aura portal

GDPR

La GDPR (Reglamento General de Protección de Datos) es un marco legal de protección de datos común en la Unión Europea que entrará en vigor a partir del 25 de mayo de 2018.

ÍNDICE

¿Qué es la GDPR y quién está obligado a su cumplimiento?

El 27 de Abril de 2016 se publicó el reglamento 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.

El objeto de dicho reglamento es la protección de los datos de carácter personal de todos los ciudadanos europeos y entrará en vigor el 25 de Mayo de 2018. Este reglamento 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".

En cuanto al ámbito territorial, conforme al artículo 3 el reglamento se aplica "al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no", en el caso de bienes o servicios y el del control del comportamiento del usuario, esta regulación será de aplicación siempre que los datos personales sean de un residente en la Unión independientemente del lugar de establecimiento del responsable o encargado de esos datos.

Así pues, en resumen, si usted trata datos de residentes en la Unión Europea debe cumplir los requisitos de esta regulación.

¿Cuáles son las obligaciones para cumplir la regulación?

Se establece que el uso de los datos debe ser lícito, leal y transparente en relación al interesado y se debe recoger con fines explícitos y legítimos, no permitiéndose el tratamiento ulterior de forma incompatible con esos principios. Los datos deben ser pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. También debe permitir la rectificación y supresión de los datos inexactos.

Debe mantenerse estos datos de forma que no sea posible la identificación de los interesados tras el tratamiento de estos datos conforme a los fines para los que fueron recabados y debe garantizar la seguridad de estos datos para evitar el tratamiento no autorizado o ilícito y su pérdida, destrucción o daño accidental.

Garantizar el uso lícito y transparente de los datos

Para que el tratamiento sea lícito es necesario que se cumpla, al menos, una de estas condiciones:

A. Que el interesado dé su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

B. Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación a petición de éste de medidas precontractuales.

C. Que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

D. Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

E. Que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

F. Que 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. Algunos de estos puntos son de aplicación para las administraciones públicas y FFCCSE.

En el caso de una empresa la forma habitual será el punto A, es decir, será necesario recabar el "consentimiento informado" y **es importante que pueda demostrar este consentimiento**.

Recomendación: revisar los contratos que actualmente tengan vigentes tanto con proveedores como con clientes para modificarlos e incluir ese "consentimiento informado".

Tenga en cuenta que el consentimiento, si forma parte de un contrato más amplio debe poderse distinguir claramente del resto del contrato, y retirar el consentimiento debe ser tan sencillo como darlo, sin afectar al tratamiento realizado previamente al consentimiento.

Si tiene que tratar datos relativos a condenas e infracciones penales "sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados".

Queda prohibido "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" aunque la regulación establece algunas circunstancias en las que esta prohibición no será de aplicación.

Para asegurar el tratamiento transparente para el interesado es necesario cumplir estas condiciones:

Deberá facilitar al interesado, como responsable del tratamiento, en el momento de la obtención de sus datos la siguiente información:

- Su identidad y sus datos de contacto o de su representante.

- Los datos de contacto del delegado de protección de datos.

- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.

- En caso de recabar los datos para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, en particular cuando el interesado sea un niño, deberá comunicar los intereses legítimos del responsable o del tercero.

- Los destinatarios o las categorías de destinatarios de los datos personales.

- Si procede, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión.

- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar ese plazo.

- La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.

- Cuando el interesado haya dado su consentimiento para uno o varios fines

específicos, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

• El derecho a presentar una reclamación ante una autoridad de control.

• Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos.

• La existencia de decisiones automatizadas, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos en el interesado. Al menos en tales casos, deberá proporcionar información significativa sobre la lógica aplicada en la automatización, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En caso de obtener los datos de una fuente diferente al interesado, deberá facilitar la siguiente información, además de la información anterior que proceda:

• Las categorías de datos personales que se traten.

• La fuente de la que proceden los datos personales, y en su caso, si proceden de fuentes de acceso público.

En caso de un tratamiento posterior de los datos para un fin distinto de aquel para el que fueron recogidos será necesaria la comunicación previa al interesado.

Garantizar el acceso, rectificación y supresión a los datos de carácter personal

El interesado tiene derecho a obtener de usted, como responsable del tratamiento de sus datos, la confirmación de este tratamiento y el acceso a sus datos personales y a la siguiente información:

• Los fines del tratamiento.

• Las categorías de datos personales de que se trate.

• Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales.

• Si es posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

• La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.

