General Data Protection Regulation

Parlamento Europeo y Consejo

Índice

Introducción

En abril de 2016 el Parlamento Europeo y el Consejo aprobaron un nuevo Reglamento relativo a protección de datos de personas físicas y a la libre circulación de estos datos

Introducción

La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la **protección de los datos personales**. En este sentido, se ha incrementado de manera significativa la magnitud de la recogida y del intercambio de datos personales, y en la actualidad la tecnología permite el tratamiento de los datos personales en una escala sin precedentes.

Estos avances requieren un **marco más sólido y coherente** para la protección de datos en la UE, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Así, surge la necesidad de que las personas físicas tengan el control de sus propios datos personales, y de reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

En este contexto, en **abril de 2016** el Parlamento Europeo y el Consejo aprobaron el **Reglamento (UE) 2016/679**[1], 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.

Algunos de los aspectos más relevantes que se incluyen en este Reglamento son los siguientes:

- Se incluyen nuevos **derechos de los interesados**. Entre otros, se les reconoce a las personas físicas el olvido, el derecho de acceso a los datos personales, el derecho a la portabilidad de los datos, etc.
- Se establece una serie de **obligaciones a los responsables y a los encargados** del tratamiento de los datos personales. Por ejemplo, deberán implementar medidas técnicas y organizativas de seguridad apropiadas.
- Se incrementa la supervisión del cumplimiento del marco normativo a través de la creación de **autoridades de control independientes** en cada Estado miembro, y a través de ciertos **recursos administrativos y judiciales**.

En esta nota técnica se analiza el **nuevo marco de protección de datos** definido por este Reglamento.

(1) También se aprobó en abril de 2016 la Directiva 2016/680, pero no será objeto de estudio dado que se refiere solo al tratamiento de datos por parte de autoridades competentes para fines de prevención, investigación o enjuiciamiento de infracciones penales.

Índice

Resumen ejecutivo

El nuevo Reglamento incluye, entre otros aspectos, principios relativos al tratamiento de los datos personales, derechos que ostentan los interesados o personas físicas, y las obligaciones del responsable y del encargado del tratamiento

Resumen ejecutivo

Ámbito de aplicación

- Protección del tratamiento de los datos personales de **personas físicas** o **interesados**.
- Aplica respecto a **responsables y encargados**[1] **establecidos en la UE**, y respecto a los no establecidos en la UE cuando el tratamiento de datos sea de **interesados que residan en la UE**.

Contexto normativo

- **Directiva 95/46/CE**, sobre protección de datos personales[2].

Próximos pasos

- El nuevo Reglamento será aplicable a partir del **25 de mayo de 2018**.

Contenido principal

- **Principios** (datos tratados de manera lícita, leal, trasparente, para fines adecuados, etc.)
- **Prohibición tratamiento de datos sensibles** (con excepciones)

- Derecho de **información**, de **acceso**, de **rectificación**, derecho **al olvido**, a la **limitación del tratamiento**, a la **portabilidad de los datos**, derecho de **oposición**, etc.

- **Autoridades de control independientes**
- **Comité Europeo de Protección de Datos**
- **Recursos y sanciones**
- Transferencia de datos **a terceros países**

- **Obligaciones generales** (ej. protección **“**desde el diseño y por defecto”)
- **Seguridad de los datos personales**
- **Evaluación de impacto**
- Delegado de protección de datos (**DPO**)
- **Códigos de conducta y certificación**

(1) En el anexo se incluye un listado de las definiciones más relevantes utilizadas a efectos del Reglamento (ej. responsable del tratamiento, encargado del tratamiento, etc.).

(2) Esta Directiva quedaría derogada una vez entre en vigor el nuevo Reglamento sobre protección de datos.

Resumen ejecutivo

Ámbito de aplicación

El Reglamento no solo se refiere a las actividades de responsables y encargados establecidos en la UE, sino que también resulta aplicable a aquellos de fuera de la UE cuando traten datos de interesados de la UE en relación a la oferta de bienes y servicios o control del comportamiento

Ámbito de aplicación

Ámbito de aplicación material

- El Reglamento se refiere a la **protección de las personas físicas** en lo que respecta al tratamiento de los datos personales. Por tanto, **no es aplicable a personas jurídicas**.
- 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**.

