REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO
de 27 de abril de 2016 , relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Al ser un Reglamento comunitario:

- Es obligatorio en todos sus elementos, está dotado de alcance general y es directamente aplicable en los Estados Miembros de la UE.
- En todos los casos en los que proporcione reglas concretas se aplica el Reglamento, en aquellos casos en los que se permite precisar algunos contenidos a los Estados miembros podrán desarrollarlos.
- En caso de contradicción entre el Reglamento europeo y la normativa española PREVALECE el Reglamento.

Objeto del Reglamento

- Proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales recogido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y garantizar la libre circulación de esos datos dentro de la UE.

La protección a los derechos fundamentales frente al tratamiento de datos personales va más allá del propio derecho a la protección de datos o de la vida privada, de hecho en el Considerando 4 se recogen otra serie de derechos que el Reglamento busca proteger

- el derecho al domicilio
- el derecho de las comunicaciones,
- el derecho de la protección de los datos de carácter personal,
- el derecho de la libertad de pensamiento, de conciencia y de religión,
- el derecho de la libertad de expresión y de información,
- el derecho a la libertad de empresa,
- el derecho a la tutela judicial efectiva y a un juicio justo, y
- el derecho a la diversidad cultural, religiosa y lingüística.

  - Ejemplos Caso RENFE y STC Alemán libertad de expresión

Ámbito territorial :

- El Reglamento se aplica al tratamiento de datos personales en las actividades de un establecimiento del responsable o del encargado en la Unión, con independencia de que el tratamiento tenga lugar en la Unión o no.

- Se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Ámbito de aplicación material:

- El RGPD se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

- No se aplica al tratamiento de datos personales:
  a) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domesticas.
     - El Reglamento no se aplica al tratamiento de datos personales por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.
  b) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión (seguridad nacional);
  c) Actividades de política exterior y seguridad común de los Estados miembros (EM).
  d) Actividades de prevención, investigación, persecución y sanción de infracciones penales.

LAS DEFINICIONES LEGALES RECOGIDAS EN EL RGPD

- a) ***Datos personales:*** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (art. 4.1 RGPD).

- Al igual que en la Directiva 95/46/CE el RGPD maneja un concepto amplio de datos personal.

  Ejemplo 1: UN Dibujo infantil en determinadas circunstancias: Resultado de una prueba neuropsiquiátrica practicada a una niña en el contexto de un procedimiento judicial sobre su custodia se presentó un dibujo suyo en el que representaba a su familia. El dibujo proporciona información sobre el estado de ánimo de la niña y sus sentimientos con respecto a los diferentes miembros de su familia. Como tal, podría entrar en la categoría de «datos personales». En efecto, el dibujo revela información relativa a la niña (su estado de salud desde un punto de vista psiquiátrico) así como a, por ejemplo, los comportamientos de su padre y de su madre. En consecuencia, los padres pueden ejercer en este caso su derecho de acceso a esta información concreta.

Los Los datos de una «seudonimización» rastreable pueden considerarse información sobre personas físicas indirectamente identificables.

los **«datos anónimos»** pueden definirse como cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. **«Datos anonimizados»** serán, por lo tanto, los datos anónimos que con anterioridad se referían a una persona identificable, cuya identificación ya no es posible.

los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha informacion anónima, inclusive con fines estadísticos o de investigación.

- b) ***Tratamiento***: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (Art. 4.3 RGPD).

- c) ***Fichero:*** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica (art. 4.6).
- d) ***Responsable del tratamiento:*** la persona física o jurídica, autoridad publica, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento (art. 4.7).
- e) ***Encargado del tratamiento***: la persona física o jurídica, autoridad publica, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (art. 4.8).

