): a) **informar y asesorar** al responsable, encargado y empleados · b) **supervisar el cumplimiento** del RGPD y políticas internas (con concienciación, formación y auditorías) · c) **asesorar y supervisar la EIPD** del art. 35 · d) **cooperar con la autoridad de control** · e) **actuar como punto de contacto** de la autoridad de control, incluida la consulta previa del art. 36.

5. Intervención del DPO en caso de reclamación — art. 37 LOPDGDD

Artículo 37 LOPDGDD · Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

Plazo DPO	Norma	Supuesto
10 días	Art. 34.3 LOPDGDD	Comunicación a la AEPD o autoridad autonómica de las **designaciones, nombramientos y ceses** del DPO (obligatorios o voluntarios)
2 meses	Art. 37.1 LOPDGDD	Plazo máximo de respuesta del DPO al afectado cuando este se dirige al DPO **antes** de presentar reclamación ante la autoridad de control
1 mes	Art. 37.2 LOPDGDD	Plazo de respuesta del DPO cuando la AEPD o autoridad autonómica le **remite** una reclamación ya presentada

RECUERDA

Plazos del DPO «10-2-1»: 10 días comunicar designación/cese a la AEPD o autoridad autonómica · **2 meses** respuesta del DPO al afectado en reclamación previa · **1 mes** respuesta del DPO cuando la autoridad de control le remite una reclamación.

MATIZ

El DPO NO está sujeto al régimen sancionador del Título IX LOPDGDD (art. 70.2 LOPDGDD). Su responsabilidad es interna —ante el responsable/encargado del tratamiento, con la inamovilidad reforzada del 36.2— y profesional, no administrativa. La AEPD no puede imponerle sanción al DPO por sus actuaciones.

6. La Agencia Española de Protección de Datos (AEPD) — arts. 44-49 LOPDGDD

Artículo 44 LOPDGDD · Disposiciones generales

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.
3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 47 LOPDGDD · Funciones y potestades de la AEPD

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48 LOPDGDD · La Presidencia de la AEPD (apartados clave)

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.
2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción

de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de

Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.
5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,

b) incapacidad sobrevenida para el ejercicio de su función,

c) incompatibilidad, o

> d) condena firme por delito doloso.
>
> En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.
>
> 6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Aspecto de la Presidencia AEPD	Regla
Nombramiento	Por el Gobierno, a propuesta del **Ministerio de Justicia**, entre personas de reconocida competencia profesional. Real decreto del Consejo de Ministros
Ratificación parlamentaria	Comisión de Justicia del Congreso: **3/5 en primera votación** o **mayoría absoluta en segunda** (con al menos 2 grupos parlamentarios)
Mandato	**5 años**, renovable **una vez** por igual período
Causas de cese anticipado	A petición propia · a) incumplimiento grave · b) incapacidad sobrevenida · c) incompatibilidad · d) condena firme por delito doloso. Las causas a/b/c **requieren ratificación parlamentaria** la d) **NO**
Independencia	Plena, sin instrucciones; régimen del alto cargo
Adjunto	Sustituye a la Presidencia, salvo en procedimientos del Título VIII
Recursos contra resoluciones	Directamente ante la **Sala de lo Contencioso-Administrativo de la Audiencia Nacional** (no Tribunal Supremo)
Circulares	Vinculantes desde su publicación en el BOE (art. 55.3 LOPDGDD)

Consejo Consultivo de la AEPD (art. 49 LOPDGDD). El Consejo Consultivo asesora a la Presidencia de la AEPD. Sus decisiones **no son vinculantes**. Se reúne cuando lo

disponga la Presidencia y, en todo caso, **al menos una vez al semestre**. Está compuesto por miembros de procedencia institucional y técnica diversa: un Diputado, un Senador, un representante del CGPJ, un representante de la AGE propuesto por el MJ, un representante por cada CCAA con autoridad propia de protección de datos, un experto de la FEMP, un experto del Consejo de Consumidores y Usuarios, dos expertos por las organizaciones empresariales, un representante de los profesionales de protección de datos, un representante de los organismos de supervisión y resolución extrajudicial de conflictos del Capítulo IV del Título V, un experto por la CRUE, un representante de los Consejos Generales/Superiores y Colegios Profesionales, un representante de los profesionales de seguridad de la información, un experto en transparencia y acceso (propuesto por el CTBG) y dos expertos propuestos por las organizaciones sindicales más representativas.

RECUERDA

Tres datos de la Presidencia AEPD: mandato **5 años renovable una vez** · cese anticipado por 4 causas (a/b/c **necesitan ratificación parlamentaria**, d) condena firme por delito doloso **no la necesita**) · recursos contra sus resoluciones directamente ante la **Audiencia Nacional** (no TS).

