

Glosario de definiciones del RGPD

- **Estado:** Redacción actual **VIGENTE**
- **Orden:** Administrativo
- **Fecha última revisión:** 18/01/2019

El [RGPD](#) proporciona -en su artículo 4- la definición de los conceptos sobre los que gravita la regulación de la protección de datos de carácter personal.

Así, los distintos operadores jurídicos, la ciudadanía, los poderes públicos, tienen a su alcance una definición "ex lege" de lo que podemos considerar "conceptos esenciales" de la norma y cuyo significado resulta necesario comprender tanto para conocer el alcance de los derechos que el [RGPD](#) reconoce a los interesados, como para cumplir adecuadamente con las obligaciones que el Reglamento impone.

Pues bien, tomado como referencia el orden establecido en el citado precepto citado, a continuación reproduciremos las definiciones establecidas en el Reglamento realizando -en su caso- la debida reseña a los considerandos relacionados con los términos que son objeto de definición por la norma. Atendiendo a lo dispuesto en el artículo 4 se entenderá por:

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

El contenido de esta definición, debe ser puesto en relación con el considerando 26 por cuanto que desarrolla determinados aspectos asociados al proceso de identificación. Así, en este considerando establece que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.

Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.

Conforme se señala en el considerando 26, para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por tanto, 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 información anónima, inclusive con fines estadísticos o de investigación.

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

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

Atendiendo al contenido del considerando 67, entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet.

En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

4) **«elaboración de perfiles»:** toda forma de tratamiento automatizado de datos personales consistente en utilizar

datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

Como señala el considerando 30, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas. Por ello, la evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas.

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

En relación con este concepto, debemos atender a lo dispuesto en el considerando 28 por cuanto que concibe la seudonimización como una medida que puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos a los datos personales. No obstante, el citado considerando indica que la inclusión expresa de esta medida en el Reglamento, no pretende excluir ninguna otra medida relativa a la protección de los datos

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

En relación con este término, resulta preciso atender al criterio del Tribunal Supremo -expuesto en la Sentencia de fecha 19 de septiembre de 2008- que ha sido claro al señalar que la pura acumulación de datos que comporte una búsqueda, acceso e identificación muy complicada no puede ser considerado “fichero” a los efectos que nos ocupan. Debemos entender en consecuencia que, como determina el Alto Tribunal, cabe apreciar la existencia de un fichero cuando el conjunto de datos esté apriorísticamente definido por el responsable del fichero, de forma que permita hablar de una estructuración conforme a criterios específicos relativos a las personas.

7) **«responsable del tratamiento» o «responsable»**: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;*

En virtud 26 del [RGPD](#) cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento.

Asimismo, los corresponsables deberán determinar de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos.

Independientemente de los términos del acuerdo a que se refiere el apartado 1 del artículo 26, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

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

Conforme determina el considerando 81, para garantizar el cumplimiento de las disposiciones del Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, deberá recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos de la [RGPD](#), incluida la seguridad del tratamiento.

9) **«destinatario»**: *la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que 4.5.2016 ES Diario Oficial de la Unión Europea L 119/33 puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los*

fin del tratamiento;

Como se indica en el considerando 31 las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial -como por ejemplo, las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores-, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros.

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

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

Sin perjuicio del análisis más pormenorizado que posteriormente realizaremos sobre el consentimiento, es preciso cabe señalar que -atendiendo al considerando 32- este puede manifestarse como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Ahora bien, debemos entender que en el caso de que el consentimiento sea prestado verbalmente resultará necesario articular un mecanismo que permita al responsable acreditar la existencia del mismo.

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

Las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por ello, en el caso de que se produzca una violación de la seguridad en los términos definidos en el artículo 4, el responsable del tratamiento deberá de proceder a comunicar tal circunstancia a la autoridad de control competente y al interesado.

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

El considerando 34 resulta coincidente con la definición que proporciona el artículo 4, ahora bien el citado considerando concreta diferentes medios de obtención de este tipo de datos, refiriéndose al análisis cromosómico, análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

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

Atendiendo a la definición reproducida, resulta necesario señalar que -conforme dispone el considerando 51- las fotografías únicamente se considerarán comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. .

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

Entre los datos personales relativos a la salud se deben considerar incluidos todos los datos relativos al estado de salud del interesado que den información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la [Directiva 2011/24/UE](#) del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

16) «establecimiento principal»:

1. a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;
2. b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

Conforme se determina en el considerando 36, el establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal.

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

La designación del representante no afecta a la responsabilidad del responsable o del encargado en virtud del Reglamento. Así, atendiendo a lo dispuesto en el considerando 80, dicho representante debe desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento.

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

La determinación de la empresa que ejerce el control, se realizará mediante la identificación de aquella que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Por ello, una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

Debemos señalar que el citado artículo 51 define y configura como una autoridad pública independiente, cuya función principal será supervisar la aplicación del 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.

Por otra parte, en virtud de lo dispuesto en el artículo 56, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

Sin perjuicio de lo señalado, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro. Ahora bien, es estos casos la autoridad de control que conozca de la reclamación deberá de informar sin dilación al respecto a la autoridad de control principal.

22) **«autoridad de control interesada»**: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

- a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
- b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento,
- o c) se ha presentado una reclamación ante esa autoridad de control;

Atendiendo a lo dispuesto en el considerando 38, en los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el Reglamento.

En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Por otra parte, en aquellos supuestos en los que el tratamiento sea efectuado por un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

23) **«tratamiento transfronterizo»**:

- a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro,
- o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) **«objeción pertinente y motivada»**: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

El termino aquí definido se configura como una suerte de “alegaciones” que pudiera ser planteada por diversos actores (autoridad de control interesada por ejemplo) frente a lo que podríamos considerar como una propuesta de resolución que implique la adopción de algún tipo de medida relativa a un responsable o un encargado del tratamiento, así se deduce de lo dispuesto en los artículo 60 y 64 del RGPD

25) **«servicio de la sociedad de la información»**: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo.

La Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, tiene por objeto establecer un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

26) **«organización internacional»**: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Como hemos visto, el Reglamento delimita numerosos conceptos que - por su trascendencia - es preciso conocer. Si bien, muchos de los términos incluidos en el prolijo listado del artículo 4 se encontraban anteriormente contemplados en la normativa derogada y en la [LOPD](#), ello en modo alguno puede llevarnos a obviar el detallado glosario que nos facilita el nuevo Reglamento por cuanto que el legislador además de redefinir y delimitar algunos conceptos, ha procedido a incorporar nuevas definiciones -como sucede por ejemplo con los datos genéticos o datos biométricos- que sin duda alguna deberán ser tenidos en cuenta para afrontar los desafíos prácticos que impone el uso de nuevas tecnologías.

Además de todas estas definiciones, la AEPD en la "guía para el ciudadano" incluye algunos otros términos y

definiciones que creemos conveniente traer a colación, tales como:

1. **Privacidad por diseño:** Adopción de medidas técnicas y organizativas cuya finalidad es aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento de los datos.
2. **Privacidad por defecto:** Adopción de medidas técnicas y organizativas cuya finalidad es garantizar que por defecto sólo se traten aquellos datos que sean necesarios para los fines del tratamiento.
3. **Evaluación de impacto relativa a la protección de datos:** Análisis de carácter previo de aquellos tratamientos de datos que puedan suponer un alto riesgo para los derechos y libertades de las personas.
4. **Elaboración de perfiles:** Toda forma de tratamiento automatizado de datos personales consistente en utilizar los datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona.
5. **Seudonimización:** El tratamiento de datos personales de tal manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.