Protección de datos personales y privacidad

- Ideas principales sobre los datos personales y privacidad
- Principales leyes que respaldan la protección de datos
- Tratamiento de los datos personales en los centros educativos y personas que intervienen
- Principios en materia de protección de datos
- El consentimiento como condición de licitud

Copyright 2026

Ideas principales sobre los datos personales y privacidad

¿Qué es un dato personal?

DATO PERSONAL (Art.4.1 RGPD):
«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.»



Fuente propia

La lista recogida en el artículo anterior del RGPD no es exhaustiva. Por lo tanto, dato personal puede ser cualquier información que sirva para identificar a una persona física. Es decir, un dato identificativo como el nombre y apellidos, el DNI, una huella dactilar, un conjunto de rasgos físicos, un número de identificación escolar o la imagen o la voz que permitan la singularización del interesado.

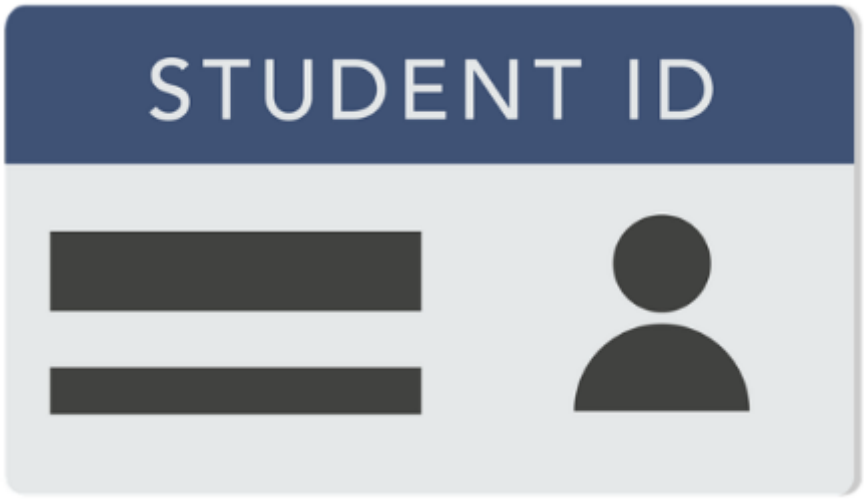


Imagen de Christina Smith en Pixabay.

> Más información en la guía para centros educativos de la AEPD

Datos de especial protección

Los datos de menores de edad tienen una especial protección:
Según el RGPD los niños merecen una protección específica, ya que pueden ser menos conscientes de los riesgos, consecuencias,
garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y cuando se utilicen servicios ofrecidos directamente a un niño.

Diversas leyes otorgan a los menores de edad una especial protección y con el concepto de “interés superior del menor” se establecen obligaciones que afectan a las instituciones públicas y privadas y a todas las personas que traten con menores de edad, en orden a proteger sus derechos y libertades, entre ellos el de protección de datos personales.

Categorías especiales de datos

Son aquellos datos personales que revelan:

- **El origen étnico o racial**

En los centros a veces se reparten algunos cuestionarios elaborados por ejemplo en el ámbito de ayudas de la UE que incluyen preguntas relativas al origen étnico o racial (entre otras cuestiones reveladoras de las circunstancias sociales de los perceptores de las ayudas).

- **Las opiniones políticas**
- **Las convicciones religiosas o filosóficas**

En el servicio de comedor también se facilitan determinados datos por las familias sobre las restricciones o preferencias derivadas de la pertenencia a determinadas religiones.
La AEPD ha considerado sin embargo que «No tiene la consideración de categoría especial de datos o datos sensibles el que un alumno curse la asignatura de religión, ya que el mero hecho de cursar la misma no implica revelación de su confesión religiosa».

- **La afiliación sindical**

La información sobre la pertenencia a sindicatos de estudiantes es un ejemplo de tratamiento de datos reveladores de la afiliación
sindical.

- **Los datos genéticos**

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.

- **Los datos biométricos**

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.

Los datos que se traten deben ser adecuados, pertinentes y proporcionados en función de su finalidad. Es decir, hay que realizar un
juicio de necesidad y proporcionalidad para descartar «que no haya otros medios menos intrusivos para ello y que de su tratamiento se deriven más beneficios para el interés general que perjuicios sobre otros bienes y valores».
La AEPD ha admitido la utilización de la huella dactilar para finalidades como el control de acceso al servicio de comedor en centros escolares con un gran número de alumnos, siempre que se

adopten medidas que refuercen la confidencialidad de los datos como la conversión de la huella a un algoritmo, el cifrado de la información, la vinculación a un dato distinto de la identificación directa del alumno o la limitación de los protocolos de acceso a los datos.

> Para más información sobre datos biométricos pulsa aquí

- **Datos relativos a la salud**

Revelan la salud física o mental del alumnado, en el pasado, presente o futuro.

«Los centros educativos recaban en muchos casos, a través de sus servicios médicos o botiquines, datos de salud relacionados con las lesiones o enfermedades que pudieran sufrir los alumnos durante su estancia en el centro. También recogen datos de salud de los alumnos para el ejercicio de la función educativa, discapacidades físicas o psíquicas, por ejemplo del síndrome TDAH (trastorno por déficit de atención e hiperactividad).
Para prestar el servicio de comedor también es necesario recabar datos de salud que permitan conocer los alumnos que son celiacos, diabéticos o que padecen alergias alimentarias. También son datos de salud los contenidos en los informes psicopedagógicos de los alumnos»

- **Datos relativos a la vida sexual**
- **Datos relativos a la orientación sexual**

Para el cumplimiento de los principios y derechos de diversidad sexual y de género y la no discriminación, se han establecido en las
Comunidades Autónomas protocolos que obligan al tratamiento en los centros educativos de datos reveladores de la orientación sexual.

¿Cuáles pueden ser las primeras acciones para velar por los datos personales en un centro educativo, a la hora de presentar datos a la comunidad educativa?

- **Seudonimización** es una medida utilizada para impedir la identificación del interesado por terceras personas, mediante la disociación de la identidad del interesado y del dato personal, sustituyendo la identidad real por un identificador ficticio (seudónimo) y manteniendo determinada información adicional separada que permite volver a realizar la identificación.
  Por ejemplo, si en un **listado que incluya el nombre y apellidos** de los alumnos con

medidas educativas especiales, la dirección de un centro **sustituye la identificación por códigos individuales** de uso único que guarda de forma separada y segura en un repositorio, estaría aplicando una técnica de seudonimización, porque evita que terceras personas puedan identificarlos, pero las personas autorizadas podrían en cualquier momento volver a asociar cada código a cada alumno para identificarlos.