MATIZ

La AEPD se relaciona con el Gobierno a través del Ministerio de Justicia (art. 44.1 LOPDGDD), no del Ministerio de la Presidencia ni del Ministerio del Interior. El nombramiento y la propuesta de candidatos también vienen del MJ.

MATIZ

Las circulares de la AEPD son obligatorias desde su publicación en el BOE (art. 55.3 LOPDGDD). Son normas reglamentarias dentro del ámbito de competencias de la Agencia y vinculan a los responsables y encargados sometidos a su control.

7. Las autoridades autonómicas de protección de datos — arts. 57-62 LOPDGDD

Artículo 57 LOPDGDD · Autoridades autonómicas de protección de datos

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 59 LOPDGDD · Tratamientos contrarios al RGPD

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento

(UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Aspecto autoridades autonómicas	Regla
Ámbito competencial (art. 57 LOPDGDD)	Tratamientos del sector público autonómico/local · funciones públicas autonómicas/locales · materia de Estatutos de Autonomía
Circulares propias	Permitidas, con el régimen del art. 55 LOPDGDD (efecto desde publicación en boletín autonómico)
Cooperación con AEPD (art. 58 LOPDGDD)	Reuniones semestrales · intercambio de información (incluida la del CEPD) · grupos de trabajo conjuntos
Requerimiento de la AEPD (art. 59 LOPDGDD)	Si la AEPD considera que un tratamiento autonómico vulnera el RGPD: requerimiento de **1 mes** para cesación. Si no atiende → **acciones contencioso-administrativas**
Coordinación CEPD (arts. 60-62 LOPDGDD)	Las comunicaciones autonómicas con el CEPD se canalizan a través de la AEPD. La AEPD es asistida por un representante autonómico en su intervención ante el CEPD
Tratamientos transfronterizos (art. 61 LOPDGDD)	Las autoridades autonómicas pueden ser autoridad de control principal o interesada en el procedimiento del art. 60 RGPD

MATIZ

Las autoridades autonómicas pueden dictar circulares vinculantes (art. 57.2 LOPDGDD), con el mismo régimen del art. 55 LOPDGDD aplicable a las circulares de la AEPD. La diferencia es el ámbito subjetivo de aplicación: solo a los tratamientos sometidos a su competencia autonómica.

MATIZ

Conducto AEPD obligatorio para el CEPD (arts. 60 y 62 LOPDGDD): las autoridades autonómicas no se relacionan directamente con el CEPD, sino a través de la AEPD, que es el «representante común» de España (art. 44.2 LOPDGDD). En la intervención de la AEPD ante el CEPD asiste un representante de la autoridad autonómica.

8. El Comité Europeo de Protección de Datos (CEPD) — art. 68 RGPD + art. 44.2 LOPDGDD

El **Comité Europeo de Protección de Datos (CEPD)** —regulado en los arts. 68-76 del RGPD, Capítulo VII— es el organismo de la Unión Europea (con personalidad jurídica) que **garantiza la aplicación coherente del RGPD** en todos los Estados miembros. Está compuesto por el director de la autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos (SEPD), o sus respectivos representantes.

Función del CEPD	Norma
Aplicación coherente del RGPD en toda la UE	Art. 70.1 RGPD
Dictámenes sobre proyectos de decisión de las autoridades de control	Art. 64 RGPD
Decisiones vinculantes para resolver conflictos entre autoridades de control	Art. 65 RGPD
Directrices, recomendaciones y mejores prácticas	Art. 70 RGPD

Lista de tratamientos que requieren EIPD	Art. 35.4 RGPD
Cláusulas contractuales tipo y **normas corporativas vinculantes** (BCR): dictamen previo	Art. 64.1.f RGPD
Asesoramiento a la Comisión sobre nivel de protección de terceros países y temas de tratamiento	Art. 70.1.s RGPD

RECUERDA

AEPD = representante común de las autoridades de protección de datos del Reino de España ante el CEPD (art. 44.2 LOPDGDD). Las autoridades autonómicas no están representadas directamente, sino a través de la AEPD, que es asistida por un representante autonómico cuando el asunto les afecte.

MATIZ

CEPD ≠ Comisión Europea ≠ Supervisor Europeo de Protección de Datos (SEPD). El CEPD es un organismo de la UE con personalidad jurídica propia (art. 68.1 RGPD) que coordina a las autoridades nacionales de control. La Comisión adopta las **decisiones de adecuación** (art. 45 RGPD) y las **cláusulas contractuales tipo** (art. 46.2.c RGPD). El SEPD supervisa los tratamientos de las **instituciones, órganos y organismos de la Unión**. Son tres figuras distintas con funciones complementarias.