Excepciones

- El Reglamento **no se emplea** en el tratamiento de datos personales:
  - En el ejercicio de una actividad **fuera del ámbito de aplicación del Derecho de la UE**.
  - Por parte de los Estados miembros cuando lleven a cabo actividades relacionadas con la **política exterior y la seguridad nacional**.
  - Efectuado por una persona física en el ejercicio de **actividades exclusivamente personales o domésticas**.
  - Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de **infracciones penales**, o de ejecución de sanciones penales.

Ámbito de aplicación territorial

- 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 UE**.
  - De **interesados que residan en la UE** por parte de un responsable o encargado no establecido en la UE, cuando las actividades de tratamiento estén relacionadas con:
    - La oferta de bienes o servicios a dichos interesados en la UE.
    - El control de su comportamiento, en la medida en que éste tenga lugar en la UE.

Índice

Detalle

Principios relativos al tratamiento de los datos

En primer lugar, el Reglamento recoge una serie de principios relativos al tratamiento de los datos que deberá garantizar el responsable. Al respecto, es relevante el principio de licitud, que solo se verá cumplido si se da alguna de las condiciones previstas (ej. consentimiento)

Principios relativos al tratamiento de los datos (1/2)

Principios

- El responsable del tratamiento deberá garantizar que los datos personales son:
  - Tratados de **manera lícita, leal y transparente**.
  - Recopilados con **fines determinados**, **explícitos y legítimos**.
  - **Adecuados**, **pertinentes y limitados** a los fines para los que son tratados.
  - **Exactos** y, si fuera necesario, **actualizados**.
  - Mantenidos de forma que se permita la **identificación** de los interesados durante **no más tiempo del necesario**.
  - Tratados de tal manera que se garantice una **seguridad adecuada**.

Licitud

- El tratamiento solo será lícito si se cumple al menos **una de las siguientes condiciones**:
  - El interesado dio su **consentimiento**.
  - El tratamiento es **necesario** para:
    - La **ejecución de un contrato** en el que el interesado es parte, o para el cumplimiento de **una obligación legal** aplicable al responsable del tratamiento.
    - **Proteger intereses vitales** del interesado u otra persona física.
    - El cumplimiento de una misión realizada en **interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
    - La satisfacción de **intereses legítimos** del responsable del tratamiento o de un tercero[1].

Algunas de las condiciones para el consentimiento

- El responsable deberá ser **capaz de demostrar** que el interesado consintió el tratamiento de sus datos personales.
- El interesado tendrá **derecho a retirar su consentimiento** en cualquier momento, lo cuál no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.
- A la hora de evaluar si el consentimiento se ha dado **libremente**, se tendrá que tener en cuenta si la ejecución de un contrato se supedita al consentimiento en el tratamiento de datos personales no necesarios para la ejecución de dicho contrato.

Se incluyen condiciones específicas aplicables al **consentimiento del niño** (ej. mínimo 16 años, y si no lo deberán dar sus padres).

(1) Siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del interesado.

Detalle

Principios relativos al tratamiento de los datos

El Reglamento otorga una especial protección al tratamiento de datos sensibles (ej. datos relativos a origen étnico o racial, datos genéticos, etc.), quedando prohibido su tratamiento salvo en ciertas circunstancias, como cuando el interesado otorga consentimiento explícito

Principios relativos al tratamiento de los datos (2/2)

Prohibición tratamiento de datos sensibles

- 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.**
  - **Datos genéticos y 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.

Excepciones

- No obstante, lo anterior no será de aplicación cuando concurra, entre otras, **una de las siguientes circunstancias**:
  - El interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales.
  - 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.
  - El tratamiento es efectuado 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.
  - El tratamiento es necesario por razones de un **interés público esencial**.