- **Anonimización** es un proceso que disocia de forma permanente la identidad y el dato, de forma que no permita volver a singularizar o identificar al interesado, que se oculta con un proceso irreversible. Por ejemplo, si en un listado Excel de calificaciones de todos los alumnos de un centro suprimimos las columnas que contienen los datos de identificación del alumnado para elaborar una estadística, si no existiese ninguna información adicional (característica física, un dato de localización o un rasgo cultural o biológico) que permita identificar qué alumno ha obtenido cada nota hemos aplicado un proceso de anonimización.



Imagen de Jan en Pixabay

- **Publicación de parte de los datos**. La Agencia Española de Protección de Datos nos transmite posibles criterios prácticos, como el que mostramos a continuación, a la hora de publicar listados tablones de anuncios o en sus comunicaciones digitales ante la necesidad legal de tener que dar información pública de la divulgación del documento nacional de identidad, para ello, seleccionaremos aleatoriamente el grupo de cuatro cifras numéricas que se van a publicar para la identificación de los interesados en las publicaciones de actos administrativos. El procedimiento para la determinación de forma aleatoria de las cuatro cifras numéricas a publicar del código de identificación de un interesado se realiza mediante el proceso de selección aleatoria en una bolsa opaca de

una bola de entre cinco **bolas numeradas del 1 al 5**, si a bola resultante es la **número 4**, la publicación de documento nacional de identidad será de la siguiente forma:
Dado un DNI con formato **12345678X**, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo:

*****4567****

Medidas preventivas, herramientas y configuraciones para proteger la privacidad

Para preservar nuestra privacidad deberemos de tener una serie de precauciones, configuraciones y herramientas concretas que nos ayuden a preservar nuestros datos y por tanto nuestra privacidad, debemos de tener muy presente:

- Mantener los dispositivos que utilicemos **actualizados.**
- **Protección frente accesos no deseados**. La primera barrera de seguridad son los patrones de desbloqueo y las contraseñas que tienen que ser robustas (difíciles de romper), no predecibles y secretas.
- **Cifrado del contenido** del dispositivo.
- **Gestión de contraseñas.**
- **Detección de accesos y/o usos no controlados** del dispositivo.

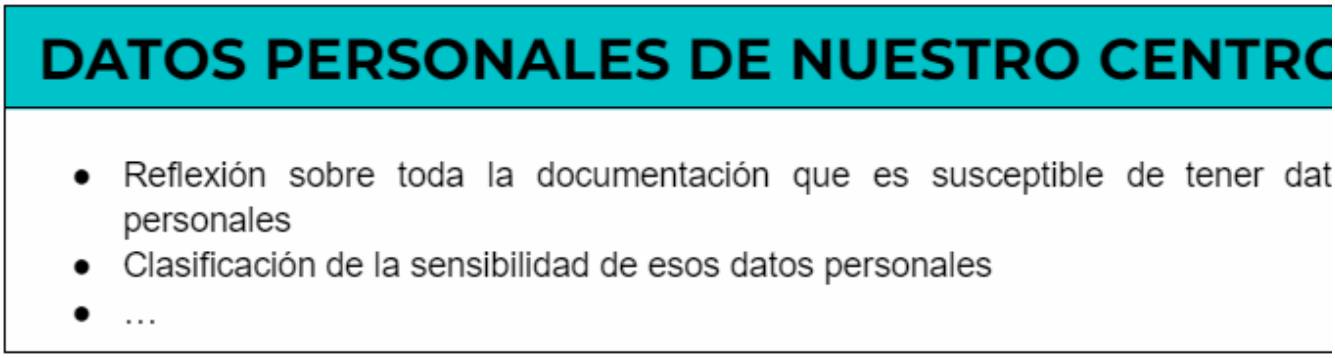
> Para más información y conocer más herramientas que nos ayudan a tener mayor privacidad pulsa en el siguiente enlace

- **Configurar las opciones de privacidad** de RR.SS., navegadores, sistemas operativos, aplicaciones de mensajería instantánea, etc.

> Para más información sobre configuraciones pulsa en el siguiente enlace

Copyright 2026

Una ejemplo de plantilla para ir constatando los acuerdos y compromisos del centro puede ser esta.



Principales leyes que respaldan la protección de datos

- **CONSTITUCIÓN ESPAÑOLA** (ART. 18 CE).

En el Art. 18 de la Constitución Española se garantiza:

1. El derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

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.

> Para más información pulsa en el siguiente enlace

- REGLAMENTO (UE) 216/679, DE 27-4-2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (**REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, RGPD**)

> Para más información pulsa en el siguiente enlace

- **LEY ORGÁNICA** 3/2018, DE 5 DE DICIEMBRE, DE **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES** (**LOPDGDD**)

1. Está en vigor desde el 07/12/2018.

Copyright 2026

2. Completa y aplica el RGPD e incorpora un Título X dedicado a la “Garantía de los derechos digitales”, que desarrolla aspectos como el derecho a la educación digital, la protección de los menores en Internet o un nuevo catálogo de derechos de la “Era digital”, como los relacionados con internet y redes sociales o en el ámbito laboral y funcionarial.

> Para más información pulsa en el siguiente enlace

- LEY ORGÁNICA 2/2006, DE 3 DE MAYO, DE EDUCACIÓN (**LOE**), RECIENTEMENTE MODIFICADA POR LA LEY ORGÁNICA 3/2020, DE 29 DE DICIEMBRE (**LOMLOE**)

Disposición adicional vigesimotercera. Datos personales de los alumnos:

1. Los centros docentes podrán recabar datos necesarios para el ejercicio de su función educativa, que podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea estrictamente necesaria para la función docente y orientadora. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información.
2. La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad.
3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad.
4. El profesorado y el resto del personal que acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

Artículo 111 bis. Tecnologías de la información y la comunicación. Esta disposición regula aspectos tan relevantes como:

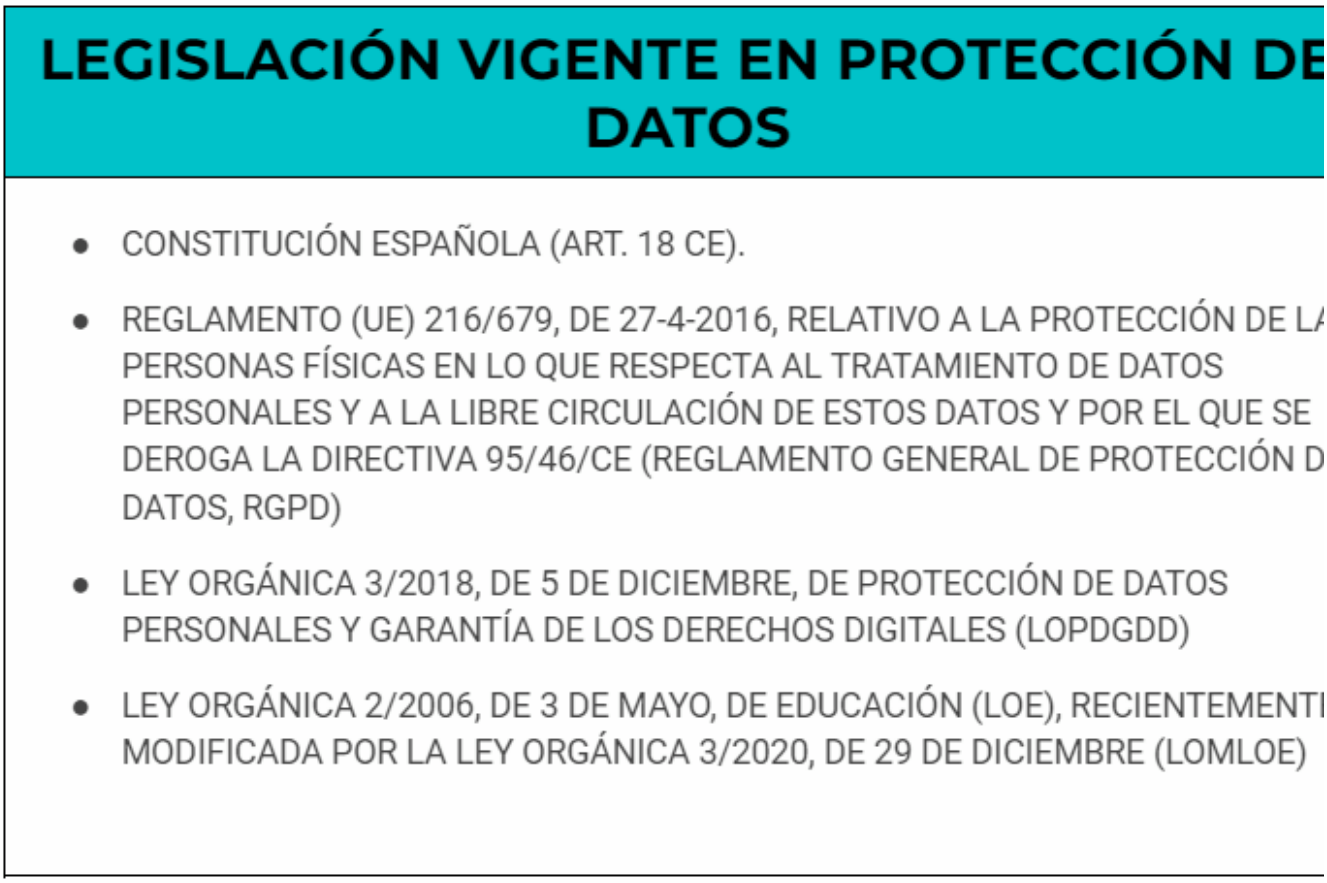
- Los estándares que garanticen la interoperabilidad entre los distintos sistemas de información del Sistema Educativo Español y los distintos niveles de compatibilidad y seguridad en el tratamiento de los datos.
- El número identificativo para cada alumno o alumna, a fin de facilitar el intercambio de la información relevante con respeto de la privacidad y protección de datos personales.
- Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos que deben permitir el acceso del alumnado, desde cualquier sitio y en cualquier momento, con respeto de la normativa de propiedad intelectual, privacidad y protección de datos personales y de los principios de accesibilidad universal y diseño para todas las personas y procurando su compatibilidad e interoperabilidad. Así mismo, se regulan las características de las plataformas digitales y tecnológicas ofrecidas por el

Ministerio de Educación y Formación Profesional a toda la comunidad educativa.

- La obligación de las Administraciones educativas y de los equipos directivos de los centros de promover el uso de las tecnologías de la información y la comunicación (TIC) en el aula. También se obliga a establecer las condiciones que hagan posible la eliminación en el ámbito escolar de las situaciones de riesgo por la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.
- La obligación estatal de fijar los marcos de referencia de la competencia digital en la formación inicial y permanente del profesorado para el desarrollo de una cultura digital en los centros y en las aulas.
- La obligación de las Administraciones públicas de velar por el acceso de todos los estudiantes a los recursos digitales necesarios (para disminuir la denominada brecha digital).

Para más información pulsa en el siguiente enlace

Una ejemplo de plantilla de centro donde iremos anotando las legislación vigente en protección de datos puede ser esta:



Tratamiento de los datos personales en los centros educativos y personas que intervienen

¿Qué es el tratamiento de datos?

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.

Resumiendo, es **cualquier actuación que se haga sobre datos personales**, y podrá ser considerada un tratamiento de datos personales.

Copyright 2026



Fuente propia

Desde la tramitación de los procesos de **admisión del alumnado**, los centros educativos tratan información personal del alumno para proporcionarle los servicios de educación y orientación, que se traduce en acciones muy diversas realizadas por parte de diferentes intervinientes: las autoridades educativas estatales y autonómicas, el centro docente, los órganos de gobierno y participación de los centros, los integrantes de la comunidad educativa (profesorado, alumnado, familias...), con finalidades tan distintas como la confección de los **expedientes académicos**, la **gestión de los comedores** y **transporte escolares**, la **concesión de ayudas para estos conceptos y para material curricular**, la concesión de **premios académicos**, la organización y promoción de actividades educativas, **culturales, deportivas** y de ocio, la evaluación académica, la **orientación del alumnado con necesidades educativas** especiales o específicas, la corrección disciplinaria. Para ello se recogen y registran datos personales, se captan y difunden imágenes del alumnado y profesorado, se organizan eventos, se utilizan recursos didácticos digitales, se comunican datos a diversas instituciones...

Todo ello implica el **tratamiento de un considerable volumen de datos personales** que afectan a toda la comunidad educativa. Este tratamiento se realiza en diversos **formatos, en papel, a través de aplicaciones informáticas,** por medio de empresas externas, con y sin transferencias internacionales de datos.