9. Régimen sancionador — Título IX LOPDGDD (arts. 70-78) + art. 83 RGPD

Artículo 70 LOPDGDD · Sujetos responsables

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Infracciones y prescripción de la infracción — arts. 71-74 LOPDGDD.

Tipo de infracción	Norma	Prescripción de la infracción	Sanción máxima del art. 83 RGPD
Muy graves	Art. 72 LOPDGDD (16 letras a-p) ↔ art. 83.5 y 83.6 RGPD	**3 años**	Hasta **20.000.000 €** o **4%** del volumen de negocio anual mundial total del ejercicio anterior (el importe mayor)
Graves	Art. 73 LOPDGDD (29 letras a-ac) ↔ art. 83.4 RGPD	**2 años**	Hasta **10.000.000 €** o **2%** del volumen de negocio anual mundial total del ejercicio anterior (el importe mayor)
Leves	Art. 74 LOPDGDD ↔ apartados 4 y 5 del art. 83 RGPD	**1 año**	Apercibimiento o multas dentro de los techos del art. 83.4 RGPD

Selección de infracciones muy graves (art. 72 LOPDGDD).

- **a)** Tratamiento de datos vulnerando los principios y garantías del art. 5 RGPD.
- **b)** Tratamiento sin alguna de las condiciones de licitud del art. 6 RGPD.
- **c)** Incumplimiento de los requisitos del art. 7 RGPD para el consentimiento.
- **e)** Tratamiento de categorías especiales del art. 9 RGPD sin amparo.

- **f)** Tratamiento de datos penales fuera de los supuestos del art. 10 RGPD/LOPDGDD.
- **h)** Omisión del deber de informar al afectado (arts. 13/14 RGPD + 12 LOPDGDD).
- **i)** Vulneración del deber de confidencialidad del art. 5 LOPDGDD.
- **k)** Impedimento, obstaculización o no atención reiterada del ejercicio de los derechos 15-22 RGPD.
- **l)** Transferencia internacional sin garantías de los arts. 44-49 RGPD.
- **m)** Incumplimiento de resoluciones de la autoridad de control (art. 58.2 RGPD).
- **n)** Incumplimiento de la obligación de bloqueo del art. 32 LOPDGDD.
- **o)** Resistencia u obstrucción a la función inspectora.
- **p)** Reversión deliberada de un procedimiento de anonimización.

Sanciones y publicación — arts. 76 y 78 LOPDGDD.

Aspecto	Regla
Criterios de graduación	Los del art. 83.2 RGPD + criterios adicionales del 76.2 LOPDGDD a-h (carácter continuado, vinculación al tratamiento, beneficios obtenidos, conducta del afectado, fusión por absorción posterior, afectación a menores, DPO voluntario, mecanismos alternativos de resolución de conflictos)
Publicación BOE de la sanción (art. 76.4 LOPDGDD)	Cuando la AEPD sanciona con importe **superior a 1.000.000 €** y el infractor sea **persona jurídica**, se publica en el BOE: identidad del infractor, infracción y importe
Prescripción de las sanciones (art. 78 LOPDGDD)	Hasta 40.000 € → **1 año** · entre 40.001 y 300.000 € → **2 años** · más de 300.000 € → **3 años**

RECUERDA

Tres prescripciones del art. 78 LOPDGDD en escala con el importe: **40.000 € → 1 año · 300.000 € → 2 años · >300.000 € → 3 años**. Distinguir de la prescripción **de la infracción** (3/2/1 años para muy graves/graves/leves del 72-74 LOPDGDD).

MATIZ

Los techos del art. 83 RGPD se aplican siempre el importe MAYOR (€ o % del volumen de negocio mundial), nunca el menor: **20M€ o 4%** para muy graves del 83.5 · **10M€ o 2%** para graves del 83.4. La cifra del 4% suele aplicar a multinacionales con facturación >500M€ anuales.

MATIZ

El DPO no está sujeto al régimen sancionador del Título IX (art. 70.2 LOPDGDD), pero **el responsable o encargado sí pueden ser sancionados** por no posibilitar la efectiva participación del DPO, no respaldarlo o interferir en sus funciones (infracción **grave** del art. 73.w LOPDGDD).