Detalle

Derechos del interesado

El Reglamento establece también una serie de derechos que podrá ejercer el interesado. Así, en primer lugar, se le reconoce el derecho de información, por el cual el responsable del tratamiento deberá facilitar cierta información al interesado de manera concisa

Derechos del interesado (1/3)

Derecho de información

- El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado cierta información en forma **concisa**, **transparente**, **inteligible** y de **fácil acceso**. La información será facilitada **por escrito** o por otros medios (ej. medios electrónicos), pero si lo solicita el interesado puede facilitarse verbalmente.
- En concreto, la información que debe facilitar el responsable del tratamiento al interesado es la siguiente[1]:

Identidad y datos de contacto del responsable del tratamiento de datos	✓	✓
Datos de contacto del delegado de protección de datos	✓	✓
Fines del tratamiento de los datos	✓	✓
Las categorías de datos personales de que se trate	✗	✓
Los destinatarios o categorías de destinatarios de los datos personales	✓	✓
Intereses legítimos del responsable	✓	✓
Intención del responsable de transferir datos persales a un tercer país u organización internacional	✓	✓
Plazo de conservación de datos personales	✓	✓

Derecho de acceso al interesado	✓	✓
Derecho a la rectificación y supresión de los datos personales	✓	✓
Derecho a la limitación del tratamiento de datos	✓	✓
Derecho a la portabilidad de datos	✓	✓
Derecho de oposición	✓	✓
Derecho a retirar el consentimiento del interesado	✓	✓
Derecho de presentar una reclamación ante la autoridad control	✓	✓
Existencia de decisiones automatizadas, incluida la elaboración de perfiles	✓	✓
La fuente de la que proceden los datos personales	✗	✓

Cuando los datos se obtengan del interesado

Cuando los datos no se hayan obtenido del interesado

(1) En todo caso, deberá facilitarse a título gratuito. Por otro lado, no existe obligación de facilitar dicha información en ciertas circunstancias (ej. el interesado ya dispone de ella).

Detalle
Derechos del interesado

Asimismo, también se reconoce al interesado el derecho de acceso, el derecho de rectificación, el derecho al olvido, el derecho a la limitación del tratamiento…

Derechos del interesado (2/3)

Derecho de acceso

- El interesado tendrá derecho a obtener del responsable del tratamiento **confirmación de si se están tratando o no datos personales** que le conciernen y, en tal caso, **derecho de acceso** a los datos personales.
- El responsable del tratamiento facilitará una **copia de los datos personales** objeto de tratamiento.

Derecho de rectificación[1]

- El interesado tendrá derecho a obtener del responsable del tratamiento la **rectificación de los datos personales inexactos** que le afecten, y tendrá derecho a que se **completen los datos personales que sean incompletos**, inclusive mediante una declaración adicional.

Derecho al olvido (supresión)[1]

- El interesado tendrá derecho a obtener del responsable del tratamiento la **supresión de los datos personales** que le afecten. El responsable estará obligado a suprimir **sin dilación indebida** los datos personales cuando concurra **alguna de las circunstancias siguientes**:
  - Los datos personales ya **no son necesarios** en relación con los fines iniciales.
  - El interesado **retira el consentimiento**, o se opone al tratamiento.
  - Los datos personales han sido **tratados ilícitamente**.
  - Deben ser suprimidos para el cumplimiento de una **obligación legal**.
  - Los datos se han obtenido en relación con la oferta de **servicios de la sociedad de la información**.
- No obstante, existen ciertas **excepciones al derecho al olvido** (ej. por razones de interés público, cuando se desee ejercer la libertad de expresión e información, etc.).

Derecho a la limitación del tratamiento[1]

- El interesado tendrá derecho a obtener del responsable del tratamiento la **limitación del tratamiento** de los datos, debiendo ser informado de ello, cuando se cumpla alguna de las condiciones siguientes:
  - El interesado **impugna la exactitud de los datos personales**, durante un plazo que permita al responsable verificar la exactitud de los mismos.
  - El tratamiento es **ilícito**.
  - El responsable **ya no necesita los datos personales** para los fines del tratamiento, pero el interesado los necesita para la formulación de reclamaciones.

(1) El responsable del tratamiento comunicará cualquier rectificación, supresión o limitación a cada uno de los destinatarios a los que se haya comunicado los datos.

Detalle
Derechos del interesado

…el derecho a la portabilidad de los datos, el derecho de oposición, y el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado

Derechos del interesado (3/3)

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**, y a transmitirlos a otro responsable del tratamiento, cuando se cumplan las siguientes condiciones:
  - El tratamiento está basado en el **consentimiento** o en un **contrato**.
  - El tratamiento se efectúa por **medios automatizados**.
- Además, el interesado tendrá derecho a que los datos personales se transmitan **directamente de responsable a responsable** cuando sea **técnicamente posible**.
- No obstante, existen ciertas **excepciones** a este derecho (ej. por razones de interés público).