• El derecho a presentar una reclamación ante una autoridad de control.

• Cuando los datos personales no se hayan obtenido del interesado, deberá facilitarse cualquier información disponible sobre su origen.

• La existencia de decisiones automatizadas, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos en el interesado. Al menos en tales casos, deberá proporcionar información significativa sobre la lógica aplicada en la automatización, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En caso de solicitar el interesado la rectificación o supresión de sus datos personales deberá realizar la misma sin “dilación indebida”.

El responsable del tratamiento deberá suprimir los datos en los siguientes casos:

- Cuando ya no sean necesarios para el fin para el cual fueron recogidos.
- Cuando el interesado retire el consentimiento.

- Cuando el interesado se oponga al tratamiento de los datos, posibilidad que le deberá ser informada en el momento de la primera comunicación.

- En caso de uso ilícito de los datos personales.

Deberá limitar el tratamiento de los datos cuando el interesado impugne su exactitud, hasta que verifique la rectificación; cuando el tratamiento sea ilícito, pero el interesado se oponga a la supresión de los mismos y solicite su limitación; cuando ya no sean datos necesarios para usted, pero si lo sean para que el interesado pueda reclamar.

En el caso de que el interesado se oponga al tratamiento de los datos, pero haya discrepancia sobre el uso por parte de usted, en ese caso deberá limitar su uso mientras se resuelve la discrepancia.

En caso de limitar el uso de los datos, sólo podrán ser objeto de tratamiento con el "consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro" exceptuando el tratamiento para su conservación.

Como responsable del tratamiento deberá comunicar "cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada" que el interesado haya solicitado "a cada uno de los destinatarios a los que se haya comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado", y en caso de que el interesado solicite información sobre los destinatarios a los que se haya enviado sus datos personales deberá proporcionársela.
El interesado tiene derecho a la portabilidad de sus datos a otra compañía, sin perjuicio de su derecho a la supresión de los mismos y siempre que no afecte negativamente a los derechos y libertades de otros.

Responsable del tratamiento y encargado del tratamiento. Delegado de Protección de Datos (DPO).

Como responsable del tratamiento está obligado a aplicar medidas técnicas y organizativas para garantizar y demostrar que el tratamiento de los datos y su seguridad es conforme al reglamento, en ese sentido debe nombrar un encargado del tratamiento, que puede ser una persona física o jurídica, autoridad pública, servicio u otro organismo.

Dicho encargado debe ofrecer garantías suficientes respecto a la implementación y el mantenimiento de las medidas técnicas y organizativas apropiadas.
Para demostrar que el encargado ofrece esas garantías puede servir como mecanismo de prueba la adhesión a códigos de conductas o la posesión de un certificado de protección de datos.

Este encargado puede ser personal de su empresa o personal externo, pero es obligatorio el establecer un contrato o acto jurídico que vincule al encargado respecto al responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Es necesario que dicho contrato estipule, en particular, que el encargado:

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

B. Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad.

C. Tomará todas las medidas necesarias a la seguridad en el tratamiento de la información.

D. En caso de tener que recurrir a otro encargado deberá comunicarlo al responsable que podrá oponerse o autorizar por escrito ese recurso. Entre ambos encargados debe haber un contrato u acto jurídico similar al existente entre responsable y encargado.

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

F. Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas.

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

H. Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el reglamento, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. En caso de recibir una instrucción contraria al reglamento deberá informar inmediatamente al responsable.

Como responsable del tratamiento de datos, debe llevar un registro de los tratamientos efectuados bajo su responsabilidad si su empresa es de más de 250 empleados o "el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales".

Dicho registro debe contener la siguiente información:

- Nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.

- Los fines del tratamiento.

- Una descripción de las categorías de interesados y de las categorías de datos personales.

- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

- En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida

la identificación de dicho tercer país u organización internacional.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

- Nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos.

- Las categorías de tratamientos efectuados por cuenta de cada responsable.

- Las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Los registros constarán por escrito, inclusive en formato electrónico.

El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

El responsable y el encargado del tratamiento designarán un delegado de protección de datos o DPO conforme a sus siglas en inglés (Data Protection Officer) atendiendo a sus conocimientos de Derecho y a su práctica en materia de protección de datos y a su capacidad para desempeñar sus funciones.

Recomendación: aunque no es necesario que el delegado de protección de datos (DPO) sea jurista, sí debería poseer conocimientos de derecho y protección de datos.

