OBJETO Y ÁMBITO DE APLICACIÓN DEL RGPD Y LA LOPDPGDD

	OBJETO	ÁMBITO DE APLICACIÓN
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 –> RGPD	1.- Protección de los DATOS PERSONALES DE PERSONAS **FÍSICAS (independientemente de su nacionalidad o de su lugar de residencia)** --> se entiende por dato personal cualquier información concerniente a personas físicas i**dentificadas o identificables**. Excepción donde el RGPD NO es de aplicación --> "excepción doméstica". 2.- LIBRE CIRCULACIÓN DE DATOS POR LA U--> que no podrá ser restringida ni prohibida por motivos relacionados con la protección de datos personales las personas físicas (esto es, se le da prioridad a la libre circulación de datos, pero con unos niveles óptimos de protección respecto a los datos personales Se pretende eliminar las diferencias en el tratamiento de protección de datos personales entre EM que puedan restringirla).	**1.- Ámbito de aplicación material.** A.- El tratamiento total o parcialmente automatizado de datos personales. B.- El tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. *El RGPD NO se aplica al tratamiento de datos personales en lo relativo a:* *1.- Actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión;* *2.- Actividades relativas a la política exterior y de seguridad común.* *3.- Actividades realizadas por una persona física en el ejercicio de act exclusivmente personales o domésticas;* *4.- Actividades de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales.* **2.- Ámbito de aplicación territorial.** A.- Actividades en donde el responsable o encargado es de la Unión, independientemente de que el tratamiento de los datos personales tenga lugar en la Unión o no. B.- Actividades en donde el responsable o encargado NO es de la Unión, pero tratan datos personales de interesados que SÍ residen en la Unión y que están relacionadas con: a) la oferta de Bs o Ss a dichos interesados en la Unión, independientemente de si a estos se les requiere un pago b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. C.- Actividades en donde el responsable o encargado NO es de la Unión, pero está establecido en un lugar en que el Derecho de los EM sea de aplicación en virtud del Derecho internacional público.
Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales --> LOPDPGG	a) Adaptar el ordenamiento jurídico español al RGPD y completar sus disposiciones. b) Garantizar los derechos digitales de la ciudadanía conforme el art 18.4 CE: *"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* " *Aunque el objeto de la LOPDPGDD eran a), durante su tramitación parlamentaria, se añadió también como objeto garantizar los derechos digitales de los ciudadanos.	Los Títulos I a IX y los art 89 a 94* se aplican a --> ÁMBITO DE APLICACIÓN MATERIAL DEL RGPD. La LOPDPGDD NO se aplica a: --> los tratamientos excluidos en el RGPD (1-4), con los siguientes matices: *a.- Los tratamientos de datos de actividades no comprendidas en el ámbito de aplicación del Derecho de la U (ej.:LO régimen electoral general, instituciones penitenciarias, Registro Civil, Registros de la Propiedad y Mercantiles...), se regirán por su legislación específica si la hubiere y supletoriamente por el RGPD y en la LOPDPGDD.* *b.- El tratamiento de datos en la tramitación de los órganos judiciales y la Oficina Judicial, se regirán por lo dispuesto en el RGPD y en la LOPDPGDD, sin perjuicio de las disposiciones de la LOPJ, que le sean aplicables .* --> Los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido sobre el tratamiento de datos de personas fallecidas (art 3). --> Los tratamientos sometidos a la normativa sobre protección de materias clasificadas. **Se excluyen art 79-88 (derechos de la era digital, neutralidad en Internet, acceso universal en Internet, seguridad digital, educación digital, protección de menores en Internet, derecho de rectificación en Internet, derecho a la actualización de informaciones en medios de comunicación digitales, derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral y derecho a la desconexión) y 95-97(derecho de portabilidad en servicios de redes sociales y equivalentes, derecho al testamento digital y políticas de impulso de los derechos digitales) .*

DEFINICIONES LOPD

DATOS PERSONALES

DEFINICION

Toda información sobre una persona **física identificada o identificable** (es decir, que permita, directa o indirectamente, a través de un indentificador, determinar la identidad física, fisiológica, genética, psíquica, económica, cultural o social de una persona física -un apodo, una foto, un email, un dato sobre tu salud, etc.-).

CARAC.

Deben ser tratados de manera **lícita, leal y transparente** («licitud, lealtad y transparencia»);

Para su tratamiento el interesado debe dar el **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos.

El tratamiento es necesario para:

(solo habrá que informar)

- La **ejecución de un contrato o de medidas contractuales** en el que el interesado es parte (CONTRATO DE COMPRAVENTA)
- El cumplimiento de una **obligación legal exigible al responsable** del tratamiento (ej.: adopción de medidas adicionales de seguridad)
- El cumplimiento de una **misión realizada en interés público** o en el ejercicio de **poderes públicos conferidos al responsable** del tratamiento, ambos casos establecidos por una **norma con rango de ley** *(ej.: procedimiento disciplinario).*
- Proteger **intereses vitales** del interesado o de otra persona física.
- La satisfacción de **intereses legítimos** perseguidos por el **responsable del tratamiento o por un tercero**, siempre que sobre dichos intereses no prevalezcan los intereses, derechos y libertades fundamentales del interesado, en particular si es un niño.

Son recogidos con **fines determinados, explícitos y legítimos**, y no serán tratados ulteriormente de manera incompatible con dichos fines.
El tratamiento ulterior de los datos con fines de archivo en interés público, de investigación científica e histórica o estadísticos será COMPATIBLE («**limitación de la finalidad**»).
**La expresión "sus datos personales se tratarán para mejorar su experiencia como usuario", supone un incumplimiento del principio de limitación , ya que es una fórmula genérica.*

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

Deben ser **exactos y, si fuera necesario, actualizados:** se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos inexactos respecto a los fines de que se tratan.