Por otra parte, algunos de estos datos deberán destruirse tras finalizar el curso escolar o tras agotarse la finalidad de su tratamiento, pero otros se mantienen por tiempo indefinido en los gestores y repositorios de expedientes académicos. Cada uno de estos medios y cada uno de estos períodos de conservación tiene unos riesgos específicos para la protección de datos que debemos

Copyright 2026

tener en cuenta.

Por lo tanto, desde el origen de un tratamiento hasta su supresión se realizan determinadas operaciones con los datos personales. Cada operación tiene unas reglas básicas que afectan al diseño de cualquier proyecto, al registro del tratamiento, a la transparencia e información a los interesados, a la gestión del tratamiento por el propio responsable o a través de otra persona encargada, al sistema informático utilizado y las medidas de seguridad aplicables, así como a la gestión de los incidentes o brechas de seguridad, al ejercicio de derechos o a cómo conservar y destruir adecuadamente los datos una vez agotada su finalidad.



Infografía Quién es quién. Fuente AEPD.

Responsable

Persona física o jurídica, autoridad pública, servicio u organismo que solo o con otros determine los fines y medios del tratamiento.
En los tratamientos educativos realizados por los centros educativos públicos, son responsables,

habitualmente, los órganos administrativos de la **Consejería de Educación** o del Ministerio de Educación en su ámbito de actuación respectivo, aunque actúen en muchos tratamientos a través de los centros docentes o de otro personal. El tratamiento de los datos por estas personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable no se considera cesión o comunicación de datos, porque estas personas actúan en nombre del responsable.

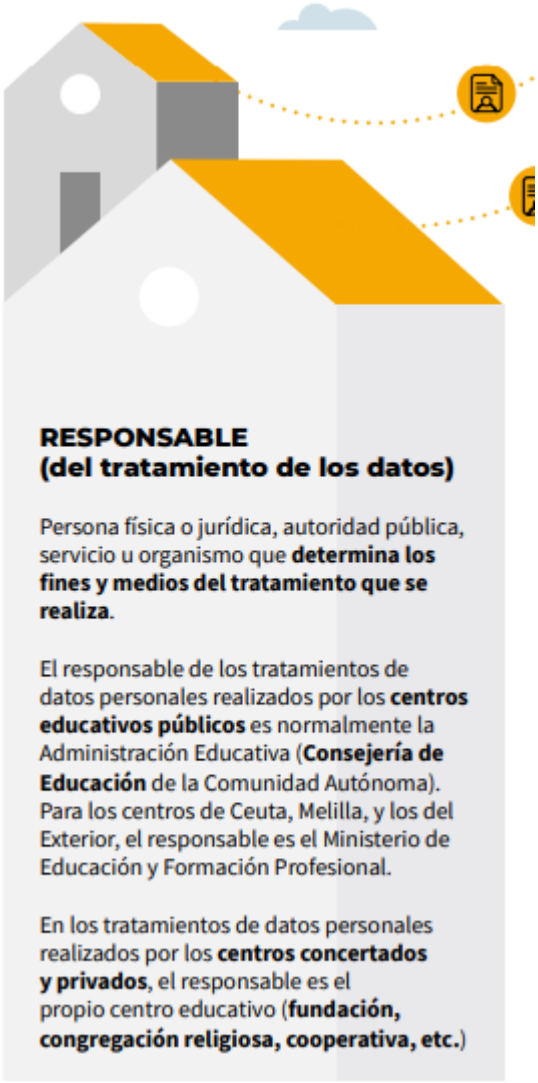
El **registro de actividades de tratamiento (RAT)** en las Administraciones Públicas (incluidos los centros docentes) es público y debe ser accesible por medios electrónicos (art. 31.2 LOPDGDD). En los centros públicos, normalmente será **la Consejería de Educación la que se encargue de actualizar ese RAT,** en su caso, con el asesoramiento de los Delegados de Protección de Datos, a quienes deben comunicarse por el responsable las modificaciones, adiciones o supresiones que se hagan en el RAT.



Modificación de la imagen de Mohamed Hassan en Pixabay.

> A continuación se muestran dos ejemplos de RAT de los Departamentos de Educación de Valencia (enlace) y de Educación de Madrid (enlace), donde se desglosan los diferente tipos de actividades y agente involucrados.

En los centros concertados y privados son responsables los titulares de los propios Centros

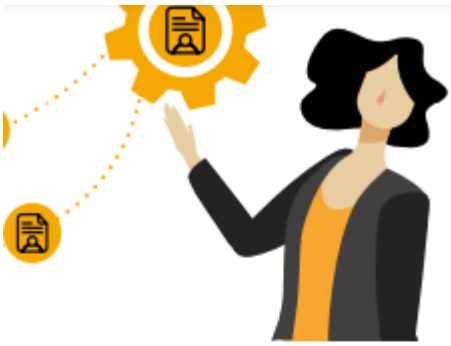


Fuente AEPD

Encargado del tratamiento

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del responsable.** Al igual que en el caso de los responsables del tratamiento, **el encargado puede actuar por sí mismo o a través de otras personas que actúan bajo su autoridad directa**. Además, el encargado puede subencargar el tratamiento a otras personas o entidades que actúan siguiendo las instrucciones del encargado principal (y a su vez, ambos, siempre deben actuar en el marco de las instrucciones fijadas por el responsable).
El encargado de tratamiento debe ofrecer las garantías suficientes de aplicación de medidas técnicas y organizativas adecuadas para garantizar la protección de datos y su seguridad.
El encargo requiere la firma de un contrato. En resumen, los encargados asumen la mayor parte de las obligaciones de los responsables con respecto al encargo realizado, pero actúan por cuenta de estos y siguiendo sus instrucciones, fijadas en el acto jurídico correspondiente.

Copyright 2026



ENCARGADO
(del tratamiento de los datos)

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del responsable**. El responsable determina a quién le encarga el tratamiento que se va a llevar a cabo. Debe ser elegido por éste únicamente **entre los que ofrezcan garantías suficientes** de cumplimiento de la normativa de protección de datos.

El encargado siempre debe actuar en el marco de las instrucciones fijadas por el responsable.

El flujo de datos personales entre el responsable y el encargado no constituye una cesión de datos.

Ejemplos de encargados en el ámbito educativo: prestadores de servicios tecnológicos, empresas que gestionan el comedor escolar, la ruta escolar, las actividades extraescolares, etc.

