# 1

# Reglamento Europeo de Protección de Datos

**CONTENIDO:**

Aproximación a la normativa europea de protección de datos

Introducción a los ámbitos de aplicación y definiciones

Definición de principios

Gestión de derechos del interesado y principios generales

Conocimiento de obligaciones del RF y RT

Aplicación de medidas de seguridad

**OBJETIVOS:**

Conocer el Reglamento Europeo destacando todos aquellos aspectos que pueden generar algún tipo de incidencia de acuerdo con la normativa y las obligaciones, derechos y responsabilidades existentes de cara al tratamiento de datos.

# 1. APROXIMACIÓN A LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS

## 1.1 Introducción

### A. ¿Qué se considera un dato personal?

Un dato personal es **cualquier información que permita identificar** a una persona física, directa o indirectamente. Esto puede incluir, pero no se limita a, nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, direcciones IP, datos de localización, identificadores en línea y datos de salud.

Ejemplo

- *Si una aplicación de seguimiento de la salud recoge información sobre el peso, la dieta y el nivel de actividad física de una persona, todos estos serían considerados datos personales.*

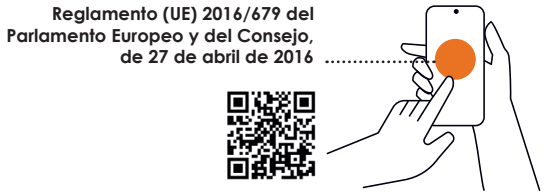
## B. ¿Qué significa el tratamiento de datos personales?

El tratamiento de datos personales se refiere a cualquier **operación o conjunto de operaciones** que se realizan sobre datos personales, ya sea por medios automatizados o no. Esto incluye 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.

Ejemplo

- *Si una organización recoge direcciones de correo electrónico para enviar un boletín informativo, está tratando datos personales. Del mismo modo, si una empresa utiliza un sistema automatizado para clasificar y organizar las solicitudes de servicio al cliente basándose en el contenido del mensaje, también está tratando datos personales.*

# 1.2 Nociones básicas del Reglamento (UE) 2016/679




## A. ¿Qué es?

El 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) o **RGPD**, es una norma que se aplica en todos los países de la Unión Europea (UE) y que tiene como **finalidad** principal proteger los datos personales de las personas físicas y garantizar su libre circulación. En este sentido, de acuerdo con el artículo 1 del Reglamento (UE) 2016/679, este tiene por **objeto**:

- Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
- Proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

> La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

El RGPD afecta a todas las organizaciones, tanto dentro como fuera de la UE, que tratan **datos personales de personas físicas en la UE**. Esto significa que, si una organización ofrece bienes o servicios a personas en la UE o monitoriza su comportamiento, debe cumplir con el RGPD, independientemente de su ubicación geográfica. Por ejemplo, si una empresa con sede en Argentina vende productos en línea y acepta pedidos de clientes en España, esa empresa tendría que cumplir con el RGPD en lo que respecta a los datos personales de sus clientes españoles.

La estructura del Reglamento (UE) 2016/679 es la siguiente:

| **REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL** |
|---|
| CAPÍTULO I. Disposiciones generales |
| CAPÍTULO II. Principios |
| CAPÍTULO III. Derechos del interesado |
| CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento |
| CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales |
| CAPÍTULO VI. Autoridades de control independientes |
| CAPÍTULO VII. Cooperación y coherencia |
| CAPÍTULO VIII. Recursos, responsabilidad y sanciones |
| CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento |
| CAPÍTULO X. Actos delegados y actos de ejecución |
| CAPÍTULO XI. Disposiciones finales |

## B. ¿Por qué es importante?

El Reglamento General de Protección de Datos (RGPD) es una norma de vital importancia en la era digital en la que vivimos. Su relevancia radica en varios aspectos que vamos a desarrollar a continuación.

> La protección de los datos personales es un derecho fundamental de todas las personas. El RGPD proporciona un marco para proteger estos derechos y garantizar que los datos personales se tratan de manera segura y respetando la privacidad de las personas.

### a. Derecho fundamental a la protección de datos

En primer lugar, la protección de los datos personales es un derecho fundamental reconocido por la Unión Europea. **Cada persona** tiene derecho a que sus datos personales sean tratados con respeto y seguridad. El RGPD proporciona un **marco legal** que protege este

derecho y establece las **obligaciones y responsabilidades** de las organizaciones que tratan datos personales.

El Reglamento (UE) 2016/679 se transpone en España a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ejemplo:

- *Si una persona se suscribe a un boletín informativo, tiene derecho a saber cómo se utilizarán sus datos, quién tendrá acceso a ellos y durante cuánto tiempo se conservarán. Además, tiene derecho a acceder a sus datos, rectificarlos si son incorrectos y solicitar su supresión cuando ya no sean necesarios para los fines para los que se recogieron.*

## b. Responsabilidad y transparencia

El RGPD introduce el principio de **responsabilidad proactiva**, que implica que las organizaciones deben ser capaces de demostrar que cumplen con el reglamento. Esto promueve una cultura de protección de datos y transparencia, ya que las organizaciones deben implementar medidas adecuadas para garantizar el cumplimiento del RGPD y ser capaces de demostrarlo.