Deben **mantenerse 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 con fines de archivo en interés público, de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas a fin de proteger los derechos y libertades del interesado («**limitación del plazo de conservación**»).

Deben ser tratados de tal manera que se garantice una **seguridad adecuada** de los datos personales, s**u integridad y confidencialidad**, 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 --> *Ojo! contra su simulación NO.*
Las obligaciones de **confidencialidad y de **secreto profesional** se mantendrán aun finalizada la relación del obligado con el responsable o encargado (no establece años).*

*El **responsable del tratamiento** será responsable del cumplimiento de lo indicado y capaz de demostrarlo («**responsabilidad proactiva**»).

TRATAMIENTO

Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no *(recogida, registro, organización,estructuración, conservación, modificación, extracción, consulta, utilización, acceso, difusión, limitación, supresión, etc.).*

SEUDONIMIZACIÓN

Tratamiento de los 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 (ej.: cambiar el nº del DNI por un código alfanumérico).

FICHERO

Conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

CONSENTIMIENTO

DEFINICION

Toda **manifestación de voluntad libre, específica, informada e inequívoca** por la que este acepta, ya sea mediante una **declaración o una clara acción afirmativ**a, el tratamiento de datos personales que le conciernen.
Ojo! el consentimiento no es la única base jurídica que legitima el tratamiento de datos, es una más. Por ej., cuando el responsable sea una autoridad pública, el tratamiento debe basarse en fundamentos jurídicos.

CARAC.

1.- Ha de ser l**ibre, específico, informado e inequívoco,** ya sea mediante una declaración o una clara acción afirmativa.
2.- Deberá de ser **explícito** si se refiere a categorías especiales de datos, a decisiones individuales automatizadas o a la posibilidad de realizar transferencias internacionales. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
3.- 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. La solicitud de consentimiento se presentará de tal forma que se distingan claramente todos los asuntos.
4.- El tratamiento de los datos personales de un **menor de edad** únicamente podrá fundarse en su consentimiento cuando sea **mayor de catorce años,** salvo que una ley detemine lo contrario (si es menor, deberá constar el consentimiento de los titulares de la patria potestad o tutela) --> *¡Ojo! de conformidad con el Reglamento (UE) 2016/679), el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Los EM podrán establecer por ley una edad inferior* ***no inferior a 13 años.***

RETIRADA

1.- El interesado tendrá derecho a retirar su consentimiento **en cualquier momento**.
2.- Será tan fácil retirar el consentimiento como darlo.
3.- La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.

INFORMACIÓN	**Órgano competente**	La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el **responsable del tratamiento.** Es el responsable el que tomará las medidas para facilitar al interesado toda la información, tanto la básica como adicional, de forma **concisa, transparente, inteligible y de fácil acceso,** con un lenguaje **claro y sencillo**, y en particular cualquier información dirigida específicamente a un niño, además de facilitarle el ejercicio de sus derechos. El responsable **deberá poder acreditar con posterioridad** que la obligación de informar ha sido satisfecha.		
	Tipos de información	**1.- Información básica (**1º nivel): *a) La identidad y los datos de contacto del responsable del tratamiento y de su representante, en su caso.* *b) Los datos de contacto del delegado de protección de datos, en su caso.* *c) La finalidad del tratamiento y su base jurídica.* *d) Cuando el tratamiento se base en la satisfacción de intereses legítimos del responsable del tratamiento o de un tercero, los intereses legítimos.* *e) Los destinatarios o categoría de destinatarios, en su caso (en su caso, la intenciónde transferir los datos a un 3º país u organización internacional).* 2.- **Información adicional** (2º nivel): donde se presenta **de forma detallada completa** el resto de la información, en un medio más adecuado.		
	Información por capas	Cuando los datos personales sean obtenidos del afectado, el responsable del tratamiento podrá dar cumplimiento al deber de información a través de la infromación por capas, facilitándole, en el momento y en el mismo medio en el que se recojan los datos, solo la información básica y una dirección electrónica u otro medio (ej.: un enlace directo) que le permita acceder de forma sencilla e inmediata a la restante información (información adicional).		
	Cuando es necesario informar	1.- **Si los datos se obtienen directamente del interesado**: la información se debe poner a su disposición en el momento en que se soliciten los datos, **previamente a la recogida o registro.** 2.- **Si los datos NO se obtienen directamente del interesado** (vía cesión legítima o fuentes de acceso público): la información se debe poner a disposición del interesado **dentro de un plazo razonable,** pero siempre: ✓ *Antes de un mes desde que se obtuvieron los datos personales,* ✓ *Antes o en la primera comunicación con el interesado,* ✓ *Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios*		
	Cuando NO es necesario informar	1.- Cuando el interesado ya disponga de la información. 2.- En el caso de que los datos no procedan del interesado, cuando: ✓ *La comunicación resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.* ✓ *El registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros,* ✓ *Cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto (secreto profesional).*		
DATOS ESPECIALES	**DATOS SENSIBLES**	**Tipos:**	a) Datos personales que revelen **origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas y afiliación sindical.** b) Datos **genéticos** (que proporcionen una información única sobre la fisiología o la salud de esa persona). c) Datos **biométricos** dirigidos a identificar de manera unívoca a una persona física (¡ojo! jurídica NO). Son datos relativos a las características físicas, fisiológicas o conductuales de una persona física que permiten su identificación única (ej.:imágenes faciales o datos dactiloscópicos). d) Datos relativos a la **salud** (física o mental). e) Datos relativos a la **vida sexual o la orientación sexual** de una persona física.	
		Exención de la prohibición de su tratamiento:	a) El interesado dio su **consentimiento explícito**, excepto si el Derecho UE o de los EM establece que la prohibición no puede levantarse. b) El tratamiento es necesario para el **cumplimiento de obligaciones y el ejercicio de derechos específicos** del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social. c) El tratamiento es necesario para **proteger intereses vitales** del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento. d) El tratamiento es efectuado, en el ámbito de sus **actividades legítimas de determinados organismos** (con finalidades políticas, filosóficas, religiosas o sindicales), siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos y siempre que los datos no se comuniquen fuera de ellos sin el consentimiento de los interesados. e) El tratamiento se refiere a datos personales que el interesado ha hecho **manifiestamente públicos.** f) El tratamiento es necesario para la formulación de **reclamaciones** o cuando los **tribunales** ejerzan su función judicial. g) El tratamiento es necesario por razones de un i**nterés público esencial, según norma con rango de ley**, que debe ser proporcional. h) El tratamiento es necesario para fines de **medicina preventiva o laboral** (evaluación de la capacidad laboral del trabajador, diagnósticos médicos, asistencia sanitaria y social, etc)**, según norma con rango de ley.** i) El tratamiento es necesario por razones de **interés público en el ámbito de la salud pública,** como la protección frente a amenazas transfronterizas graves para la salud, garantizar seguridad de la asistencia sanitaria, etc, **según norma con rango de ley.** j) El tratamiento es necesario con fines de **archivo en interés público, fines de investigación científica o histórica o fines estadísticos**, que debe ser proporcional al objetivo perseguido y establecer medidas específicas para proteger los intereses y derechos del interesado.