Derecho de oposición

- El interesado tendrá derecho a **oponerse** en cualquier momento, por motivos relacionados con su **situación particular**, a que datos personales que le afecten sean objeto de tratamiento. El responsable del tratamiento **dejará de tratar los datos personales**, salvo que acredite motivos legítimos prevalezcan sobre los motivos del interesado.
- Cuando el tratamiento de datos personales tenga por objeto la **mercadotecnia directa**, el interesado tendrá derecho a oponerse en todo momento, y deberán dejar de ser tratados para dichos fines.

Decisiones individuales automatizadas

- Salvo en ciertas circunstancias, todo interesado tendrá derecho a no ser objeto de una **decisión basada únicamente en el tratamiento automatizado**, incluida la **elaboración de perfiles**.

⚠ Los órganos de la UE o los Estados Miembros podrían **limitar** a través de medidas legislativas el **alcance de las obligaciones y derechos** anteriormente expuestos por diversos motivos (ej. seguridad del Estado, defensa, seguridad pública, etc.)

Detalle

Obligaciones del responsable y el encargado del tratamiento

Tras el elenco de derechos reconocidos a los interesados, el Reglamento establece una serie de obligaciones que deberán cumplir el responsable y el encargado del tratamiento. Por ejemplo, el responsable debe implementar la protección de datos desde el diseño y por defecto

Obligaciones generales

Responsable del tratamiento[1]

- El responsable del tratamiento aplicará **medidas técnicas y organizativas** apropiadas, lo que incluye oportunas **políticas de protección de datos**, para garantizar el cumplimiento del marco normativo. Dichas medidas se **revisarán y actualizarán** cuando sea necesario.

Protección "desde el diseño y por defecto"

- El responsable del tratamiento aplicará **en el momento de determinar los medios de tratamiento y en el momento del propio tratamiento** medidas técnicas y organizativas apropiadas (ej. 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.
- El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con el objetivo de garantizar que, **por defecto**, solo sean objeto de tratamiento los datos personales que sean **necesarios para cada uno de los fines específicos** del tratamiento.

Registro

- Cada responsable llevará un **registro de las actividades de tratamiento** efectuadas bajo su responsabilidad (ej. fines del tratamiento, categorías de destinatarios, descripción general de las medidas técnicas y organizativas de seguridad, etc.).

Encargado del tratamiento[1]

- Cuando se vaya a realizar un tratamiento por cuenta de un responsable, este elegirá solo a un **encargado** que ofrezca **garantías suficientes** para aplicar **medidas técnicas y organizativas** apropiadas[2].
- El tratamiento por el encargado se regirá por un contrato que deberá estipular, entre otras cosas, que el encargado:
  - Tratará los datos personales únicamente siguiendo **instrucciones** documentadas del **responsable**.
  - Asistirá al responsable a través de **medidas técnicas y organizativas apropiadas**.
  - A elección del responsable, **suprimirá o devolverá todos los datos personales** una vez finalice la prestación de los servicios de tratamiento.
- El encargado deberá llevar **un registro de todas las categorías de actividades de tratamiento** efectuadas por cuenta de un responsable que contenga.

(1) Cuando el Reglamento se aplique a responsables o encargados no establecidos en la UE, deberán designar un corresponsal.
(2) El encargado no recurrirá a otro encargado sin la autorización previa del responsable.

Detalle

Obligaciones del responsable y el encargado del tratamiento

En cuanto a seguridad, el responsable y el encargado deberán aplicar medidas técnicas y organizativas adecuadas acordes al nivel de riesgo. Además, las violaciones de la seguridad de los datos personales se comunicarán a la autoridad de control y a los interesados

Seguridad de los datos personales

Seguridad del tratamiento

- Teniendo en cuenta diversos factores (especialmente los riesgos que presente el tratamiento[1]), el **responsable y** el **encargado** del tratamiento aplicarán **medidas técnicas y organizativas** apropiadas para garantizar un **nivel de seguridad adecuado al riesgo**, que incluyan, entre otros aspectos:
  - la **seudonimización** y el cifrado de datos personales.
  - la capacidad de garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** permanentes de los sistemas.
  - la capacidad de restaurar la **disponibilidad y 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 estas medidas.
- La adhesión a un **código de conducta** o a un **mecanismo de certificación** podrá servir para demostrar el cumplimiento de estos requisitos de seguridad.