Ejemplo:

- *Si una empresa utiliza un sistema de inteligencia artificial para tomar decisiones basadas en datos personales, debe ser capaz de explicar cómo funciona este sistema, qué datos utiliza y cómo garantiza que los datos se tratan de manera segura y respetando los derechos de las personas.*

### c. Libre circulación de datos

El RGPD también facilita la libre circulación de datos personales dentro de la UE, lo que es esencial para el funcionamiento del **mercado único digital**. Al establecer normas comunes para la protección de datos en todos los países de la UE, el RGPD elimina barreras y facilita las actividades comerciales y la prestación de servicios a través de las fronteras.

Ejemplo

- *Si una empresa con sede en España ofrece servicios en línea a clientes en Alemania, no tiene que preocuparse por cumplir con diferentes normas de protección de datos en cada país. En su lugar, puede centrarse en cumplir con el RGPD, que se aplica en toda la UE.*

### d. Protección frente a las amenazas de seguridad

En la era digital, los datos personales pueden ser un objetivo para actividades malintencionadas, como el robo de identidad, el fraude o los ataques cibernéticos. El RGPD establece **requisitos estrictos** en términos de seguridad de los datos personales y obliga a las organizaciones a implementar medidas adecuadas para proteger los datos contra estas amenazas.

Ejemplo

- *Si una empresa almacena datos de tarjetas de crédito de sus clientes, debe implementar medidas de seguridad como la encriptación y el control de acceso para proteger estos datos. Si se produce una violación de seguridad que afecta a los datos personales, la empresa debe notificarlo a la autoridad de protección de datos y, en algunos casos, a las personas afectadas.*

El RGPD es una norma esencial que protege los derechos fundamentales de las personas, promueve la transparencia y la responsabilidad, facilita la libre circulación de datos y protege contra las amenazas de seguridad en la era digital. Su cumplimiento no es solo una obligación legal, sino también una cuestión de respeto hacia las personas cuyos datos personales se tratan.

## C. Principios

El Reglamento General de Protección de Datos (RGPD) se basa en los siguientes principios fundamentales que son la piedra angular de esta norma y proporcionan un marco sólido para el tratamiento seguro y respetuoso de los datos personales:

**Licitud, lealtad y transparencia**: este principio establece que los datos personales deben ser tratados de manera lícita, leal y transparente. Esto significa que las organizaciones deben tener una base legal para tratar los datos personales, como el consentimiento de la persona, la ejecución de un contrato o el cumplimiento de una obligación legal. Además, las organizaciones deben informar a las

personas sobre cómo se tratan sus datos de manera clara y comprensible. Por ejemplo, si una tienda en línea recoge datos de tarjetas de crédito para procesar pagos, debe informar a sus clientes de este hecho y explicar cómo se protegen estos datos.

**Limitación de la finalidad**: los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines. Esto significa que las organizaciones deben ser claras sobre por qué necesitan los datos personales y no pueden usarlos para otros fines sin el consentimiento de la persona. Por ejemplo, si una empresa recoge direcciones de correo electrónico para enviar un boletín informativo, no puede usar estas direcciones para enviar publicidad a menos que las personas hayan dado su consentimiento para ello.

**Minimización de datos**: los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Esto significa que las organizaciones no deben recoger más datos de los necesarios para cumplir con su finalidad. Por ejemplo, si una aplicación de seguimiento de la salud recoge datos sobre la dieta y el nivel de actividad física de una persona, no debería recoger también datos sobre su origen étnico o sus creencias religiosas, ya que estos datos no son necesarios para su finalidad.

**Exactitud**: los datos personales deben ser exactos y, si fuera necesario, actualizados. Las organizaciones deben tomar medidas razonables para asegurarse de que los datos inexactos se rectifican o suprimen. Por ejemplo, si una persona se muda y cambia de dirección, la organización que tiene sus datos debe actualizar esta información en sus registros.

**Limitación del plazo de conservación**: los datos personales deben ser mantenidos de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines del tratamiento de los datos personales. Esto significa que las organizaciones deben eliminar o anonimizar los datos personales cuando ya no sean necesarios. Por ejemplo, si una empresa guarda los currículums de las personas que se han presentado a una oferta de trabajo, debe eliminar estos currículums una vez que el proceso de selección ha terminado y ya no son necesarios.

**Integridad y confidencialidad**: los datos personales deben ser tratados de tal manera que se garantice su seguridad adecuada. Las organizaciones deben implementar medidas técnicas y organizativas apropiadas para proteger los datos personales contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Por ejemplo, si una empresa almacena datos de tarjetas de crédito de sus clientes, debe implementar medidas de seguridad como la encriptación y el control de acceso para proteger estos datos.