<table>
<tr><td rowspan="8">DATOS ESPECIALES</td><td>DATOS RELATIVOS A CONDENAS E INFRACCIONES PENALES</td><td colspan="2">Su tratamiento, para fines distintos de los de prevención, investigación, detección o enjuiciamiento, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de laUE, una ley o cuando sea llevado a cabo por abogados y procuradores para recoger información facilitada por sus clientes.</td></tr>
<tr><td>DATOS RELATIVOS A INFRACCIONES Y SANCIONES ADMINISTRATIVAS</td><td colspan="2">a) Que los responsables de dichos tratamientos sean los órganos competentes dentro del procedimiento sancionador.
b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.
c) Que se cuente con el consentimiento del interesado.
d) Que se autorice por una norma con rango de ley.
e) Sea llevado a cabo por abogados y procuradores para recoger información facilitada por sus clientes.</td></tr>
<tr><td rowspan="2">VIDEOVIGILANCIA</td><td colspan="2">Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes vía cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones (incluyendo infraestructuras vinculadas al transporte), siempre que:
✓Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para preservar la seguridad.
✓En ningún caso podrán captarse imágenes del interior de un domicilio privado.
✓No se aplica la <u>obligación de bloqueo</u> (el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión).
✓Los datos serán suprimidos en el plazo 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 72h desde que se tuviera conocimiento de la existencia de la grabación.
✓El deber de información 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.</td></tr>
<tr><td>Derecho intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en lugar de trabajo:</td><td>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, siempre que se ejerzan dentro de su marco legal y resulten relevantes l para la seguridad de las instalaciones, bienes y personas, respetando el principio de proporcionalidad, de intervención mínima y las garantías previstas en los apartados anteriores.
2.- Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, acerca de esta medida.
3.- En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento, tales como vestuarios, aseos, comedores y análogos</td></tr>
<tr><td>DATOS DE COMUNICACIONES COMERCIALES</td><td colspan="2">Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición.
Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá <u>informarle de los sistemas de exclusión publicitaria existentes</u>, pudiendo remitirse a la información publicada por la autoridad de control competente.</td></tr>
<tr><td>DATOS SOBRE PROTECCIÓN PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS:</td><td colspan="2">Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.</td></tr>
<tr><td>DATOS PARA LA FUNCIÓN ESTADÍSTICA</td><td colspan="2">El tratamiento de datos personales relacionado con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, el RGPD y la LOPDPGDD.
Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio de los derechos establecidos en los art. 15-22 del RGPD (acceso,rectificación, etc.) cuando los datos se encuentren amparados por las garantías del secreto estadístico.</td></tr>
<tr><td>DATOS DE PERSONAS FALLECIDAS</td><td colspan="2">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 (ej: gestión del perfil en las redes sociales), salvo 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 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 RD se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos.
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.
4.- 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.</td></tr>
</table>

DERECHOS RECOGIDOS EN EL RGPD

CARACTERÍSTICAS

1.- Podrán ejercerse directamente o por medio de representante *(ej los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años dichos derechos).*

2.- El **responsable** del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer dichos derechos, que deberán ser fácilmente accesibles.

**La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de los derechos del afectado recaerá sobre el responsable.*

3.- El **encargado** podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere.

3.- Se podrán limitar (siempre de forma proporcionada) para salvaguardar:

a) la seguridad del Estado, la seguridad pública y la defensa.

b) la prevención o enjuiciamiento de infracciones penales y la ejecución de sus sanciones, de normas deontológicas, demandas civiles y la protección de la independencia judicial.

c) otros objetivos importantes de interés público general: intereses económicos o financieros, la sanidad pública y la seguridad social;

d) una función de supervisión, inspección o reglamentación;

e) la protección del interesado o de los derechos y libertades de otros;

4.- Serán **gratuitos** (salvo lo previsto para solicitudes infundadas o excesivas).

TIPOS

Derecho de ACCESO

El interesado tendrá derecho a obtener del **responsable** confirmación de si se están tratando o no sus datos y, en tal caso, tendrá derecho al acceso a los mismos, a concocer el fin del tratamiento y a la trazabilidad (es decir, a saber los destinatarios de estos datos (en particular terceros u organizaciones internacionales. ¡Ojo! pero NO QUIEN ACCEDE A SUS DATOS)). Igualmente, tendrá derecho a conocer, de ser posible, el plazo de conservación de esos datos, el ejercicio del derecho de rectficación, supresión, de decisiones inidividuales automatizadas, etc..., de reclamar y de cualquier otra información.