10. Régimen especial del sector público — art. 77 LOPDGDD

Artículo 77 LOPDGDD · Régimen aplicable a determinadas categorías de responsables o encargados

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.
6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Sujetos del art. 77.1 LOPDGDD (régimen especial sin multa)
a) Órganos constitucionales o con relevancia constitucional + instituciones autonómicas análogas
b) Órganos jurisdiccionales
c) AGE · Administraciones autonómicas · Administración Local
d) Organismos públicos y entidades de Derecho público vinculados o dependientes
e) Autoridades administrativas independientes

f) Banco de España
g) Corporaciones de Derecho público (cuando ejerzan potestades de derecho público)
h) Fundaciones del sector público
i) Universidades Públicas
j) Consorcios
k) Grupos parlamentarios de Cortes Generales/Asambleas autonómicas + grupos políticos locales

RECUERDA

Las entidades del sector público del art. 77.1 LOPDGDD NO se les impone multa económica. En su lugar, la autoridad de protección de datos: (i) declara la infracción · (ii) establece **medidas correctoras** para que cese la conducta o corrija sus efectos · (iii) **propone actuaciones disciplinarias** si hay indicios · (iv) cuando la infracción sea imputable a autoridades y directivos que no atendieron informes técnicos previos: **amonestación nominativa con publicación en el BOE** o boletín autonómico · (v) **comunicación al Defensor del Pueblo** o instituciones análogas.

MATIZ

El Banco de España y las autoridades administrativas independientes están en el régimen especial del 77.1 (letras e y f). Esto incluye a la propia AEPD cuando trate datos personales como responsable de sus tratamientos internos: la AEPD se autosanciona con declaración de infracción y medidas correctoras, no con multa.

11. Transferencias internacionales de datos — Capítulo V RGPD (arts. 44-49) + Título VI LOPDGDD (arts. 40-43)

Una **transferencia internacional** es el flujo de datos personales desde el ámbito del RGPD (territorio UE + EEE) a destinatarios en **terceros países u organizaciones**

internacionales. El **Espacio Económico Europeo (EEE)** comprende los 27 Estados de la UE más Liechtenstein, Islandia y Noruega; las transferencias dentro del EEE no son internacionales a efectos del RGPD.

Artículo 44 RGPD · Principio general

> Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Mecanismo	Norma RGPD	Requisito / Quién decide
1. Decisión de adecuación	Art. 45 RGPD	El tercer país/organización internacional ofrece un nivel de protección adecuado. Decisión de la **Comisión Europea** mediante acto de ejecución, con revisión periódica al menos cada **4 años**. **Sin necesidad de autorización adicional**
2. Garantías adecuadas sin autorización	Art. 46.2 RGPD	a) Instrumento jurídicamente vinculante entre autoridades públicas · b) **normas corporativas vinculantes (BCR)** del art. 47 · c) **cláusulas tipo** adoptadas por la Comisión · d) cláusulas tipo adoptadas por una autoridad de control y aprobadas por la Comisión · e) código de conducta aprobado · f) mecanismo de certificación aprobado

3. **Garantías adecuadas con autorización**	Art. 46.3 RGPD	a) Cláusulas contractuales no estándar entre responsables/encargados · b) acuerdos administrativos entre autoridades u organismos públicos. Requieren autorización de la **autoridad de control competente** y aplicación del mecanismo de coherencia
4. **Excepciones para situaciones específicas**	Art. 49.1 RGPD	a) Consentimiento explícito tras información de los riesgos · b) ejecución de contrato con el interesado · c) contrato en interés del interesado · d) razones importantes de interés público · e) reclamaciones · f) intereses vitales · g) registro público. **Las letras a, b y c NO se aplican a autoridades públicas en ejercicio de poderes públicos** (49.3)
5. **Intereses legítimos imperiosos**	Art. 49.1 párrafo 2 RGPD + art. 43 LOPDGDD	Cuando ningún mecanismo anterior es aplicable: no repetitiva · número limitado de interesados · necesaria para intereses legítimos imperiosos no superados por los del interesado · responsable evaluó garantías apropiadas · informa a la AEPD y al interesado. **NO aplica a autoridades públicas en ejercicio de poderes públicos**

Artículo 41 LOPDGDD · Supuestos de adopción por la AEPD (apartados clave)

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42 LOPDGDD · Autorización previa (apartados clave)

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos […]

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de

> Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Plazo del procedimiento de transferencias internacionales	Norma	Duración
Aprobación de cláusulas contractuales tipo por la AEPD	Art. 41.1 LOPDGDD	Sometido previamente al dictamen del CEPD; sin plazo numérico fijado
Aprobación de normas corporativas vinculantes (BCR)	Art. 41.2 LOPDGDD	**9 meses** (suspendido durante remisión al CEPD)
Autorización previa de la AEPD para transferencias sin garantías	Art. 42.1 LOPDGDD	**6 meses** (suspendido durante remisión al CEPD)
Información previa por intereses legítimos imperiosos	Art. 43 LOPDGDD	Antes de la transferencia + información al afectado