En el caso de España la Agencia Española de Protección de Datos permite la certificación en caso de demostrar experiencia previa en materia de protección de datos y/o haber recibido con éxito una formación previa impartida por entidades reconocidas.

El delegado puede formar parte de la plantilla o desempeñar sus funciones en el marco de un contrato de servicios.

El delegado de protección de datos (DPO) debe participar en todas las cuestiones relativas a la protección de datos personales y debe ser respaldado por el responsable y encargado del tratamiento de datos que garantizarán que el DPO no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones.

El delegado de protección de datos (DPO) podrá desempeñar otras funciones y cometidos y está obligado a mantener el secreto o confidencialidad en lo que respecta al desempeño de sus funciones. Realizará estas funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. El DPO no podrá ser destituido ni sancionado por desempeñar sus funciones y rendirá cuentas al nivel jerárquico más alto.

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

A. Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la GDPR y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

B. Supervisar el cumplimiento de lo dispuesto en la GDPR, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

C. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

D. Cooperar con la autoridad de control.

E. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

Seguridad del tratamiento

Respecto a la seguridad el reglamento demanda que se aplique las **medidas técnicas y organizativas** apropiadas para garantizar el nivel de seguridad adecuado. Estas medidas deben incluir:

- La **seudonimización** y el **cifrado** de datos personales.

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de 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.

Deberá tener en cuenta, al evaluar la adecuación del nivel de seguridad, los **riesgos** que presente el tratamiento de los datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Como en otras ocasiones la adhesión a un **código de conducta** o un mecanismo de **certificación** puede servir de elemento de prueba del cumplimiento del reglamento.

En caso de existir una violación de la seguridad de los datos se debe notificar a la autoridad de control competente en el plazo máximo de 72 horas después de que se haya tenido constancia de ella. Para ello es necesario que el encargado del tratamiento notifique "sin dilación indebida" al responsable del tratamiento.

La notificación a la autoridad de control competente deberá, como mínimo:

A. Describir la **naturaleza de la violación** de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

B. Comunicar el nombre y los datos de **contacto del delegado** de protección de datos o de otro punto de contacto en el que

pueda obtenerse más información.

C. Describir las posibles **consecuencias** de la violación de la seguridad de los datos personales.

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

En caso de no poder facilitar esa información en el primer momento, deberá facilitarla de manera gradual "sin dilación indebida".

Cuando la violación de la seguridad de los datos pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas es necesario comunicar al interesado, en un lenguaje claro y sencillo, y "sin dilación indebida" la naturaleza de la violación de seguridad y como mínimo el nombre y los datos de contacto del delegado de protección de datos, las posibles consecuencias de esta violación y describir las medidas adoptadas o propuestas para poner remedio a la violación.

Si comunica **en primer lugar a la autoridad de control**, esta puede obligarle a comunicarlo al interesado o decidir si se cumplen algunas de las condiciones que no hacen necesaria esa comunicación. Estas condiciones son:

A. Ya se han adoptado las medidas de protección a los datos afectados y son ininteligibles.

B. Se han tomado medidas ulteriores que garantizan que ya no existe probabilidad de que se concrete el alto riesgo para los derechos y libertades de las personas físicas.

C. La comunicación suponga un esfuerzo desproporcionado. En este caso se optará por una comunicación pública o semejante.

Conclusiones

Este nuevo reglamento de protección de datos establece un control mayor al tratamiento de datos y obliga a su protección. En el caso de existir una violación de seguridad se deberá notificar a la autoridad competente en un plazo máximo de 72 horas.

Además se establece una nueva figura que es el delegado de protección de datos (DPO) que tiene como obligación la supervisión del cumplimiento de las obligaciones relacionadas con la protección de los datos personales.

Desde **AuraPortal** podemos ayudarle al cumplimiento de la GDPR automatizando sus procesos, estableciendo filtros de control sobre los datos tratados y junto con el uso del "Centro de Protección de Datos" centralizar la accesibilidad y gestión de todos los procesos relacionados con la regulación GDPR mediante un acceso único.

Definiciones

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.

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.

Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

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.

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.

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

Responsable del tratamiento: 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.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

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

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.

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.

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.

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.

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.

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.

Representante: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones.

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.

Grupo empresarial: grupo constituido por una empresa que ejerce el control y sus empresas controladas.

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.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro.

Autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que: el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; 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 se ha presentado una reclamación ante esa autoridad de control.

Objeción pertinente y motivada: la objeción a una propuesta de decisión sobre la existencia o no de infracción, o sobre la conformidad con el 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.

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 (1).

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.