Forma de acceso: si la solicitud se presenta por medios electrónicos, y a menos que se solicite que se facilite de otro modo, el responsable facilitará una copia de los datos en un formato electrónico de uso común. El acceso se entenderá otorgado si el responsable facilitara al afectado un **sistema de acceso remoto, directo y seguro** a sus datos que garantice, de modo permanente, el acceso a su totalidad.

Si así se solicita, la **información podrá facilitarse verbalmente** siempre que se demuestre la identidad del interesado.

Cuando el responsable trate una gran cantidad de datos del afectado y este no especifique a qué datos se refiere, el responsable podrá solicitarle que lo especifique.

Plazo: 1m desde la recepción de la solicitud, prorrogable por 2m más según la complejidad y el nº de solicitudes (el responsable informará de dichas prórrogas y los motivos).

Si el responsable no da curso a la solicitud , le informará **sin dilación y a más tardar en un mes,** de las razones y la posibilidad de presentar una reclamación o ejercitar acciones judiciales.

Solicitudes infundadas y excesivas --> la información facilitada será gratuita salvo:

*1) Cuando las solicitudes sean **manifiestamente infundadas o excesivas,** especialmente debido a su **carácter repetitivo** (ej.: solicitar el derecho de acceso más de una vez en 6m), el responsable podrá negarse a actuar o cobrar un canon razonable en función de los costes administrativos afrontados. El responsable soportará la carga de demostrar el carácter manifiestamente fundado o excesivo.*

*2) 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.***

*3) El responsable podrá percibir por cualquier otra **copia solicitada** por el interesado un **canon razonable.***

Derecho de RECTIFICACIÓN

A.- Datos inexactos (datos erroneos, cambio de domicilio, etc, previa documentación justificativa, en su caso): cuando se solicite la rectificación, el responsable deberá cursarla **sin dilación indebida**.

B.- Datos adicionales: según los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales incompletos, inclusive vía declaración adicional.

Derecho de SUPRESIÓN (derecho al olvido)

Se tendrá derecho a obtener **sin dilación indebida** del responsable la supresión de los datos (y que su rastro quedé borrado), cuando:

a) los datos personales **ya no sean necesarios** en relación con los fines para los que fueron recogidos;
b) el interesado **retire el consentimiento** y este no se base en otro fundamento jurídico;
c) el interesado **se oponga al tratamiento** y no prevalezcan otros motivos legítimos para el tratamiento;
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 UE o de los EMs;
f) los datos personales se hayan obtenido en relación con la **oferta de servicios de la sociedad de la información** (esto es, a cambio de una remuneración).

Este derecho no se aplicará cuando el tratamiento sea necesario para:

a) ejercer el derecho a la **libertad de expresión e información;**
b) cumplir una **obligación legal** de derecho de la UE o de los EMs, una misión de interés público o determinados poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la **salud pública;**
d) con fines de **archivo** en interés público, fines de **investigación científica o histórica** o fines **estadísticos;**
e) la formulación, el ejercicio o la defensa de **reclamaciones.**

Cuando haya hecho públicos los datos personales y esté obligado a suprimirlos, el responsable, teniendo en cuenta la tecnología disponible y el coste, adoptará las medidas razonables posibles para informar a los otros responsables que estén tratando los datos objeto de supresión (y que actuen en el mismo sentido).

Cuando la supresión derive ddel derecho de oposición, el responsable podrá conservar los datos del afectado necesarios para impedir tratamientos futuros con fines de mercadotecnia directa.

** ¡Ojo! es el derecho a no aparecer no a que se borren los datos de esa base de datos.*

** **Obligación del BLOQUEO:** el responsable estará obligado a bloquear los datos cuando proceda a su **rectificación o supresión.** Para ello, los identificará y reservará, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para su puesta a disposición a jueces y tribunales, M. Fiscal o APs (AEPD) hasta el fin de plazo de prescripción (transcurrido el cual deberán destruirse).*

*La AEPD y las autoridades autonómicas de protección de datos, podrán fijar **excepciones** a la obligación de bloqueo,s en caso de que existiesen determinados riesgos o cuando su conservación bloqueados supusiese un coste desproporcionado para el responsable.*

TIPOS			
	Derecho de LIMITACIÓN	Se tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando:	a) se impugne por el interesado su **inexactitud**, 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 los necesite, pero el interesado sí, para la formulación, el ejercicio o la defensa de **reclamaciones;** d) el interesado se haya **opuesto al tratamiento,** mientras se verifica si los **motivos legítimos** del responsable **prevalecen** sobre los del interesado.
		Cuando el tratamiento de los datos se haya limitado, dichos datos solo podrán ser objeto de tratamiento:	a) si existe consentimiento del interesado; b) para formular o defender reclamaciones; c) para proteger derechos de otras personas físicas o jurídicas; d) por razones de interés público importante para la UE o para un EM.
		el hecho de que el tratamiento de los datos esté limitado **debe constar claramente en los sistemas de información** del responsable. Todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación. El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento **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.	
	Derecho de OPOSICIÓN	El interesado tendrá derecho a oponerse en cualquier momento, por motivos particulares, a que sus datos sean objeto de tratamiento, incluida la elaboración de perfiles, salvo que: 1.- El responsable acredite motivos legítimos imperiosos que prevalezcan, derechos y libertades del interesado o para la defensa de reclamaciones (en lo relativo a la mercadotecnia directa, el responsable no podrá acreditar motivo alguno). 2.- Los datos personales se traten con fines de **investigación científica o histórica o fines estadísticos,y exista una misión de interés público.** **Por ej., yo compro un coche pero una vez que ya este comprado quiero que borres los datos.*	
	Derecho de PORTABILIDAD	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 (ej.: compañías de teléfonos), cuando: *a) el tratamiento esté basado en un consentimiento por parte del interesado.* *b) el tratamiento se efectúe por medios automatizados.* Al ejercer la portabilidad, el interesado tendrá derecho a que los datos se transmitan directamente de responsable a responsable cuando sea técnicamente posible.	
	Derecho de DECISIONES INDIVIDUALES AUTOMATIZADAS (incluida la elaboración de perfiles)	El 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. **Se entiende por «elaboración de perfiles» toda forma de tratamiento automatizado de datos personales para evaluar determinados aspectos de una persona física (rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etc). Si alguien conoce tus gustos, como en google o amazon, te puede crear un perfil psicológico o comercial y a través del mismo, te puede mandar spam relacionado para que compres, etc…* Este derecho 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 UE o de los EM, o c) se basa en el consentimiento explícito del interesado. "d)"**Los profesionales inciden en que es contraria a este derecho la DA de la LOPDPGDD, por la que se incluye el art. 58 bis a la Ley Orgánica de Libertad Sindical:* *"La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas (es decir no se puede ejercer este derecho en estos casos)".*	

El derecho de cancelación YA no existe, como tal.