RECUERDA

Cinco mecanismos para transferir datos fuera del EEE, en orden de mayor a menor garantía: (1) **decisión de adecuación** de la Comisión · (2) **garantías adecuadas sin autorización** (BCR · cláusulas tipo · códigos de conducta · certificación) · (3) **garantías adecuadas con autorización** de la autoridad de control · (4) **excepciones del 49.1** (consentimiento explícito, contrato, interés público…) · (5) **intereses legítimos imperiosos** del 49.1 párr. 2 (residual, con información a AEPD).

RECUERDA

Plazos de los procedimientos LOPDGDD: **9 meses** para aprobación de BCR (art. 41.2 LOPDGDD) · **6 meses** para autorización previa de transferencia sin garantías (art. 42.1 LOPDGDD). Ambos suspendibles por remisión del expediente al CEPD (que emite dictamen ex art. 64 RGPD).

MATIZ

La decisión de adecuación la adopta la Comisión Europea, no la AEPD ni el CEPD (art. 45.3 RGPD). La AEPD puede, en cambio, aprobar cláusulas contractuales tipo propias (sometidas a dictamen previo del CEPD), aprobar BCR y autorizar transferencias específicas. Las actuales decisiones de adecuación cubren, entre otros, países como Andorra, Argentina, Canadá (entidades comerciales), Israel, Japón, Nueva Zelanda, Reino Unido, Suiza, Uruguay, Corea del Sur y los EE. UU. (bajo el *Data Privacy Framework*).

MATIZ

El mecanismo de intereses legítimos imperiosos del art. 43 LOPDGDD NO es aplicable a autoridades públicas en ejercicio de sus poderes públicos (último párrafo del 43, en remisión al art. 49.3 RGPD). Para las AAPP que actúan en su esfera pública solo caben los mecanismos generales (decisión de adecuación, garantías del 46 o autorización previa).

MATIZ

Una transferencia a un país sin decisión de adecuación NO es automáticamente ilícita. Puede ampararse en garantías adecuadas (cláusulas tipo, BCR, códigos, certificación), en garantías con autorización previa o en una excepción del 49.1. Lo prohibido es transferir **sin ningún mecanismo** de garantía.

TEMA 4

Epígrafe 6 — Derechos digitales

El **Título X LOPDGDD** —arts. 79 a 97— recoge el catálogo de **derechos digitales** específico del ordenamiento español, que excede la materia armonizada del RGPD y constituye uno de los rasgos diferenciales de la LO 3/2018. La estructura interna del Título X es cuádruple: derechos en internet (arts. 79-86), derechos en el ámbito laboral (arts. 87-91), derechos digitales sobre contenidos —olvido, portabilidad y testamento digital— (arts. 92-96) y políticas de impulso (art. 97). En el capítulo laboral se integra también el **art. 22 LOPDGDD** (tratamientos con fines de videovigilancia), por su conexión directa con el art. 89 (videovigilancia laboral): el art. 22 fija la regla general y el art. 89 la especialización en el centro de trabajo.

1. Derechos en internet — arts. 79-86 LOPDGDD

Artículo 79 LOPDGDD · Los derechos en la era digital

> Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80 LOPDGDD · Derecho a la neutralidad de Internet

> Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81 LOPDGDD · Derecho de acceso universal a Internet

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.
2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.
4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.
5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.
6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82 LOPDGDD · Derecho a la seguridad digital

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83 LOPDGDD · Derecho a la educación digital

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el

respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.
4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84 LOPDGDD · Protección de los menores en Internet

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información

a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85 LOPDGDD · Derecho de rectificación en Internet

1. Todos tienen derecho a la libertad de expresión en Internet.
2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86 LOPDGDD · Derecho a la actualización de informaciones en medios de comunicación digitales

> Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.
>
> En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Art.	Derecho	Idea-fuerza
79	Derechos en la era digital	Los derechos constitucionales y de Tratados son **plenamente aplicables en internet**. Prestadores SSI y proveedores de internet **contribuyen** a su aplicación
80	Neutralidad de internet	Oferta transparente sin **discriminación técnica o económica**
81	Acceso universal	Independientemente de la condición personal, social, económica o geográfica. Garantías específicas: brecha de género, brecha generacional (personas mayores), entornos rurales, personas con necesidades especiales
82	Seguridad digital	Derecho a la seguridad en las comunicaciones de internet. Los proveedores **informan** a los usuarios

