

LOPD Y NUEVO REGLAMENTO UE 2016/679

Conceptos básicos – Art. 3 LOPD

- Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
- Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Excepto:

Ficheros de personas físicas en el ámbito privado, ficheros especificados como material clasificado, ficheros para investigación terrorista y ficheros de regulación especial como INE y cuerpos de seguridad del estado.

Se clasifican en Automatizados (con tratamiento informático) o no Automatizados.

- Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una Norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

- Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.
- Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y USO del tratamiento.

- Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta Del responsable Del tratamiento.
- Responsable de Seguridad: Persona o personas a las que el Responsable Del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables (RD 994/1999)
- Usuario del fichero: Sujeto o proceso autorizado para acceder a datos o recursos (RD 994/1999)
- Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del Interesado
- Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- Contacto: Persona que trabaja en la empresa y sirven de contacto a dicha empresa. No están sujetos a medidas de protección específicas: Sus nombres y apellidos, funciones o puestos desempeñados, la dirección postal o electrónica, teléfono y número de fax profesionales. Si estará sujeto a protección su DNI.

Nuevo Reglamento UE 2016/679 de 27 de Abril

Con este Reglamento (99 Artículos) se quiere dar más control a los interesados sobre su información privada, a nivel tecnológico.

A pesar de que es una única norma para toda la Unión Europea, y de aplicación inmediata una vez entre en vigor, debe ser interpretada a nivel nacional, es decir, nuestra AEPD, deberá pronunciarse ya que en muchos artículos (unos 50) se deja la puerta abierta a los Estados Miembros para que regulen esos aspectos.

Novedades	
Evaluación de Impacto	En la privacidad de futuros desarrollos tecnológicos
Ventanilla única (One Stop Shop)	Para toda la UE con competencias similares a la AEPD
Elaboración de perfiles	Para algunos aspectos personales
Seudonimización	Consiste en el tratamiento de datos personales de forma que no puedan atribuirse a una persona física identificada o identificable
Derecho al olvido	Mediante rectificación y/o supresión de datos personales
Derecho a la portabilidad de datos	De un proveedor de servicios a otro
Multas de hasta 20 millones de euros o el 4% de fact. global	Optándose por la mayor cuantía
Licitud del consentimiento	El consentimiento queda como un acto afirmativo claro
Delegado de Protección de Datos	Para el sector público, actividades de Big Data y análisis de perfiles.

Notificar una violación de seguridad.	En 72 horas al órgano de control, o si es de alto riesgo, al interesado.
Datos genéticos/ Datos biométricos	Sobre la fisiología o salud o que permiten la identificación única de personas
Responsabilidad proactiva	Los responsables tienen que demostrar la carga de la prueba



CAPÍTULO I - ARTÍCULO 2

1- 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.

2- 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 (SOBRE LA POLÍTICA EXTERIOR Y DE SEGURIDAD COMÚN)
- 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

CAPÍTULO I -ART. 4- DEFINICIONES

- 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

- Violación de la seguridad: 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

- 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 presente Reglamento

- 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

- 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;

- Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro
- Autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.

· 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;

Capítulo II - Art. 8 Condiciones para el consentimiento del menor con los servicios de la Sdad. De la información

1- Si el niño es menor de 16 años, el tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. En España la edad es de 14 años.

Capítulo II - Art. 9 Tratamiento de categorías especiales de datos personales

1- Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física

2- El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales

b) en el ámbito del Derecho laboral y de la seguridad y protección social

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física

- d) el tratamiento es efectuado, por una asociación o cualquier otro organismo sin ánimo de lucro
- e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos
- f) para la formulación, ejercicio, defensa de reclamaciones o los tribunales en ejercicio de su función
- g) el tratamiento es necesario por razones de un interés público esencial
- h) para fines de medicina preventiva o laboral, capacidad laboral o diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas.
- i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública
- j) Para fines de archivo en interés público, investigación científica o histórica o fines estadísticos

Capítulo III - Art. 17 Derecho de supresión – Derecho al olvido

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

- a) Los fines para los que se captaron los datos ya no estén vigentes
- b) Exista revocación del consentimiento por parte del interesado
- c) Exista oposición al tratamiento por parte del interesado
- d) Los datos personales hayan sido tratados ilícitamente
- e) Por obligación legal
- f) Si los datos se han obtenido en virtud de la LSSICE para publicidad

EXCEPCIONES:

- a) Para ejercer el derecho a la libertad de expresión e información
- b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos
- c) Por razones de interés público en el ámbito de la salud pública
- d) Con fines de archivo público, fines de investigación científica o histórica o fines estadísticos

Capítulo III - Art. 20 Derecho a la portabilidad de datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento lícito, no haya ninguna Ley que lo impida, o el tratamiento sea necesario para ejecución de un contrato.

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

Capítulo III - Art. 21 y 22 Elaboración de perfiles

Art. 21

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Art. 22

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) Es necesaria para la celebración o la ejecución de un contrato entre interesado y responsable

b) Está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

c) Se basa en el consentimiento explícito del interesado.

Capítulo IV - Art. 33 Notificación de una violación de seguridad de los datos personales a la autoridad de control



1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Capítulo IV - Art. 34 Comunicación de una violación de seguridad de los datos personales al interesado

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

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Capítulo IV - Art. 35 y 36 Evaluación de impacto relativa a la protección de datos – Consulta previa

Art. 35

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

- a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- b) tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales.
- c) observación sistemática a gran escala de una zona de acceso público.

Art. 36

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

Capítulo IV - Art. 37 Designación del delegado de protección de datos

Art. 37

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

- a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
- b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Capítulo IV - Art. 38 Posición del delegado de protección de datos

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados

miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Capítulo IV - Art. 39 Funciones del delegado de protección de datos

1. 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 del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, 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 de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control.

2. El delegado de protección de datos desempeñará sus 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.

Capítulo IV - Art. 40 y 41 Códigos de conducta y supervisión de los mismos

Art. 40.

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características

específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento

3. Los responsables o encargados podrán adherirse a códigos de conducta aprobados a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales. Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

Capítulo IV - Art. 42 y 43 Certificación – Organismo de certificación

Art. 42.

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

Capítulo VI y IX - Art. 51 a 91 Autoridades de control – Comité europeo de protección de datos

Art. 51.

1. Cada Estado miembro establecerá una o varias autoridades públicas independientes (en adelante «autoridad de control») para supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.
2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.
3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité.
4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Art. 83.

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento
2. El Comité estará representado por su presidente.
4. Las infracciones de las disposiciones siguientes se sancionarán, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
 - a) las obligaciones del responsable y del encargado
 - b) las obligaciones de los organismos de certificación
 - c) las obligaciones de la autoridad de control
5. Las infracciones de las disposiciones siguientes se sancionarán, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
 - a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento
 - b) los derechos de los interesados
 - c) las transferencias de datos personales a un destinatario en un tercer país

d) toda obligación en virtud del Derecho de los Estados miembros con arreglo al capítulo IX

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control.

Capítulo XI - Art. 94 a 99 Disposiciones finales

Art. 94.

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.

Art. 99.

2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.