Derechos digitales de los usuarios

Carac	1.- Regulados únicamente en la LOPDPGDD. 2.- Los derechos y libertades consagrados en la CE y TI son plenamente aplicables en Internet. 3.- Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.	
Tipos	**Derecho a la neutralidad de Internet.**	La **neutralidad de red** es el principio por el cual los proveedores de servicios de Internet deben tratar todo tráfico de datos que transita por la red de igual forma, sin discriminación por motivos técnicos o económicos, sin cobrar una tarifa dependiendo del contenido (esto es, todos los datos serán tratados de la misma forma independientemente de su contenido, sin poder dar prioridad a paquetes de datos de pago).
	Derecho de acceso universal a Internet.	Se garantizará un **acceso universal, asequible, de calidad y no discriminatorio** para toda la población, teniendo en consideración los entornos rurales (superación brecha territorial) y las personas con necesidades especiales (superación **brecha de género y brecha generacional**).
	Derecho a la seguridad digital.	**Doble protección:** art. 18.3 CE "secreto de las comunicaciones" + LOPDPGDD recalcando el derecho a la seguridad de las comunicaciones a través de Internet.
	Derecho a la educación digital.	1.- El sistema educativo garantizará la plena **inserción del alumnado en la sociedad digital** y el aprendizaje del uso de los medios digitales de un modo seguro y respetuoso, garantizando intimidad personal y familiar y la protección de datos personales. Ejemplos: A.- *Se deberán incluir asignaturas de* ***libre configuración*** *relacionadas con la competencia digital, con especial atención a la* ***violencia en la red.*** *B.- El* ***profesorado*** *recibirá las competencias digitales y la* ***formación necesaria.*** *C.- Los* ***planes de estudio*** *de los títulos universitarios, en especial, los de profesorado,* ***garantizarán la form*** *ación en medios digitales.* *D.- Las APs 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.* 2.- Las actuaciones realizadas tendrán carácter **inclusivo,** en particular en lo que respecta al **alumnado con necesidades educativas especiales.** 3.- El Gobierno, en colaboración con las CCAA, 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 mediante, entre otras medidas, un bono social de acceso a Internet;* *b) impulsar los espacios de conexión de acceso público; y* *c) fomentar medidas educativas que promuevan la formación en competencias digitales básicas a personas y colectivos en riesgo de exclusión digital.* 4.- Asimismo se aprobará un **Plan de Actuación** dirigido a promover la formación, difusión y concienciación necesarias para que los menores hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales.
	Protección de los menores en Internet.	1.- Los **padres, madres, tutores, curadores o representantes** legales procurarán que los menores hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información, con el fin de garantizar una decuado desarrollo de su personalidad y preservar 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 precisas.
	Protección de datos de los menores.	1.- Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades con menores garantizarán la protección de sus derechos. 2.- Cuando la publicación o difusión de su imagen fuera a tener lugar a través de redes sociales o deberán contar con el consentimiento del menor o con el de sus representantes.
	Derecho de rectificación en Internet.	1.- Todos tienen derecho a la **libertad de expresión** en Internet. 2.- Los **responsables** de redes sociales adoptarán protocolos adecuados para posibilitar el ejercicio del d**erecho 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 *(se recoge también, por tanto, la libertad de expresión en Internet, prohibiendo que se niegue el servicio o se bloquee la participación de los usuarios por sus opiniones).* 3.- Cuando los medios de comunicación digitales deban atender una solicitud de rectificación deberán publicar en sus archivos digitales de un aviso aclaratorio visible que ponga de manifiesto **"la noticia original no refleja la situación actual del individuo".**
	Derecho a la actualización de info. en medios comunicación.	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, causaçandole un perjuicio *(ej.: cuando se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado).* *Ej.: "solicto que se proceda a la efectiva actualización de los datos inexactos relativos a mi persona que se encuentren en medios de comunicación digitales...".*