Notificación de una violación de la seguridad

- Se ha de distinguir entre la notificación de una violación de la seguridades de los datos personales que se realiza a la **autoridad de control** y la que se realiza al **interesado**.

Autoridad de control

- El **responsable del tratamiento** la notificará **sin dilación indebida** y, de ser posible, a más tardar en el **plazo de 72 horas** después de que haya tenido constancia de ella[2].
- Esta notificación deberá incluir un **contenido mínimo** especificado en el Reglamento (ej. naturaleza de la violación, posibles consecuencias, etc.). El responsable deberá **documentar** cualquier violación.
- El **encargado del tratamiento** notificará sin dilación indebida al responsable las **violaciones**.

Interesado

- Cuando sea probable que la violación suponga un alto riesgo para los derechos de las personas físicas, el **responsable** la comunicará al interesado **sin dilación indebida**. Deberá incluir un **contenido mínimo** especificado en el Reglamento (ej. posibles consecuencias, etc.), y utilizar un **lenguaje claro**.
- La comunicación no será necesaria en **ciertas situaciones** especificadas en el Reglamento (ej. el responsable ha adoptado medidas de protección técnicas y organizativas apropiadas y se han aplicado).

(1) Consecuencias de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, o la comunicación o acceso no autorizados a dichos datos.
(2) Si la notificación no tiene lugar en el plazo de 72 horas deberán indicarse los motivos.

Detalle

Obligaciones del responsable y el encargado del tratamiento

Otra de las novedades del nuevo marco de protección es la obligación por parte del responsable de realizar una evaluación del impacto de las operaciones de tratamiento cuando el tipo de tratamiento entrañe un alto riesgo para los derechos de los interesados

Evaluación de impacto relativa a protección de datos

Evaluación de impacto

- Cuando sea probable que un **tipo de tratamiento**, en particular si utiliza nuevas tecnologías, entrañe un **alto riesgo** para los derechos 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[1].
- La evaluación de impacto se requerirá en particular en **ciertos casos** especificados en el Reglamento (ej. tratamiento a gran escala de las categorías especiales de datos). La autoridad de control podrá publicar una lista de los tipos de tratamiento que no requieren evaluaciones de impacto.
- La evaluación deberá incluir **como mínimo**:
  - una descripción de las **operaciones** de tratamiento previstas y de los **fines** del tratamiento.
  - una evaluación de la **necesidad y proporcionalidad** de las operaciones con respecto a su finalidad.
  - una evaluación de los **riesgos** para los derechos de los interesados.
- El responsable del tratamiento recabará el **asesoramiento del delegado de protección de datos**.

Consulta previa

- El responsable **consultará a la autoridad de control** antes de proceder al tratamiento cuando una evaluación de impacto muestre que el tratamiento entrañaría un **alto riesgo** si el responsable no toma medidas para mitigarlo.
- Cuando la autoridad de control considere que el dicho tratamiento podría infringir el marco normativo, la **autoridad de control** deberá **asesorar por escrito al responsable** (y en su caso al encargado). Para ello se le otorga un **plazo de 8 semanas** desde la consulta (prorrogable por otras 6 semanas).

(1) Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares

Detalle

Obligaciones del responsable y el encargado del tratamiento

Para finalizar con las obligaciones del responsable y del encargado, el Reglamento establece el requerimiento de designar un delegado de protección de datos (DPO) en ciertos casos. Asimismo, incluye disposiciones relativas a códigos de conducta y certificación

Delegado de protección de datos y códigos de conducta y certificación

Delegado de protección de datos (DPO)

- El **responsable y el encargado del tratamiento** deberán designar un DPO en los siguientes casos[1]:
  - El tratamiento lo lleva a cabo una **autoridad u organismo público**.
  - Las actividades principales del responsable o del encargado consisten en operaciones de tratamiento que requieren una observación habitual y sistemática de **interesados a gran escala**.
  - Las actividades principales del responsable o del encargado consisten en el **tratamiento a gran escala** de **categorías especiales de datos**.