83	Educación digital	Sistema educativo: inserción en sociedad digital + competencia digital en currículo + formación del profesorado + formación en planes universitarios. **AA. PP. incorporarán** materias de derechos digitales **a los temarios de cuerpos superiores** y de cuerpos con acceso habitual a datos personales
84	Protección de menores	Padres/tutores/representantes **procurarán** uso equilibrado. Difusión ilegítima de imágenes de menores → **intervención del Ministerio Fiscal** con medidas cautelares de la LO 1/1996
85	Rectificación en internet	Libertad de expresión en internet + responsables de redes sociales con protocolos para rectificación (LO 2/1984). Medios digitales que deban rectificar: **publicar aviso aclaratorio visible junto a la información original**
86	Actualización en medios digitales	Solicitud motivada de **aviso de actualización visible** cuando la noticia original no refleje la situación actual y cause perjuicio. **Especial mención** de actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado por decisiones judiciales posteriores

RECUERDA

Tres fórmulas literales del art. 81 LOPDGDD sobre brechas digitales que el acceso universal debe procurar superar: **brecha de género** (81.3) · **brecha generacional / personas mayores** (81.4) · **entornos rurales** (81.5) · **personas con necesidades especiales** (81.6). Cuatro grupos protegidos del derecho de acceso universal a internet.

MATIZ

El art. 83.4 LOPDGDD obliga a las AA. PP. a incorporar materias de derechos digitales a los temarios de las pruebas de acceso a los cuerpos superiores y a aquellos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales.

MATIZ

Distinguir derecho de rectificación (art. 85) y derecho de actualización (art. 86). La **rectificación** se ampara en la LO 2/1984 frente a información ofensiva contra honor o intimidad: el medio publica aviso aclaratorio. La **actualización** procede cuando la noticia ya no refleja la situación actual del afectado por circunstancias **posteriores a la publicación**, especialmente actuaciones policiales o judiciales favorables sobrevenidas: el medio publica aviso de actualización con referencia a la decisión posterior.

2. Derechos en el ámbito laboral — arts. 87-91 LOPDGDD + art. 22 LOPDGDD

Artículo 87 LOPDGDD · Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.
2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.
3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88 LOPDGDD · Derecho a la desconexión digital en el ámbito laboral

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.
3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 22 LOPDGDD · Tratamientos con fines de videovigilancia (régimen general)

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.
2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.
7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.
8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 89 LOPDGDD · Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respecti-

vamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.
3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90 LOPDGDD · Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.
2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91 LOPDGDD · Derechos digitales en la negociación colectiva

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Art.	Derecho laboral	Idea-fuerza
22 LOPDGDD	Videovigilancia (general)	**1 mes** plazo de conservación · **72 horas** para poner a disposición de autoridad si capta acto ilícito · cartel informativo del 22.4 cumple deber de información del art. 12 RGPD · exclusión doméstica del 22.5 (no aplica si hay empresa de seguridad privada contratada)

87	Intimidad en dispositivos digitales	Acceso del empleador solo para **controlar cumplimiento laboral** o **garantizar integridad** de los dispositivos. Criterios de uso con **participación de representantes**. Si se admite uso privado: especificación precisa de usos autorizados + garantías para preservar la intimidad
88	Desconexión digital	Fuera del tiempo de trabajo legal o convencional. Aplica también en **teletrabajo y trabajo a distancia**. Política interna del empleador con audiencia previa de representantes + acciones de formación contra fatiga informática
89	Videovigilancia laboral	Funciones de control del art. 20.3 ET y legislación de función pública. **Información previa expresa, clara y concisa**. Acto ilícito flagrante: basta con el cartel del 22.4. **PROHIBIDO** en vestuarios, aseos, comedores y análogos. Grabación de sonidos solo si hay riesgos relevantes
90	Geolocalización	Información previa **expresa, clara e inequívoca** + información sobre derechos de acceso, rectificación, limitación y supresión
91	Negociación colectiva	Los convenios colectivos pueden establecer **garantías adicionales**

RECUERDA

Plazos del art. 22 LOPDGDD: **1 mes** plazo máximo de conservación de las imágenes desde su captación · **72 horas** para poner a disposición de la autoridad competente si las imágenes acreditan un acto ilícito · **NO aplica** la obligación de bloqueo del art. 32 LOPDGDD a estos tratamientos.

MATIZ

El cartel informativo del art. 22.4 LOPDGDD cumple por sí solo el deber de información del art. 12 RGPD, siempre que identifique al menos: (i) **existencia del tratamiento** · (ii) **identidad del responsable** · (iii) **posibilidad de ejercer los derechos 15-22 RGPD**. Puede incluir además código QR o dirección de internet.