Tipos	**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. 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** (ej: correo electrónico) requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores.
	Derecho a la desconexión digital en el ámbito laboral.	1.- Los trabajadores y empleados públicos tendrán **derecho a la desconexión digital** a fin de garantizar, fuera del tiempo de trabajo su tiempo de descanso, permisos, vacaciones e intimidad. En particular, se preservará este derecho en los supuestos de realización total o parcial del **trabajo a distancia** así como en el domicilio del empleado. 2.- Las modalidades de ejercicio de este derecho atenderán a la naturaleza de la relación laboral, potenciarán el derecho a la conciliación y se sujetarán a negociación colectiva . 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 sensibilización para evitar el riesgo de fatiga informática.
	Derecho a la intimidad	**a) Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (visto).** **b) Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral --> l**os 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, siempre dentro del marco legal. Con carácter previo, los empleadores habrán de informar de forma **expresa, clara e inequívoca** a los trabajadores o empleados públicos y, en su caso, a sus representantes, sobre la existencia y características de estos dispositivos asi como del posible ejercicio de los derechos de acceso, rectificación, limitación y supresión.
	Derechos digitales en negociación colectiva	Los convenios colectivos podrán establecer garantías adicionales de estos os derechos y libertades.
	Derecho al olvido.	**a) Derecho al olvido en búsquedas de Internet -->** 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: *1.- Cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos .* *2.- Cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos.* *El ejercicio de este derecho al qno impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda. **b) Derecho al olvido en servicios de redes sociales y servicios equivalentes --> t**oda persona tiene derecho a que sean suprimidos, con su simple solicitud: *1.- Los datos personales que hubiese facilitado para su publicación por servicios de redes sociales .* *2.- Los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos (esto es, si yo compro una lavadora, no me pueden exigir datos tipo salud, hobbies, peso, etc).* Se exceptúan los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.
	Derecho de portabilidad en redes sociales	Los usuarios de servicios de redes sociales tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado, así como a que los prestadores los transmitan directamente a otro prestador, **siempre que sea técnicamente posible.** Los prestadores podrán conservar, sin difundirla, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.
	Derecho al testamento digital.	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, así como sus herederos (o M Fiscal en caso de menores o personas con discapacidad) podrán dirigirse a los prestadores para acceder a los contenidos y solicitar su modificación o eliminación (ej: redes sociales), salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.* *b) El albacea testamentario (albacea digital o testamento digital) también podrá solicitar el acceso a los contenidos.* Mediante RD se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones.

PERSONAS CLAVE en la PROTECCIÓN DE DATOS

	DEFINICIÓN	Medidas para demostrar que cumplen con sus obligaciones	OBLIGACIONES
RESPONSABLE DEL TRATAMIENTO	Persona **física o jurídica, autoridad pública, servicio u otro organismo** que determina los **fines y medios** del tratamiento de los datos (si se van a conservar, ceder, eliminar...). Tendra consideración de responsable: *--> Quien **en su propio nombre** y sin que conste que actúa por cuenta de otro, **establezca relaciones con los afectados.*** *---> Quien figurando como encargado utilizase los datos para sus **propias finalidades .*** ***CORRESPONSABILIDAD**: Cuando dos o más responsables determinen conjuntamente los objetivos y los medios serán considerados corresponsables.	**a.- Códigos de Conducta (en función de los sectores y las necesidades específicas de las PYMES):** Promoción: los EM, las autoridades de control y los organismos que asuman la supervisión y resolución extrajudicial de conflictos, el Comité, la Comisión, las asociaciones, las empresas o grupos de empresas y los responsables o encargados del tratamiento. Aprobación: En España, por la AEPD o por la autoridad autonómica de protección. Adhesión: en todo caso, los responsables o encargados a los que se les aplica el RGPD. No obstante, si NO se les aplica, podrán adherirse también. Características: en cualquier caso (obligatorios o no), los códigos de conducta serán vinculantes para quienes se adhieran a los mismos. Además, podrán dotarse de mecanismos de resolución extrajudicial de conflictos. Supervisión: sin perjuicio de la autoridad de control, también podrá supervisar un organismo con un nivel adecuado de pericia, que así haya sido acreditado por la autoridad de control. Registro: la AEPD y las autoridades autonómicas de protección mantendrán registros de los códigos de conducta (su contenido se establece por RD). Dichos registros estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos. **b.- Los Mecanismo de Certificación en materia de protección de datos -sellos y marcas-:** a fin de demostrar el cumplimiento del RGPD. En el caso de España, la acreditación podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC).	A.- Los responsables (y encargados) determinarán las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento es conforme con la normativa. En particular, se valorará si procede: ***1.- La evaluación de impacto** : cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas, el responsable realizará, antes del tratamiento, una evaluación del impacto a la protección de datos que **deberá incluir las medidas previstas para afrontar los riesgos.*** *El responsable recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto.* *La autoridad de control publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto y también , podrá publicar la lista de los que no la requieren.* ***2.- Una consulta previa:** el responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto muestre que el tratamiento entraña un alto riesgo si no se toman medidas.*
ENCARGADO DEL TRATAMIENTO	1.- Persona física o jurídica, o autoridad pública (determinado órgano de una AP), que **trata datos** personales **por cuenta del responsable.** Suele ser un tercero externo. 2.- Cuando se vaya a realizar un tratamiento, el responsable elegirá únicamente a un encargado, con el que formalizá un contrato o acto jurídico (encomiendas, convenios, RD de estructura etc) que establezca el objeto, duración, naturaleza y finalidad del tratamiento. **El acceso del encargado a los datos no es comunicación de datos.* 3.- Su objeto es garantizar un nivel de seguridad adecuado, que incluya: --> la seudonimización y cifrado de datos. --> la capacidad para garantizar: *- la confidencialidad --> garantizará también que las personas autorizadas para tratar datos respeten la confidencialidad.* *- la integridad.* *- la disponibilidad.* *- la resiliencia a los cambios.* *- la evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.* **4.- El encargado puede recurrir a otro encargado:** SIEMPRE con autorización previa por escrito, específica o general, del responsable y formalizandose con este, igualmente un contrato o acto jurídico. **Si ese otro encargado incumple sus obligaciones, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento.*	1.- Tratará los datos únicamente siguiendo las **instrucciones** del responsable, salvo que este obligado a ello (además de asistirle y ayudarle). 2.- Podrá adherirse a un **código de conducta o a un mecanismo de certificación** como elemento para demostrar la garantía del cumplimiento de dichos requisitos. **Si un encargado infringiera el RGPD, será considerado responsable con respecto a dicho tratamiento.* 3.- Seguridad: en caso de violación de la seguridad (por destrucción, pérdida o alteración accidental o ilícita o la comunicación o acceso no autorizados), el encargado lo notificará **sin dilación indebida** al responsable y será dicho responsable el que lo notificará a la autoridad de control sin dilación indebida y, de ser posible, a no más tardar de **72 horas** después de que haya tenido constancia, **a menos que sea improbable que dicha violación de la seguridad constituya un riesgo p**ara los derechos y las libertades de las personas físicas. Si la notificación no tiene lugar en 72 h, deberá ir acompañada de indicación de los motivos de la dilación. Igualxjmete, cuando sea probable que la violación de la seguridad de los datos entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable lo comunicará al interesado **sin dilación indebida** con un lenguaje claro y sencillo, salvo excepciones (ej: el responsable ha tomado medidas ulteriores que garanticen que ya no exista el alto riesgo o si supone un esfuerzo desproporcionado). 4- A la finalización del servicio: a elección del responsable, suprimirá o devolverá (al responsable o a un nuevo encargado) todos los datos y suprimirá todas las copias salvo que se requiera su conservación en virtud del Derecho de la U o de los EM. **Podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades del responsable.*	