Posición del DPO

- El responsable y el encargado garantizarán que el DPO participa de **forma adecuada y en tiempo oportuno** en las cuestiones relativas a la protección de datos personales. En este sentido, deberán facilitar los **recursos necesarios**, y garantizar que **no recibe ninguna instrucción** en lo que respecta al desempeño de sus funciones. Los interesados podrán ponerse en contacto con el DPO.

Funciones del DPO

- El DPO tendrá **como mínimo** las siguientes funciones:
  - **Informar y asesorar** al responsable o al encargado de las obligaciones que les incumben.
  - **Supervisar el cumplimiento** del Reglamento y de las políticas del responsable o encargado.
  - Ofrecer el asesoramiento que se le solicite acerca de la **evaluación de impacto**.
  - **Cooperar** y actuar como punto de contacto con la **autoridad de control**.

Códigos de conducta

- Las asociaciones de categorías de responsables o encargados podrán elaborar **códigos de conducta o modificar o ampliar dichos códigos** con objeto de especificar la aplicación del Reglamento (ej. en lo relativo a aspectos tales como la seudonimización, ejercicio de los derechos de los interesados, etc.).
- La **supervisión** de un código de conducta podrá ser realizada por un organismo que tenga el nivel adecuado de conocimiento en relación al código y que haya sido acreditado por la autoridad de control.

Certificación

- Podrán establecerse **mecanismos de certificación**, **sellos** o **marcas de protección de datos** aprobados por organismos de certificación o por la autoridad de control con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los **responsables o encargados no sujetos al Reglamento**.

(1) Será designado en función de sus cualidades profesionales. Un grupo empresarial podrá nombrar un único DPO siempre que sea fácilmente accesible desde cada establecimiento.

Detalle

Otros aspectos

Por último, el Reglamento incluye ciertos aspectos adicionales referidos a la supervisión del cumplimiento del marco normativo, como por ejemplo la creación de autoridades de control o el régimen sancionador

Otros aspectos

Autoridades de control independientes

- Cada Estado miembro designará una **autoridad pública independiente** (o varias) responsable de **supervisar** la aplicación del Reglamento, la cual actuará con total **independencia**.
- En el Reglamento se especifican las **funciones** de cada autoridad de control en su territorio (ej. controlar la aplicación del Reglamento, promover la sensibilización de los responsables y encargados del tratamiento acerca de sus obligaciones, etc.).
- Asimismo, también se especifican sus **poderes de investigación** (ej. llevar a cabo investigaciones en forma de auditorías, ordenar al responsable y al encargado del tratamiento que faciliten cualquier información, etc.) y sus **poderes correctivos** (ej. sancionar al responsable o encargado cuando infrinjan el Reglamento).

Comité Europeo de Protección de Datos

- Se crea el **Comité Europeo de Protección de Datos**, que actuará con total **independencia**.
- En el Reglamento se especifican las **funciones** de este comité (ej. supervisar la correcta aplicación del Reglamento, asesorar a la Comisión sobre aspectos relativos a protección de datos personales, etc.).

Recursos y sanciones

- Todo interesado tendrá derecho a presentar una **reclamación ante una autoridad de control** si considera que el tratamiento de datos personales que le afectan infringe el Reglamento.
- Asimismo, toda persona que haya **sufrido daños y perjuicios materiales o inmateriales** como consecuencia de una infracción del Reglamento tendrá derecho a recibir del responsable o el encargado una **indemnización** por los daños y perjuicios sufridos.
- Se prevé la imposición de **multas administrativas** por parte de la **autoridad de control** (ej. el incumplimiento de ciertas obligaciones puede conllevar la imposición de una multa de hasta el mayor de los siguientes importes: 20M€ o el 4% del volumen de negocio total anual global del ejercicio anterior).

Transferencia de datos a terceros países

- Solo se podrán realizar transferencias de datos personales que sean objeto de tratamiento (o vayan a serlo tras su transferencia) a un **tercer país u organización internacional** si el responsable y el encargado del tratamiento cumplen **ciertas condiciones** establecidas en el Reglamento.

Índice

Anexo
Definiciones

A continuación se incluyen una serie de definiciones empleadas a efectos del Reglamento

Definiciones

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.

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

- **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**.

Encargado del tratamiento

- La persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales** por cuenta del responsable del tratamiento.