Licitud del tratamiento

- Principios relativos al tratamiento (art. 5 rgpd)

(licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, Responsabilidad proactiva)

- PRINCPIO DE PROPORCIONALIDAD
- Base de legitimación (art. 6 rgpd)

(consentimiento, contrato, obligación legal, interés vital, misión en interés público, interés legítimo)

Principios relativos al tratamiento :

- **Principio de licitud, lealtad y transparencia:** los datos serán tratados de manera lícita, leal y transparente en relación con el interesado;

- **Principio de limitación de la finalidad**: serán recogidos con fines determinados, explícitos y legítimos, y no seran tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales;

- **P. de minimización de datos:** los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;

- **P. de exactitud:** los datos serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;

Este principio se encuentra desarrollado en la Ley Orgánica 3/2018, de Protección de Datos Personales y garantías de los derechos digitales, con el siguiente tenor:

«Artículo 4. Exactitud de los datos

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1 d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que éste haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

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

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

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

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

- **P. de limitación del plazo de conservación:** los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante el tiempo necesario para los fines del tratamiento. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado;

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

El deber de confidencialidad está desarrollado en el art. 5 de la LOPDGDD

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

- **P. de responsabilidad proactiva:** el responsable del tratamiento será responsable del cumplimiento de estos principios y capaz de demostrarlo.

- **P. de responsabilidad proactiva:** el responsable del tratamiento será responsable del cumplimiento de estos principios y capaz de demostrarlo.

Una de las novedades más relevantes del Reglamento 2016/679, General de Protección de Datos (RGPD) es la inclusión del principio de responsabilidad proactiva. Se encuentra recogido en el apartado segundo del artículo 5 y establece que el responsable del tratamiento será responsable del cumplimiento de los principios relativos al tratamiento (art. 5.1) y capaz de demostrarlo.

Este principio se encuentra desarrollado en el artículo 24 del RGPD y en los artículos 28 y siguientes de la LOPDGDD al establecer la obligación general del responsable del tratamiento de aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. El principio de responsabilidad proactiva supone un cambio de paradigma que exige pasar de un sistema de protección reactivo frente al incumplimiento a un modelo preventivo y proactivo

Para el GT29, este principio cuenta con dos elementos principales:

"i) la necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos;

ii) la necesidad de demostrar, si así se requiere, que se han adoptado medidas adecuadas y eficaces; así pues, el responsable del tratamiento de datos deberá aportar pruebas de (i)."

El GT29 considera que, por ejemplo, se podrían aplicar las siguientes medidas:

- medidas revisión interna, evaluación, establecimiento de políticas escritas y vinculantes de protección de datos para asegurar el cumplimiento de los criterios de calidad de datos;
- establecimiento de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento;
- nombramiento de un delegado de protección de datos
- realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas;
- formación a los miembros del personal, en especial a los directores de recursos humanos y a los administradores de tecnologías de la información;
- establecimiento de un mecanismo interno de tratamiento de quejas;

- **h) Principio de proporcionalidad:** El derecho a la protección de datos personales es un derecho fundamental, que si bien no es absoluto y podrá ser limitado, su limitación para garantizar otros intereses dignos de protección deberá ser proporcionada. Por lo tanto, será necesario que exista una relación de proporcionalidad entre la finalidad legítima perseguida por el responsable del tratamiento y la medida restrictiva de dicho derecho.

- Este principio se encuentra expresamente recogido en el artículo 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea: *"Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás."*

- **Requisitos que exige la doctrina del TC:**

1. *Que tal medida sea susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**);*
2. *Además, debe ser necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**);*
3. *Finalmente, que la medida sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto**)"* .

Licitud del tratamiento

- La licitud del tratamiento de los datos personales vendrá determinada por una doble exigencia:

1. respetar los principios relativos al tratamiento, y
2. contar con una base de legitimación adecuada para ese tratamiento.

Las bases de legitimación

(artículo 6.1 rgpd) El tratamiento solo será lícito en los siguientes casos:

- a) Cuando el interesado haya dado su consentimiento para uno o varios fines específicos;
- b) Si el tratamiento es necesario para la ejecución de un contrato o precontrato
- c) Si el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) Cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física;
- e) Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- f) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Esta excepción no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

¿Cómo ha de prestarse el consentimiento?

- El Reglamento lo define como "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". **Esto significa que no se admiten formas de consentimiento tácito o por omisión o basadas en la inacción.**

- En determinados casos el consentimiento, además de inequívoco, ha de ser ***explícito***:
  - Tratamiento de datos sensibles.
  - Adopción de decisiones automatizadas.
  - Transferencias internacionales.

- El consentimiento ***puede ser inequívoco y otorgarse de forma implícita*** cuando se deduzca de una acción del interesado. Por ejemplo, me coloco para salir en una fotografía institucional.