**Responsabilidad proactiva**: el responsable del tratamiento será responsable del cumplimiento de los principios anteriores y deberá ser capaz de demostrarlo. Esto significa que las organizaciones deben implementar medidas adecuadas para garantizar el cumplimiento del RGPD y ser capaces de demostrarlo. Por ejemplo, una empresa podría implementar políticas de protección de datos, realizar evaluaciones de impacto de protección de datos y designar a un delegado de protección de datos para demostrar su cumplimiento con el RGPD.

# 2. INTRODUCCIÓN A LOS ÁMBITOS DE APLICACIÓN Y DEFINICIONES

## 2.1 Ámbito de aplicaciones

### A. Introducción

El Reglamento General de Protección de Datos (RGPD) tiene un amplio ámbito de aplicación:

- A nivel **geográfico**: el RGPD se aplica a todas las organizaciones que se encuentran dentro de la Unión Europea (UE). Pero su alcance va más allá de las fronteras de la UE. También se aplica a organizaciones fuera de la UE si ofrecen bienes o servicios a personas en la UE o si monitorizan su comportamiento. Por ejemplo, si una empresa con sede en México vende productos en línea a clientes en España, esa empresa tendría que cumplir con el RGPD en lo que respecta a los datos personales de sus clientes españoles. Esto significa que la empresa debe informar a sus clientes sobre cómo se tratan sus datos personales, obtener su consentimiento para hacerlo, y tomar medidas para proteger sus datos y garantizar su seguridad. Además, si una organización fuera de la UE monitoriza el comportamiento de las personas en la UE, también está sujeta al RGPD. Por ejemplo, si una empresa de tecnología con sede en Estados Unidos utiliza cookies para rastrear el comportamiento en línea de las personas en la UE con el fin de personalizar la publicidad, esa empresa también tendría que cumplir con el RGPD.
- A nivel **objetivo** (actividades reguladas): el RGPD se aplica a casi todas las actividades que implican el tratamiento de datos personales. Esto incluye la recogida, el almacenamiento, la utilización, la transmisión y la eliminación de datos personales. También se aplica tanto al tratamiento de datos personales por medios automatizados (como ordenadores) como no automatizados (como archivos de papel). Por ejemplo, si una biblioteca mantiene un registro de los libros que cada persona ha sacado, estaría tratando datos personales y tendría que cumplir con el RGPD. Esto significa que la biblioteca debe informar a las personas sobre cómo se tratan sus datos, obtener su consentimiento para hacerlo, y

tomar medidas para proteger sus datos y garantizar su seguridad. Además, si una empresa utiliza un sistema de inteligencia artificial para analizar los datos de los clientes y hacer recomendaciones personalizadas, también estaría tratando datos personales y tendría que cumplir con el RGPD. Esto significa que la empresa debe informar a los clientes sobre cómo se utilizan sus datos, obtener su consentimiento para hacerlo, y tomar medidas para proteger sus datos y garantizar su seguridad.

El RGPD tiene un amplio ámbito de aplicación y afecta a una amplia gama de actividades y organizaciones. Su objetivo es proteger los derechos y libertades fundamentales de las personas en relación con el tratamiento de sus datos personales y garantizar que estos datos se tratan de manera segura y respetando su privacidad.

## B. Ámbito de aplicación material

Según el artículo 2 del Reglamento (UE) 2016/679, el Reglamento **se aplica** a:

- El tratamiento **total o parcialmente automatizado** de datos personales.
- El tratamiento **no automatizado** de datos personales contenidos o destinados a incluirse en un fichero.

El Reglamento **no se aplica** al tratamiento de datos personales:

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.

b) Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE.

c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

d) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

De conformidad con lo dispuesto en su artículo 98, **se adaptarán** a los principios y normas del Reglamento (UE) 2016/679:

- El Reglamento (CE) n.o 45/2001, que es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión.
- Otros actos jurídicos de la Unión aplicables al tratamiento de datos de carácter personal.

El Reglamento (UE) 2016/679 se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

## C. Ámbito territorial

De acuerdo con el artículo 3 del Reglamento (UE) 2016/679, 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.
- De interesados que se encuentren en la Unión por parte de un responsable o encargado **no establecido en la Unión**, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o con el control de su comportamiento, en la medida en que este tenga lugar en la Unión.
- Por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros se aplique en virtud del **Derecho internacional público**.

# 2.2 Definiciones

Conforme a su artículo 4, a efectos del Reglamento (UE) 2016/679 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.
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.

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.

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.

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.

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.

Si una empresa decide recoger las direcciones de correo electrónico de sus clientes para enviarles un boletín informativo, esa empresa sería el responsable del tratamiento de esos datos personales. Si esa misma empresa contrata a un proveedor de servicios de nube para almacenar los datos de sus clientes, dicho proveedor de servicios de nube sería el encargado del tratamiento de esos datos personales.

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.

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 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.

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.

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.

13) «**Datos genéticos**»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que pro-

porcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

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.

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.

16)«**Establecimiento principal**»:

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.

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 Reglamento.

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 Reglamento.