Fuente AEPD

Delegado de protección de datos

El DPD tiene funciones principales de **supervisión del cumplimiento de la legislación sobre protección de datos**, **asesoramiento a responsables y encargados** en esta materia de protección de datos, cooperación e interlocución con la autoridad de control respectiva, participación en las reclamaciones de los interesados, evaluaciones de impacto y en otros asuntos encomendados a los responsables de los tratamientos.

El DPD puede formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Copyright 2026



DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Figura que debe designar el responsable **de forma obligatoria** para todos los centros educativos que ofrecen enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación.

Funciones**, entre otras, del **DPD
Asesorar e informar al responsable sobre la aplicación de la normativa de protección de datos y supervisar su cumplimiento.

Interlocutor con las personas afectadas para cualquier cuestión de protección de datos, lo que incluye **dudas**, tanto de las familias como de profesionales de la educación, así como **quejas y reclamaciones**.

El DPD será nombrado por la Administración Educativa correspondiente cuando sea esta la responsable del tratamiento de datos en centros de titularidad pública y, en caso de centros privados o concertados, por el centro educativo.

Fuente AEPD

La LOPDGDD especifica los responsables y encargados que deberán designar un DPD, mencionándose entre ellos los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles educativos. **Esto no significa que cada centro docente deba tener un DPD distinto, sino que todos los centros deben tener un DPD**. A estos efectos, el artículo 37.3 RGPD establece que 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».

agencia española protección datos

Contactos DPD Educación CC.AA.

COMUNIDAD/CIUDAD AUTÓNOMA	E-mail del DPD
Andalucía [1] (Autoridad de control propia)	DPD.CED@JUNTADEANDALUCIA.ES
Aragón	PROTECCIONDATOSECD@ARAGON.ES
Asturias	DPD-PRESIDENCIA@ASTURIAS.ORG
Baleares	PROTECCIODADES@DPD.CAIB.ES
Canarias	VEUD.EDUCACION@GOBIERNODECANARIAS.ORG
Cantabria	DPDCENTROSDOCENTES@EDUCANTABRIA.ES
Castilla-La Mancha	PROTECCIONDATOS@JCCM.ES
Castilla y León	DPD.EDUCACION@JCYL.ES
Cataluña [2] (Autoridad de control propia)	DPD.PRESIDENCIA@gencat.cat
Extremadura	DPD@JUNTAEX.ES
Galicia	DPD.CULTURA.EDUCACION@XUNTA.GAL
La Rioja	DELEGADAPD@LARIOJA.ORG
Madrid	PROTECCIONDATOS.EDUCACION@MADRID.ORG
Murcia	DPD.CENTROS@MURCIAEDUCA.ES
Navarra	DPD@NAVARRA.ES
País Vasco [3] (Autoridad de control propia)	DPD-DBO@AVPD.EUS
Valencia	DPD@GVA.ES
Ceuta y Melilla	DPD MINISTERIO DE EDUCACIÓN Y F.P. DPD@EDUCACION.GOB.ES

Fuente AEPD

Los centros concertados y privados también están obligados a tener su propio DPD, si bien, entre varios centros pueden compartir uno.

Interesado

Es la **persona física titular (propietaria) de los datos personales**. Es importante recordar que los responsables o encargados de tratamiento tratan (administran) los datos de los interesados, pero los datos pertenecen únicamente a cada persona física identificada o identificable a la que se refieren.



Fuente AEPD

Además a los interesados les ampara la normativa de protección de datos y le otorga una serie de derechos, los cuales los puede ejercer dirigiéndose ante quien está tratando sus datos (responsable). Los derechos son los siguientes:

- Derecho de información
- Derecho de rectificación
- Derecho de oposición
- Derecho a la limitación de tratamiento
- Derecho de acceso
- Derecho de supresión
- Derecho de portabilidad

Copyright 2026



Fuente AEPD

Destinatario

Es la persona física o jurídica, autoridad u organismo **a quien se comuniquen (cedan) los datos personales**, ya sea esta persona otro responsable o un tercero.
La cesión de datos será una transferencia internacional cuando el destinatario de los datos está establecido en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega). En caso de transferencia internacional, el RGPD exige garantías o requisitos adicionales para el tratamiento de datos personales.

Tercero

Es la persona física o jurídica, autoridad, 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.

Copyright 2026

Autoridad de control

La autoridad pública independiente establecida por un Estado miembro de la UE con arreglo a lo dispuesto en el artículo 51 RGPD. Se llama «autoridad de control interesada» a la autoridad de control a la que afecta el tratamiento de datos personales.
La **Agencia Española de Protección de Datos (AEPD)** es una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

Agencia Española de Protección de Datos. Fuente AEPD

Tiene atribuidos los poderes y funciones, los más relevantes son las potestades de investigación e inspección, la atención de reclamaciones, la potestad sancionadora, dictar criterios y circulares obligatorias, los planes de auditoría preventiva y directrices.

¿Cuál es el protocolo de actuación en caso de tener una brecha de seguridad?: El **responsable** debe notificar a la correspondiente **autoridad de control** (AEPD) a través del **DPD** en un plazo muy reducido (**72 horas** desde que se tenga conocimiento del incidente), así como la adopción de las medidas cautelares que procedan para evitar perjuicios mayores en la privacidad y, en algunos casos, la notificación del incidente producido también a los **interesados**.

Una ejemplo de plantilla para ir constatando los acuerdos y compromisos del centro puede ser esta.

RESPONSABLE

- La **Consejería de Educación de la DGA** es la responsable en nuestro centro educativo público y tiene que actualizar el registro de actividades de tratamient (RAT).

ENCARGADO

- La **dirección del centro** educativo es habitualmente quien ostenta este cargo, y trata los datos por cuenta del responsable.

DELEGADO DE PROTECCIÓN DE DATOS

- La persona designada por el Departamento de Educación en Aragón tiene el siguiente contacto: **PROTECCIONDATOSECD@ARAGON.ES**

INTERESADOS

- El **alumnado** es el propietario de sus datos, cuando son menores de 14 años, lo tutores legales son los que dan el consentimiento en su nombre, pero los datos son del alumnado. Respecto a sus datos tienen derecho de información, rectificación, oposición, limitación de tratamiento, acceso, supresión y portabilidad

Copyright 2026

DESTINATARIO

- El **centro educativo**, dependiente del Departamento de Educación, es el organismo al que ceden los datos los interesados.