MATIZ

Exclusión doméstica con su excepción (art. 22.5 LOPDGDD): el tratamiento por persona física de imágenes que solo capten el interior del propio domicilio queda excluido del RGPD/LOPDGDD. **PERO** la exclusión NO se aplica si quien vigila el domicilio es una **empresa de seguridad privada contratada** que tenga acceso a las imágenes (en ese caso sí hay tratamiento sometido a la LOPDGDD).

MATIZ

Distinción art. 22 (videovigilancia general) vs art. 89 (videovigilancia laboral). El art. 22 regula la videovigilancia como tratamiento de datos en general (cualquier responsable, finalidad de seguridad). El art. 89 regula específicamente la videovigilancia del **empleador sobre los trabajadores** (función de control del art. 20.3 ET). Son dos regímenes distintos pero complementarios: el art. 22.8 LOPDGDD remite expresamente al 89 para el tratamiento por el empleador.

MATIZ

PROHIBICIÓN ABSOLUTA del art. 89.2 LOPDGDD: NUNCA se admite la videovigilancia ni la grabación de sonidos en **vestuarios, aseos, comedores y análogos** —lugares destinados al descanso o esparcimiento de los trabajadores —. Es prohibición absoluta sin excepción.

MATIZ

El derecho a la desconexión digital aplica también en teletrabajo y trabajo a distancia (art. 88.3 LOPDGDD in fine). El empleado que trabaja desde casa también tiene derecho a desconectarse fuera del tiempo de trabajo, y la política interna del empleador debe preservar expresamente este derecho en esos supuestos.

MATIZ

La desconexión digital aplica también a los empleados públicos vía art. 14.j bis del TREBEP, introducido por la disp. final 14.ª LO 3/2018. El derecho no es solo laboral privado sino estatutario funcionarial (sin distinción).

3. Derechos digitales sobre contenidos: olvido, portabilidad y testamento digital — arts. 92-96 LOPDGDD

Artículo 92 LOPDGDD · Protección de datos de los menores en Internet

> Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
>
> Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93 LOPDGDD · Derecho al olvido en búsquedas de Internet

> 1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
>
> Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus

derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94 LOPDGDD · Derecho al olvido en servicios de redes sociales y servicios equivalentes

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.
2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen

la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95 LOPDGDD · Derecho de portabilidad en servicios de redes sociales y servicios equivalentes

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96 LOPDGDD · Derecho al testamento digital

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido

hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.
4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Art.	Derecho	Régimen
92	Protección de datos de menores en internet	Centros educativos y cualquier persona/entidad que desarrolle actividades con menores → garantizan interés superior + derechos fundamentales. Publicación/difusión en redes sociales → **consentimiento del menor o representantes legales** (remisión al art. 7 LOPDGDD: ≥14 años por sí mismos / <14 años titulares de la patria potestad o tutela)
93	Olvido en buscadores	Eliminación de enlaces obtenidos por búsqueda **a partir del nombre** del afectado cuando los datos sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos. **Subsiste** aunque sea lícita la conservación en el sitio web original.

		No impide el acceso a la información usando criterios de búsqueda distintos del nombre
94	Olvido en redes sociales	Datos **propios** del afectado: supresión **a simple solicitud** · Datos de **terceros**: supresión cuando sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos · Datos facilitados durante la **minoría de edad**: supresión sin dilación a simple solicitud, sin necesidad de las condiciones del apartado 2 · **Excepción**: datos facilitados por personas físicas en ejercicio de actividades personales o domésticas
95	Portabilidad en redes sociales	Recibir y transmitir contenidos facilitados al prestador + transmisión directa a otro prestador designado por el usuario cuando sea técnicamente posible. Los prestadores pueden conservar copia (sin difusión) cuando lo exija una obligación legal
96	Testamento digital	Cuatro bloques de legitimados (a/b/c/d): a) familiares/de hecho + herederos · b) albacea testamentario o designado expresamente · c) (menores) representantes legales y MF · d) (personas con discapacidad) designados para apoyo. Excepción: prohibición expresa del fallecido o ley en contra; **subexcepción**: la prohibición no afecta a los herederos respecto de los contenidos que formen parte del **caudal relicto**. Apartado 2: decisión sobre mantenimiento o eliminación de perfiles en redes sociales (salvo instrucciones del fallecido). Apartado 4:

		en CC. AA. con derecho civil propio se aplica su normativa

RECUERDA

Tres regímenes de olvido distintos en el sistema español: (i) **olvido en buscadores** (art. 93 LOPDGDD): eliminación de enlaces tras búsqueda por nombre · (ii) **olvido en redes sociales** (art. 94 LOPDGDD): supresión de datos propios o de terceros · (iii) **derecho de supresión general** del art. 17 RGPD + art. 15 LOPDGDD (Ep. 3): supresión de datos del responsable del tratamiento. Cada uno con su régimen y condiciones específicas.