- 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.

- El consentimiento será revocable en cualquier momento.

El consentimiento de los menores de edad:

- En relación con la oferta directa a niños de servicios de la sociedad de la información, el consentimiento

  - Se considerará válido cuando tenga como mínimo 16 años.
  - Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

- Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

El consentimiento de los menores de edad está regulado en el art. 7 de la LOPDGDD

- El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.
- Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.
- El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Ejemplos:

1. Interés legítimo: cesión datos sobre calificaciones a padres cuando los hijos dependan económicamente de ellos; cesión de imágenes del aparcamiento de la universidad a un particular siempre que la finalidad de la comunicación de datos no sea otra que la de su presentación en juicio

2. Consentimiento: comunicación de datos de alumnos o egresados a empresas que pretenden contratarlos.

3. Cumplimiento de un acuerdo de colaboración y el interés público (prácticas curriculares) o el consentimiento (por ejemplo prácticas extracurriculares): comunicación a una institución o empresa para que el alumnado realice prácticas.

4. Obligación legal: PRL, S. Social, hacienda, a juzgados y tribunales previo mandamiento judicial...

5. **Puede haber más de una base de legitimación.**

Los datos sensibles

- Artículos 9 y 10 del RGPD

Categorías especiales de datos

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

Excepciones:

- a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

- 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, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

- 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 y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, 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 en relación con sus fines y siempre que los datos personales 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, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

- g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

- h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

- 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, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

- j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

- 3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

- **Artículo 9 LOPDGDD. Categorías especiales de datos**

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

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

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

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

- Tratamiento de datos relativos a infracciones y sanciones penales: autoridades públicas competentes en los términos que establezca la ley

Derechos del interesado :

- 1. **Transparencia de la información:** Toda la información a los interesados, tanto respecto a las condiciones del tratamiento como cuando ejerza sus derechos, deberá proporcionarse de 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.
  - Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

Art. 13

Si los datos se obtienen directamente del interesado, habrá de facilitársele la siguiente información:

- la identidad y los datos de contacto del responsable (o de su representante);
- los datos de contacto del delegado de protección de datos, si lo hubiera;
- los fines y la base jurídica del tratamiento. Si el tratamiento se basa en un interés legítimo del responsable o de un tercero, deberá informarle de ese extremo;
- sobre los destinatarios de los datos personales o si se va a realizar una transferencia internacional;
- el plazo durante el cual se conservarán los datos personales o, si no fuera posible conocerlo, los criterios utilizados para determinar este plazo;
- que tiene derecho a acceder, rectificar, suprimir sus datos personales de acuerdo con lo dispuesto en el RGPD. Asimismo, que tienen derecho a la limitación de su tratamiento, o a oponerse al mismo y a la portabilidad de los datos;
- que tiene derecho a retirar el consentimiento en cualquier momento, sin que ello produzca efectos retroactivos;
- que tiene derecho a presentar una reclamación ante una autoridad de control;
-de si es obligatorio o no facilitar los datos y de las consecuencias de la negativa a facilitarlos cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato;
-de la existencia de decisiones automatizas, incluida la elaboración de perfiles.

- Cuando los datos no se obtengan del interesado, deberá informarle de todas las cuestiones anteriores y además de las categorías de datos que se traten y de *la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público* (art. 14).

Derechos de acceso, rectificación, supresión y oposición (derechos arco)

- **Dº de ACCESO**: Cuando ejercite su derecho de acceso, el responsable del tratamiento deberá confirmarle, en primer lugar, si se están o no tratando sus datos. Si los está tratando deberá proporcionarle el acceso a sus datos y a la información sobre su tratamiento.

- Deberá informarle sobre: los fines del tratamiento; las categorías de datos personales; los destinatarios, en particular destinatarios en terceros países u organizaciones internacionales;, el plazo previsto de conservación o, de no ser posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar la rectificación o supresión o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; si los datos personales no se han obtenido del interesado, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22 (art.15 RGPD).