TERCEROS

- Cualquier persona física o jurídica, autoridad, servicio u organismo autorizado p la Consejería de Educación o dirección. Por ejemplo empresa encargada del comedor escolar o empresa de actividades extraescolares.

AUTORIDAD DE CONTROL

- La Agencia Española de Protección de Datos (AEPD)

Copyright 2026

Principios en materia de protección de datos

Los principios en materia de protección de datos pretenden asegurar que se está actuando de forma adecuada para no verse comprometida la privacidad, en total son 9 los principios que los detallamos a continuación:

1. **Licitud** : el tratamiento solo es posible si concurren las condiciones previstas en los artículos 6.1 RGPD (condiciones de licitud) y siempre que se den las circunstancias del 9.2 RGPD, para el caso de las categorías especiales de datos.

2. **Lealtad** : debe haber coincidencia entre la información facilitada al interesado sobre el tratamiento y el tratamiento efectivamente realizado en cada momento.

3. **Transparencia** : debe cumplirse con los deberes de información de los artículos 12 al 14 del RGPD, en los que se prevé concretamente la información mínima que debe facilitarse a los interesados en todo tratamiento, y garantizar que toda información y comunicación relativa al tratamiento sea fácilmente accesible y fácil de entender y que se utiliza un lenguaje sencillo y claro. Así mismo, debe permitirse el acceso a la información , en los términos previstos en el RGPD.



Imagen de pikisuperstar en Freepik

4. **Limitación de la finalidad**: la recogida de datos se hará para fines determinados, explícitos y legítimos y el tratamiento posterior debe ser compatible con dichos fines, con la excepción prevista para el archivo, investigación y estadística (y para estas finalidades el art. 89 exige garantías adecuadas, entre ellas la minimización y seudonimización, cuando sea posible).
En todo caso, se debe garantizar la información del interesado sobre esos otros fines posteriores y sobre sus derechos, incluido el derecho de oposición.



Fuente propia

5. **Minimización de datos**: solo pueden tratarse los datos adecuados, pertinentes y necesarios para los fines del tratamiento.

Este principio está relacionado la protección de datos por defecto que también debe garantizar el responsable; con el principio de limitación de la finalidad, ya que solo es pertinente el tratamiento que se limita a la finalidad informada, así como con los principios de necesidad y proporcionalidad, en virtud de los cuales en los tratamientos siempre deberá buscarse la mínima incidencia posible en el derecho de protección de datos de forma que solo es adecuado el tratamiento que es proporcionado a la finalidad perseguida y siempre que esta finalidad no pudiera lograrse razonablemente por otros medios.

6. **Exactitud y calidad de los datos**: Los datos deben ser exactos y actualizados y ello exige adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.
De acuerdo con la LOPDGDD, la inexactitud no es imputable al responsable del tratamiento cuando

este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que procedan, si los datos inexactos hubiesen sido obtenidos por el responsable:

- Directamente del afectado.
- De un mediador o intermediario en caso de que las normas aplicables al sector de actividad establecieran su posibilidad de intervención.
- De otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad.
- De un registro público.

7. **Limitación del plazo de conservación**: los datos deben mantenerse solo durante el tiempo necesario para los fines del tratamiento, salvo fines de archivo en interés público, investigación científica o histórica o estadísticos. Para ello es importante fijar plazos para la supresión y revisión periódica del tratamiento. Este principio también está relacionado con otros, como el de minimización, limitación de la finalidad y protección de datos por defecto.
En la conservación de datos en las Administraciones Públicas debe tenerse en cuenta la normativa sobre archivos y gestión de
documentos, aunque con frecuencia existe una gran indefinición en los plazos de conservación y una tendencia a conservar la información durante períodos superiores a los realmente necesarios. Por otra parte, las políticas de conservación o archivo deben tener en cuenta medidas de seguridad adecuadas, al igual que la supresión debe realizarse con seguridad.



Imagen de storyset en Freepik

8. **Integridad y confidencialidad**: debe garantizarse 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.

El RGPD se refiere a la seguridad del tratamiento de datos que debe garantizarse por el responsable y, en su caso, el encargado, mediante la adopción de medidas técnicas y organizativas proporcionadas, por ejemplo:

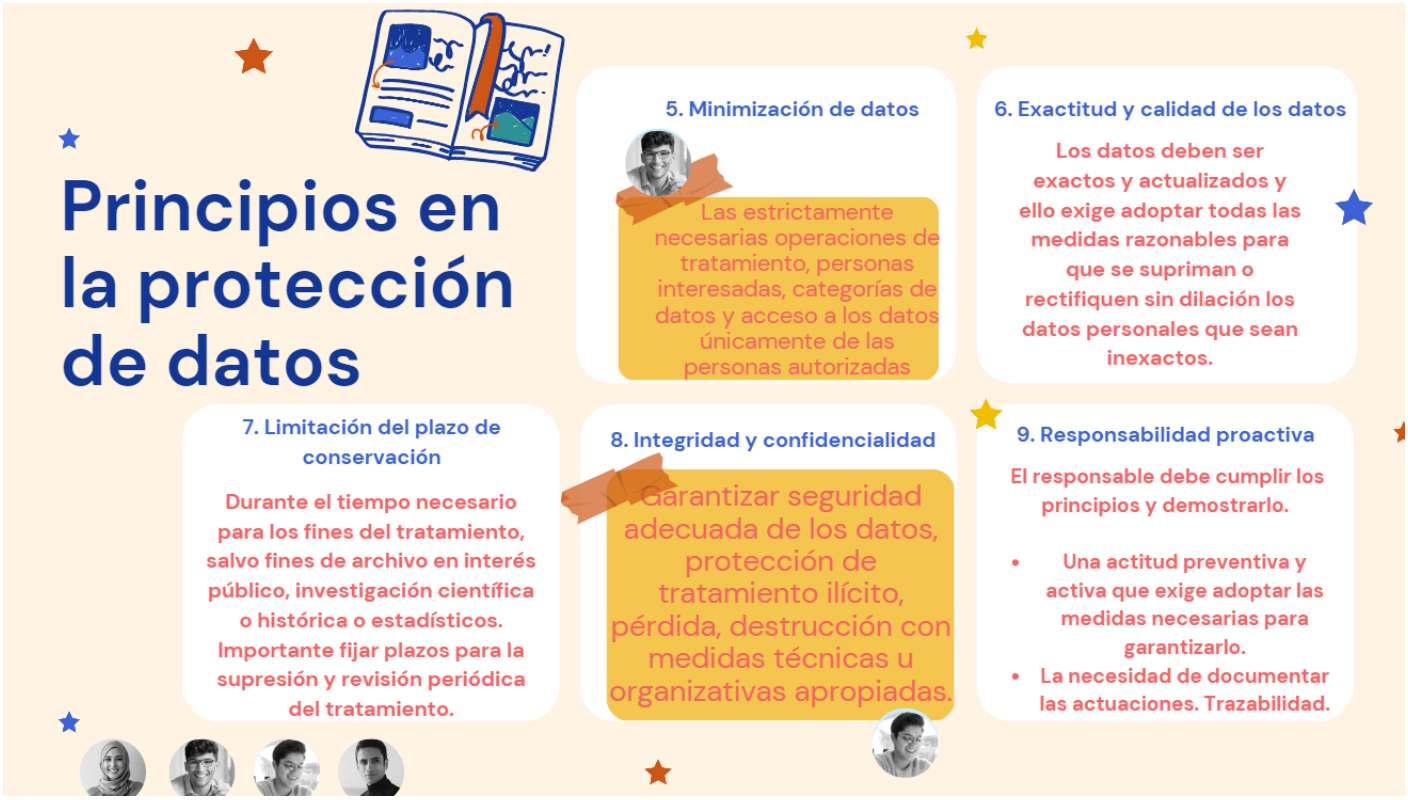
- La seudonimización y el cifrado de datos personales
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios del tratamiento
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Con respecto al deber de confidencialidad, la LOPDGDD establece este deber no solo para los responsables y encargados del tratamiento, sino para todas las personas que intervengan en cualquier fase de un tratamiento, manteniéndose aun después de finalizar la relación con el responsable o encargado. Además, esta obligación se establece con carácter complementario a los deberes de secreto profesional.