DELEGADO DE PROTECCIÓN DE DATOS (DPD)

DEFINICIÓN y CARACTERÍSTICAS	OBLIGACIONES
1.- Figura creada por el RGPD, como una persona física o jurídica con **conocimientos especializados** de la normativa (certificados o no) y, en particular, con **conocimientos especializados del Derecho**. Dichos requisitos podrán demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación (ej.: poseer una titulación universitaria específica). 2.- El DPD podrá ser **interno,** formando parte de la plantilla o **externo**, vinculado a través de un contrato de servicios, pero, en todo caso, deberá estar en condiciones de desempeñar sus funciones de manera **independiente.** Cuando se trate de una persona física integrada en la organización, no podrá ser removido ni sancionado o por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. 3.- La dedicación del DPD podrá ser **completa o a tiempo parcial, e**n función del volumen de los tratamientos, la categoría especial de los datos o de los riesgos para los derechos o libertades de los interesados. 4.- Según el RGPD, el DPD **solo es obligatorio en 3 supuestos:** *a) el tratamiento lo lleve a cabo una* ***autoridad pública u OOPP,*** *excepto los tribunales en su función judicial. En estos casos, SI se podrá designar un único DPD para varias autoridades u OOPP.* *b) las actividades principales del responsable o del encargado consistan en tratamientos que requieran una o* ***bservación habitual y sistemática de interesados a gran escala, o*** *c) las actividades principales consistan en el* ***tratamiento a gran escala de categorías especiales de datos*** *personales y de datos relativos a* ***condenas e infracciones penales.*** No obstante, la LOPDPGDD añade estas obligatoriedades: *a) Los* ***colegios profesionales*** *y sus consejos generales.* *b) Los* ***centros docentes*** *a cualquier nivel, públicos y privados.* *c) La* ***redes de comunicaciones, energía y gas natural.*** *d)* ***Sociedades de la información*** *si elaboran a gran escala perfiles.* *e) La* ***s entidades crédito, financieras, de inversión, aseguradoras*** *y reaseguradoras, etc.* *f) Actividades de* ***publicidad y comerciales, si elaboran perfiles.*** *g) Los* ***centros sanitarios*** *obligados al mantenimiento de las historias clínicas. Se exceptúan los profesionales que ejerzan su actividad a título individual.* *i) Los operadores que desarrollen la* ***actividad de juego.*** *j) Las empresas de* ***seguridad privada.*** *k) Las* ***federaciones deportivas en el caso de tratar datos de menores*** . 5.- Respecto al DPD, el responsable o el encargado del tratamiento: *a.- Publicarán sus datos de contacto y los comunicarán a la autoridad de control (en el caso de España, el pazo para comunicar a la AEPD o autoridadaes autonómicas, tanto los datos del DPD, como ceses u otras modificaciones, será de 10 días, tanto si el cargo es obligatorio como si es voluntario).* *b.- Garantizarán que participe en todas las cuestiones sobre protección de datos.* *c.- Le respaldarán en el desempeño de sus funciones, facilitando los recursos necesarios.* 6.- Respecto al DPD, la AEPD y las autoridades autonómicas mantendrán, dentro de sus ámbitos, una lista actualizada de los DPD que será accesible por medios electrónicos.	a) Informar y asesorar al responsable, al encargado y a los empleados (por ej., sobre la evaluación del impacto). b) Actuará como interlocutor y punto de contacto entre el responsable o encargado y la AEPD y las autoridades autonómicas. c) Cooperará con la autoridad de control. d) Podrá inspeccionar los procedimientos y emitir recomendaciones. e) Supervisar el cumplimiento de la normativa y las políticas del responsable o del encargado. Cuando aprecie la existencia de una vulneración relevante lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado.

RESPONSABLE DE LA PRIVACIDAD: Es la persona que trabaja en la empresa y que, además de su cargo, también es designada para coordinar todos los aspectos relacionados con la protección de datos. Es la persona con la que se pondrá en contacto la AEPD si necesita conocer cualquier tipo de información, realizar hacer alguna inspección, etc.

REPRESENTANTE: Persona física o jurídica DENTRO DE LA UE, designada por escrito por el responsable o el encargado para que represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones.
La AEPD o, en su caso, las autoridades autonómicas de protección podrán imponer al representante, **SOLIDARIAMENTE** con el responsable o encargado, las medidas establecidas en el RGPD. Así, en caso de exigencia de responsabilidad, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

AUTORIDADES DE CONTROL (cooperaran entre si)