- **Derecho de rectificación:**

Como en el caso del derecho anterior, el derecho de rectificación se encuentra expresamente mencionado en el artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea. Está recogido en el artículo 16 del RGPD, que establece que *"el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional."* Se trata de que, una vez identificado el dato erróneo, el dato se corrija, se actualice o se complete para que responda a la realidad de su titular. Este derecho se encuentra íntimamente relacionado con el principio de exactitud del art. 5 RGPD.

4. Derecho de supresión o derecho al olvido:

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

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

2. El interesado retire el consentimiento y este no se base en otro fundamento jurídico;

3. el interesado se oponga al tratamiento;

4. los datos personales hayan sido tratados ilícitamente;

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

6. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Cuando se hayan hecho públicos los datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o replica de los mismos.

No procederá la supresión de los datos cuando el tratamiento sea necesario:

1. Para ejercer el derecho a la libertad de expresión e información;
2. para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
3. por razones de interés público en el ámbito de la salud pública;
4. con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
5. para la formulación, el ejercicio o la defensa de reclamaciones.

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

- 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.

5. Derecho a la limitación del tratamiento

La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Se puede solicitar en los siguientes casos:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a la portabilidad de los datos :

- 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.

- Podrá ejercerse:
  - Cuando el tratamiento se efectúe por medios automatizados;
  - Cuando el tratamiento se base en el consentimiento o en un contrato;
  - Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

Derecho de oposición: En el art. 21 se garantiza el derecho del interesado a oponerse al tratamiento de sus datos en varios supuestos.

1. En primer lugar, por motivos relacionados con la situación particular del interesado cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 6.1.e del RGPD) o cuando el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (art. 6.1.f del RGPD), incluida la elaboración de perfiles sobre la base de dichas disposiciones. En este caso, el derecho de oposición no es un derecho absoluto ya que, en este caso, el responsable del fichero podrá seguir tratando los datos cuando acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. No obstante, es importante tener en cuenta que en el considerando 69 de RGPD señala que deberá *ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.*

2. En segundo lugar, por motivos relacionados con la situación particular, podrá oponerse al tratamiento de sus datos personales con fines de investigación científica o histórica o fines estadísticos de acuerdo con lo establecido en el art. 89.1 del RGPD, salvo que el tratamiento *sea necesario para el cumplimiento de una misión realizada por razones de interés público*.

3. En tercer lugar, podrá oponerse al tratamiento de datos con fines de mercadotecnia directa, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Decisiones individuales automatizadas, incluida la elaboración de perfiles

- Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, savo en los siguientes casos:
  - si la decisión es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
  - Si está autorizada por el Derecho de la Unión o de los Estados miembros y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
  - Si se basa en el consentimiento explícito del interesado.

- El responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

- Derechos del interesado:
  - A la información del artículo 13 y 14 sobre la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, **al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.** También cuando se ejercite el derecho de acceso.
- **Derechos previstos en el art. 22:**
  - derecho a obtener intervención humana por parte del responsable,
  - a expresar su punto de vista
  - a impugnar la decisión.
- Como regla general no se podrán utilizar datos sensibles

Procedimiento para el ejercicio de los derechos:

- Será gratuito, salvo cuando el interesado formule solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas. Estos casos el responsable podrá cobrar un canon que compense los costes administrativos o negarse a actuar.

- El responsable del tratamiento debe facilitar al interesado el ejercicio de sus derechos de forma fácil, sencilla y accesible, incluso a través de medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

- **PLAZO:** El responsable deberá informar al interesado su petición en el plazo de **un mes** (dos meses más si se trata de trate de solicitudes especialmente complejas, debiendo notificar esta ampliación dentro del primer mes).

- Si el responsable decide no atender una solicitud, también deberá informar de ello, motivando su negativa, dentro del plazo de **un mes** desde su presentación.

Los derechos del interesado podrán limitarse por las siguientes razones:

- La seguridad del Estado; la defensa o la seguridad pública;
- la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
- Otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
- La protección de la independencia judicial y de los procedimientos judiciales;
- La prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
- La función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública;
- la protección del interesado o de los derechos y libertades de otros;
- la ejecución de demandas civiles.

EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

- El RGPD distingue dos figuras diferentes en la utilización de los datos personales, por una parte el responsable y por otra el encargado del tratamiento. *Responsable del fichero* es la persona física o jurídica, de naturaleza pública o privada u órgano administrativo que *solo o junto con otros, determine los fines y medios del tratamiento*. Es la persona que dirige y controla los ficheros de datos personales y cada una de la operaciones y tratamientos a las que son sometidos. El *encargado del tratamiento* es quien trata los datos personales por cuenta del responsable del tratamiento. También puede ser una persona física o jurídica, autoridad pública, servicio u organismo y es indiferente que el tratamiento de datos lo realice en exclusiva o conjuntamente con otros encargados del tratamiento.

- Tanto el responsable como el encargado del tratamiento están obligados por todas y cada una de las disposiciones del RGPD. Muchos de estos deberes se deducen del contenido de los derechos de los afectados, pero otros han sido expresamente regulados en el Reglamento y alguno de ellos se encuentra recogido en la vigente LOPD y sigue siendo aplicable.

Obligaciones del responsable y del encargado del tratamiento:

- En el RGPD se establecen obligaciones específicas para los encargados del tratamiento. Entre otras: mantener un registro de actividades de tratamiento, determinar las medidas de seguridad aplicables a los tratamientos que realizan o designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

El responsable del tratamiento:

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

Dichas medidas se revisarán y actualizarán cuando sea necesario. (PRINCIPIO DE RESPONSABLIDAD PROACTIVA)

- El RGPD describe este principio como la necesidad de que el responsable del ***tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento***.

- En términos prácticos, este principio requiere que las organizaciones analicen ***qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo***. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

- En síntesis, ***este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones*** frente a todos los tratamientos de datos personales que lleven a cabo.

(FUENTE: GUÍA PROTECCIÓN DE DATOS UE: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS)

Análisis de riesgo:

- El RGPD ***condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados***.

- Los responsables del tratamiento deben realizar una ***una valoración del riesgo*** de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

- **(FUENTE: GUÍA PROTECCIÓN DE DATOS UE: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS)**

- La adhesión a códigos de conducta o a un mecanismo de certificación, aprobados según lo establecido en el RGPD podrán, ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

PRINCIPIO DE NEUTRALIDAD TECNOLÓGICA

- El principio de neutralidad de la tecnología surge para contrarrestar el desequilibrio existente entre el usuario de los productos tecnológicos, que no tiene conocimientos específicos, y los responsables de la tecnología, que predisponen los sistemas de tratamiento de datos personales. Si la tecnología no es neutra, es decir, condiciona la autonomía de su destinatario e impone *"formas onerosas de ejercer los derechos (...), se convierte en un factor de dominación".* El principio de neutralidad está íntimamente conectado con los principios de privacidad desde el diseño y por defecto, ya que lo que se requiere es una mayor responsabilidad en la planificación y el diseño tecnológico para garantizar el derecho a la vida privada de los usuarios de esa tecnología. A través de este principio se trataría de contrarrestar la técnica contraria, tan común en muchos servicios de Internet que consiste en *"deshabilitar al máximo la privacidad de las aplicaciones por sus titulares".*

Protección de datos desde el diseño y por defecto

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

- **El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.** Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

- Podrá utilizarse un mecanismo de certificación según lo establecido en el RGPD como elemento que acredite el cumplimiento de estas obligaciones.

Registro de las actividades de tratamiento

- Cada responsable y cada encargado del tratamiento llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.
- No estarán obligadas las empresas u organizaciones que empleen a menos de 250 personas, salvo que el tratamiento pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos (datos sensibles).

Cooperación con la autoridad de control

- Los responsables y los encargados del tramiento deberán cooperar con la Autoridad de control (Agencia Española de Protección de Datos)

Seguridad del tratamiento :

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

- Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- La adhesión a un código de conducta o a un mecanismo de certificación podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

- En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

- El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

NOMBRAR A UN REPRESENTANTE

- El responsable del tratamiento tiene asimismo el deber de nombrar un representante en la Unión Europea cuando no esté establecido en la Unión Europea.

Evaluación de impacto relativa a la protección de datos

- Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

Nombramiento obligatorio de un Delegado de protección de datos para :

- Autoridades y organismos públicos
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles

LA AUTORIDAD DE CONTROL: LA AEPD

- Art. 51 RGPD:
- Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.
- 2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.
- La AEPD está regulada en los artículos 44 y siguientes de la LOPDGDD.