9. **Responsabilidad proactiva** : El responsable no solo debe cumplir los principios mencionados y otras obligaciones establecidas en el RGPD, sino que debe ser capaz de demostrarlo.
Este principio implica una inversión de la carga de la prueba que alcanza incluso a los procedimientos de infracción en materia de
protección de datos, en los que la "presunción de inocencia" es aplicable a quien demuestra que ha cumplido con sus obligaciones.
En la práctica, este principio se traduce en dos obligaciones atribuibles a los responsables:

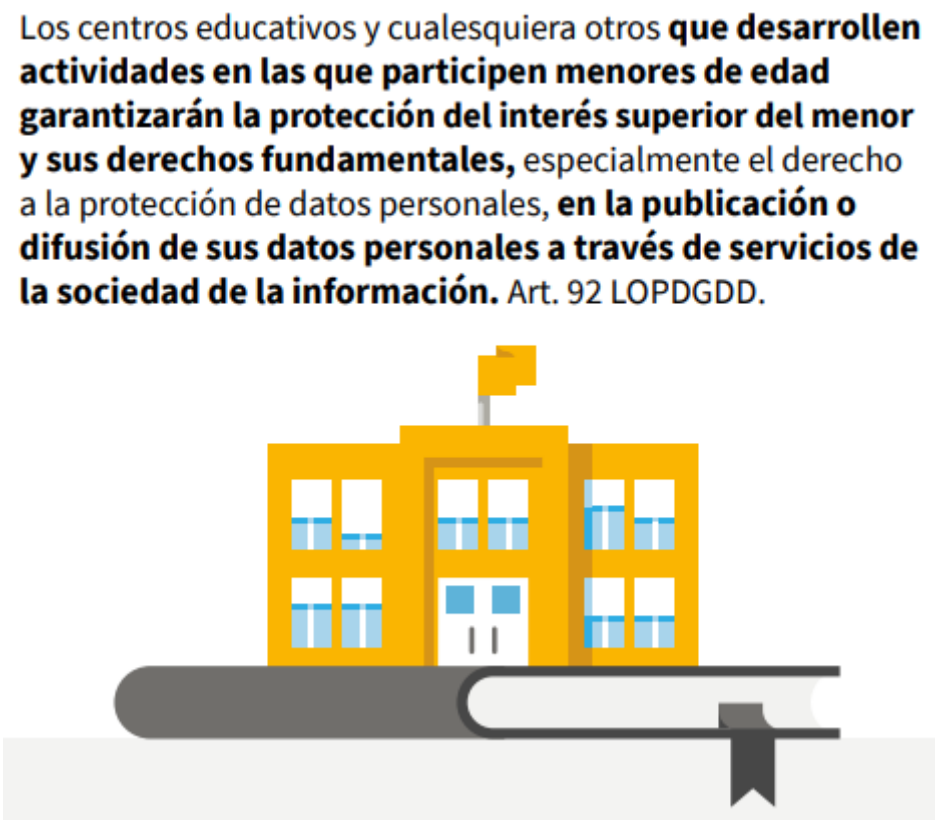
- Una actitud preventiva y activa en el cumplimiento de sus deberes, que exige adoptar las medidas necesarias para garantizarlo.
- La necesidad de documentar las actuaciones realizadas en el cumplimiento de sus deberes.

Copyright 2026



Fuente propia

El consentimiento como condición de licitud



Fuente AEPD

Los tratamientos de **datos personales** realizados con una **finalidad estrictamente docente** u orientadora del alumnado (la mayoría de los tratamientos realizados por los centros educativos tienen esta finalidad), están directamente amparados o exigidos por la LOE y, por lo tanto, **no debe recabarse el consentimiento**, sino que este tratamiento viene impuesto **por el cumplimiento de obligaciones legales o de intereses públicos**, sin perjuicio de la obligación del responsable de informar adecuadamente a los interesados. Para el resto de supuestos diferentes a la finalidad docente y orientadora del alumno, la legislación anterior al RGPD partía del principio general de que el tratamiento de los datos de carácter personal, salvo excepciones, requería el consentimiento inequívoco del afectado.

Copyright 2026



El consentimiento es **una de las causas** que puede legitimar el tratamiento de datos personales. Art. 6.1.a) RGPD.

Fuente AEPD

A partir del RGPD, el consentimiento es una más de las condiciones de licitud de los tratamientos, el artículo 6.1 del RGPD, según el cual, el tratamiento de datos debe basarse en alguna de las siguientes condiciones, que denominamos condiciones de licitud o bases de legitimación de los tratamientos de datos:

Art. 6.1.a) RGPD: el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.