AEPD	**DEF**		**Autoridad administrativa independiente (OOAA NO),** con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia.
	CARAC		1.- Se relaciona con el Gobierno a través del **Ministerio de Justicia**. 2.- La AEPD y el CGPJ colaborarán en aras del adecuado ejercicio de las competencias que la LOPJ establece en materia de protección de datos. 3.- La AEPD tendrá la condición de **representante común** de las autoridades de protección de datos de España en el Comité Europeo de Protección de Datos. 4.- Está **sujeta al Derecho Administrativo** tanto en el ejercicio de sus competencias como en su régimen patrimonial y de contratación.
	COMPOSICIÓN	**PRESIDENTE Y ADJUNTO**	1.- NOMBRAMIENTO del Presidente y su Adjunto (solo 1): ***RD CMIN*** *a propuesta del M. Justicia, entre personas de reconocida competencia, por* ***5 años RENOVABLES.*** 2.- Los actos y disposiciones del Presidente de la AEPD ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso de la Audiencia Nacional.
		CONSEJO CONSULTIVO (como asesor de la AEPD)	1.- NOMBRAMIENTO: por ORDEN del Ministerio de Justicia. 2.- Composición: *a) Un Diputado, propuesto por el Congreso y un Senador, propuesto por el Senado.* *b) Un representante designado por el CGPJ.* *c) Un representante de la AGE, propuesto por el M.Justicia, un representante de las 19 CCAA y un experto por la FEMP.* *d) Un experto por el Consejo de Consumidores y Usuarios y un representante de los Colegios Profesionales de ámbito estatal, propuesto por el M.Justicia.* *e) Dos expertos designados por las organizaciones empresariales y dos expertos designados por las organizaciones sindicales.* *f) Un representante de profesionales de protección de datos.* *g) Un representante de las entidades de supervisión y resolución extrajudicial de conflictos, por el M.Justicia.* *h) Un experto designado por Conferencia de Rectores de las Universidades Españolas.* *i) Un representante de los profesionales de la seguridad de la información.* **Ya no forma parte la Real Academia de la Historia.*
	ESTATUTO		Se aprobará por RD CMIN, a propuesta AEPD.
	FUNCIONES		1.- Supervisar la aplicación de la LOPDPGDD y del RGPD. 2.- Desempeñar otras funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea. 3.- Velar por la privacidad y la protección de datos de los ciudadanos 4.- La Presidencia podrá dictar disposiciones --> «**Circulares de la AEPD**», que serán obligatorias una vez publicadas en el BOE (pero carece de potestades de regulación). 5.- Titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos *(igualmente, le corresponde esta función, a las autoridades autonómicas).*
AUTORIDADES AUTONÓMICAS DE PROTECCIÓN DE DATOS			Podrán ejercer, las funciones y potestades establecidas para la AEPD, de acuerdo con la normativa autonómica.
COMITÉ EUROPEO DE PROTECCIÓN DE DATOS	**DEFINICIÓN**		Organismo de la UE, que gozará de personalidad jurídica, con total independencia en el desempeño de sus funciones y no solicitará ni admitirá instrucciones de nadie.
	FUNCIÓN		Su función principal es aprobar los **códigos de conducta** que afecten a varios Estados Miembros.
	COMPOSICIÓN		Estará compuesto por el director de una autoridad de control de cada EM y por el Supervisor Europeo de Protección de Datos o sus representantes y la Comisión Europea.

**Las AP, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la AEPD los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.*

OTROS DATOS

Registro de actividad del tratamiento	***Características***	1.- Una de las novedades del RGPD es que ya no será necesario inscribir los ficheros en la AEPD (ficheros de clientes, de proveedores, etc.). Esta obligación se sustituye porque determinadas empresas u organizaciones, **lleven su propio registro de actividades (por escrito, en formato electrónico).** 2.- El Registro de actividades de tratamiento deberá guardarse en la empresa, estar siempre actualizado y a disposición de la Autoridad de control. **Igualmente, cuando el responsable o el encargado hubieran designado un DPD deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.* 3.- Se considera infracción grave el no disponer de un Registro de actividades de tratamiento en los casos en que sea necesario.
	Obligatorio	1.- Empresas y organizaciones que empleen a 250 o más trabajadores. 2.- Cuando el tratamiento pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales (ej.: de salud), o datos personales relativos a condenas e infracciones penales.
Transferencia internacional de datos a un 3º país u organización internacional		1.- Cuando la Comisión así lo haya decidido (a través de un "acto de ejecución"), entendiendo que el tercer país, territorio, sectores específicos de ese tercer país, o la organización internacional garantizan un nivel de protección adecuado. En este caso, dicha transferencia no requerirá ninguna autorización específica más. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años y, no obstante, además, la Comisión supervisará de manera continuada los acontecimientos en 3º países y organizaciones internacionales que puedan vulnerar el RGPD. **¡Ojo! si una autoridad de protección de datos considerase que una decisión de la Comisión, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el RGPD, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente su suspensión, hasta la resolución del asunto.* 2.- Cuando el responsable o el encargado del tratamiento hubiera ofrecido garantías adecuadas (cláusulas, normas corporativas o políticas vinculantes, códigos de conducta, mecanismos de certificación, etc.) y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. En estos casos, el interesado tendrá derecho a ser informado de las garantías relativas a la transferencia.
Ley 39/2015 y protección de datos		**Publicaciones** de datos personales: a) Un afectado: se indentificará por nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del DNI o equivalente. b) Pluralidad de afectados: igual pero las cifras aleatorias deberán alternarse. **Notificación** de datos personales por **medio de anuncios** (interesados desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar): se identificará exclusivamente por nº completo de DNI o equivalente y, en su defecto, por nombre y apellido (pero NUNCA con DNI y nombre y apellido a la vez).
Procedimiento sancionador		• Es potestad de cada EM decidir sobre la imposición de multas administrativas a las APs. En el caso de España, se ha optado **por no imponer multas económicas.** • La **autoridad de protección de datos propondrá la iniciación** de actuaciones disciplinarias cuando existan indicios suficientes para ello. • Se **comunicarán al Defensor del Pueblo** o, en su caso, a las instituciones análogas de las CCAA las actuaciones realizadas y las resoluciones. • El **plazo para resolver** un procedimiento sancionador en materia de protección de datos es de **9 meses.** • Prescripción: --> Infracciones: las leves en 1 año, las graves en 2 años y las muy graves en 3 años. --> Sanciones: menores o iguales a 40.000€ 1 año, entre 40.001 y 200.000€ 2 años y mayores de 300.000€ 3 años.