MATIZ

El olvido en buscadores no impide el acceso por otros criterios distintos del nombre (art. 93.2 LOPDGDD). Si el afectado consigue que Google elimine el enlace cuando se busca su nombre, la noticia sigue apareciendo si se busca por palabras clave del contenido. El derecho desindexa la búsqueda nominativa, no borra la información del sitio original.

MATIZ

El olvido en redes sociales tiene tres regímenes según el origen del dato (art. 94 LOPDGDD): (i) **datos propios** = supresión a **simple solicitud**, sin necesidad de motivo · (ii) **datos de terceros** = supresión solo si son inadecuados/inexactos/no pertinentes/no actualizados/excesivos · (iii) **datos facilitados durante minoría de edad** = supresión a **simple solicitud sin necesidad de motivo**, aunque hoy sea mayor de edad. La minoría de edad activa el régimen más fuerte.

MATIZ

Testamento digital del art. 96 ≠ datos de personas fallecidas del art. 3 LOPDGDD. El art. 3 (Título I) regula los **datos personales** de fallecidos en cualquier responsable del tratamiento. El art. 96 (Título X) regula los **contenidos digitales** gestionados por prestadores SSI (perfiles, fotos, mensajes…). El art. 96 incluye al **albacea testamentario** entre los legitimados, figura ausente en el art. 3. Y la subexcepción patrimonial del art. 96.1.a se refiere a contenidos del **caudal relicto**, no a «datos de carácter patrimonial» como en el art. 3.1.

MATIZ

Portabilidad en redes sociales (art. 95) tiene contornos distintos a la portabilidad general (art. 20 RGPD). La del art. 20 RGPD exige tratamiento basado en consentimiento o contrato + medios automatizados, y NO aplica al sector público; la del art. 95 LOPDGDD se predica de los usuarios de redes sociales sin esos requisitos del 20.1, condicionada solo a la viabilidad técnica.

4. Políticas de impulso de los derechos digitales — art. 97 LOPDGDD

Artículo 97 LOPDGDD · Políticas de impulso de los derechos digitales

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.
3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Plan / instrumento	Contenido
Plan de Acceso a Internet (97.1)	Tres objetivos a-c: a) **superar brechas digitales** + bono social · b) **espacios de conexión pública** · c) **formación en competencias digitales básicas** para colectivos en riesgo. Elaboración: Gobierno **en colaboración con las CC. AA.**
Plan de Actuación para menores (97.2)	Acciones de formación, difusión y concienciación para uso equilibrado de dispositivos y servicios SSI por menores
Informe anual al Congreso (97.3)	Presentación por el Gobierno ante la comisión parlamentaria correspondiente del Congreso, sobre la evolución de los derechos, garantías y mandatos del Título X

RECUERDA

Tres instrumentos del art. 97 LOPDGDD para impulsar los derechos digitales: **Plan de Acceso a Internet** (Gobierno + CC. AA., con tres objetivos a-c) · **Plan de Actuación para menores** (formación, difusión y concienciación) · **Informe anual al Congreso** sobre evolución de los derechos del Título X.

MATIZ

Plan de Acceso a Internet — tres objetivos (art. 97.1 LOPDGDD): a) bono social y superación de brechas · b) espacios de conexión pública · c) formación en competencias digitales. Conecta con las **brechas mencionadas en el art. 81** sobre acceso universal: género (81.3), generacional (81.4), rural (81.5) y necesidades especiales (81.6). El Plan es el instrumento operativo del derecho.

MATIZ

El informe del art. 97.3 es anual y se presenta al Congreso (no al Senado ni al Consejo de Ministros). La comisión parlamentaria competente es la que tenga atribuidas las materias de derechos digitales y protección de datos. Se dará cuenta de la evolución de los derechos, garantías y mandatos del Título X y de las medidas necesarias para promover su impulso y efectividad.

TRES FORMAS DE EMPEZAR

La app Persevera complementa este temario con las herramientas para estudiarlo:

tests · flashcards con repaso espaciado · supuestos

simulacros · mindmaps · tutor IA · planificador

Suscripción mensual sin permanencia. Cancelas cuando quieras desde la app.

WEB

perseveraoposiciones.com

IOS

iPhone / iPad

ANDROID

Google Play