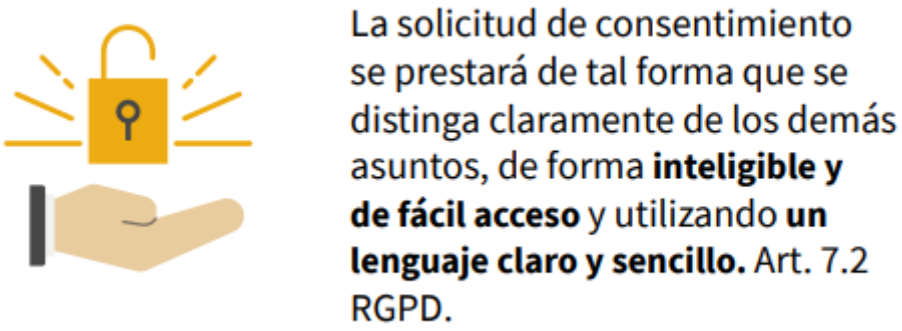
Consentimiento; toda **manifestación de voluntad libre, específica, informada e inequívoca** por la que el interesado acepta, ya sea mediante una **declaración o una clara acción afirmativa,** el tratamiento de datos personales que le conciernen. Art. 4.11 RGPD.

Fuente AEPD

De acuerdo con el RGPD, el consentimiento debe tener las siguientes características:

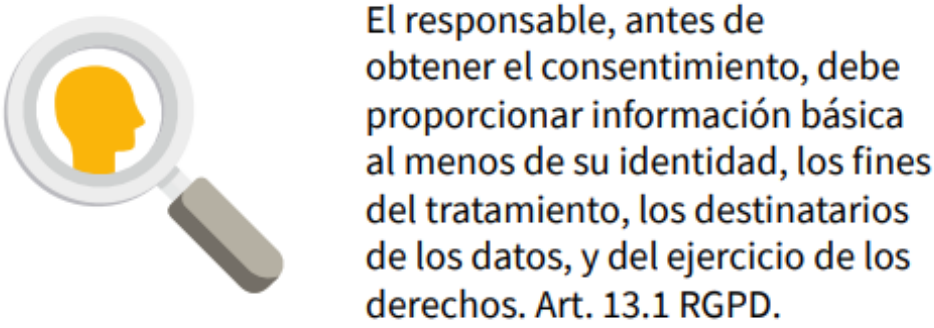
- **Manifestación de voluntad**: auténtica expresión de la voluntad del interesado.
- **Libre**: libre elección, sin sufrir perjuicio alguno, en el ámbito educativo, debe garantizarse que el interesado puede rechazar el tratamiento sin sufrir ningún perjuicio, ni quien consiente el tratamiento debe obtener un premio.
- **Específica**: No son válidos los consentimientos excesivamente genéricos. Por ejemplo, la AEPD ha admitido que se solicite el consentimiento para la captación o difusión de

imágenes de actividades escolares al principio de curso, dado que la finalidad del tratamiento y sus características en estos casos suele ser la promoción de las actividades del centro, pero no son válidas las peticiones de consentimiento genéricas y no especificadas en el propio tratamiento.



Fuente AEPD

- **Informada**: Se debe facilitar a los interesados la información, se debe informar de la existencia del derecho a retirar el consentimiento en cualquier momento, esta información deberá facilitarse en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.





El interesado tendrá derecho a **retirar su consentimiento en cualquier momento.** La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada **(sin efectos retroactivos)**. Antes de dar su consentimiento, **el interesado será informado de ello.** Será **tan fácil retirar el consentimiento como darlo.** Art.7.3 RGPD.

Fuente AEPD

- **Demostrable**: El responsable debe ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales, debe conservar la prueba de dicha manifestación (documento con la declaración escrita, grabación con la declaración verbal, etc.)



Corresponde al responsable del tratamiento la prueba de su existencia. Art. 7.1 RGPD.

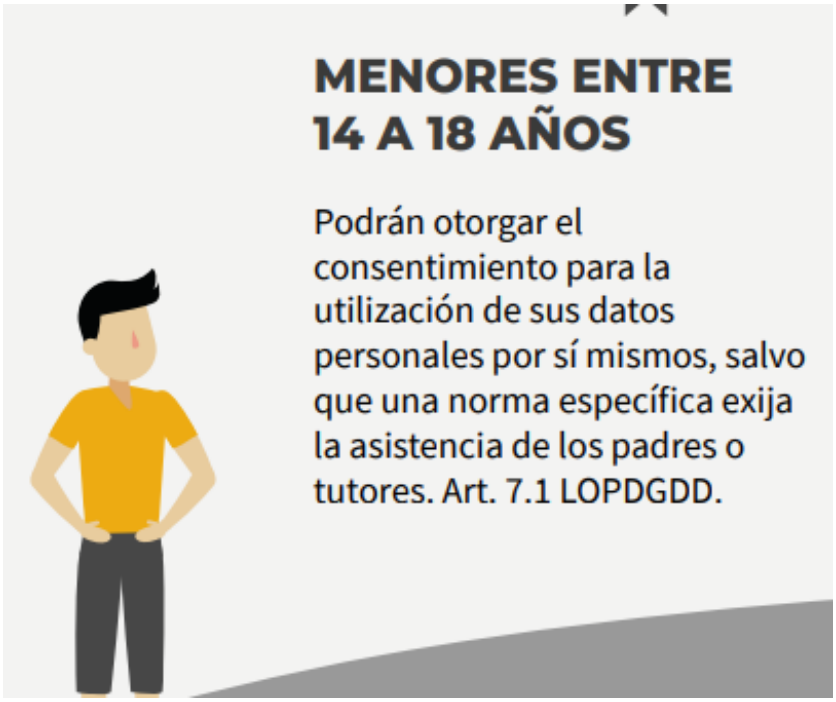
Fuente AEPD

- **Consentimiento de los menores de edad**: La LOPDGDD establece la edad mínima para prestar el consentimiento en 14 años y requiere el consentimiento del titular de la patria potestad o tutela. Por ejemplo, es preciso el consentimiento para la difusión de los datos personales de los participantes en una actividad voluntaria, realizada con fines de promoción de un centro escolar.



Fuente AEPD

A continuación podéis pulsar en el siguiente enlace para ver un ejemplo para el alumnado entre 14-18 que son capaces de consentir por sí mismos.



Fuente AEPD

Toda la información esta sintetizada en la siguiente infografía de la AEPD