GENERALITAT VALENCIANA
Conselleria de Sanitat Universal i Salut Pública

DEPARTAMENTO DE SALUD DE SAGUNTO

Comité de Bioética Asistencial

Ley Orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales (LOPDGDD)

Análisis de la normativa legal de aplicación al tratamiento de los datos personales relacionados con la salud

NOTA: **sobre la LOPDGDD efectuamos el análisis de los aspectos relacionados con la materia sanitaria.** Como hay numerosas referencias al articulado de otros textos legales, he elegido transcribir íntegramente dichas citas, por dos razones: para que no quepan dudas del alcance legal del articulado y para evitar la consulta constante de las mismas en los textos originales de procedencia (sobre todo el del Reglamento UE 2016/679).
En el documento el texto normativo tiene un tamaño de letra 12; aparecerán en cursiva y con tamaño de letra 10 las referencias citadas en el texto normativo (primer nivel); el tamaño será de 8 para las referencias citadas en el texto de las de primer nivel (serán de segundo nivel); en el anexo 5.2 se agruparán las referencias que denominamos de tercer nivel, es decir las que aparezcan en el texto normativode las de segundo nivel.

Coordinador: Vicent López Camps
Documento aprobado por el CBA del Departamento de Salud de Sagunt.
Reunión del 18/02/2021

SUMARIO

INTRODUCCIÓN

1.-Presentación de la ley orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

1.1. Artículo 1. Objeto de la ley.

1.2. Reglamento UE 2016/679

1.3. LOPDGDD: Disposición derogatoria única. Derogación normativa.

2.-Marco normativo de protección de datos: aspectos relevantes en materia sanitaria.

2.1. Bases jurídicas para el tratamiento de datos de salud.

2.2. Ejercicio de los derechos

2.3. Tratamiento de los datos de salud en la LOPDGDD:

A) Disposición adicional decimoséptima

B) Disposición final novena

2.4. Deberes de confidencialidad y secreto profesional

2.5. Consentimiento de los menores de edad

2.6. Tratamiento de datos de personas fallecidas

2.7. Relación entre el responsable y el encargado del tratamiento

2.8. Delegado de protección de datos (DPD)

3.- Resumen y conclusiones.

4.-Bibliografía

5.-Anexos:

5.1. Definiciones

5.2. Citas de tercer nivel en el articulado normativo

5.3. Preguntas relacionadas con la protección de datos

Introducción.

Sirvan como introducción, los considerandos que preceden al articulado que el *Reglamento 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 que figuran a continuación con su número identificativo.

1. "**La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.** El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

4. "El tratamiento de datos personales debe estar concebido para servir a la humanidad**. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad**. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

32. "**El consentimiento debe darse mediante un acto afirmativo claro** que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal"…."El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos".

33. "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, **debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica**. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida".

34. "Debe entenderse por **datos genéticos** los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente".

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

46. "El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. **Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano"**.

53. "**Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto**, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público,…"

54. "**El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública**. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, **«salud pública»** debe interpretarse en la definición del Reglamento (CE) nº 1338/2008 del Parlamento Europeo y del Consejo, es decir, *todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad*. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

1. Presentación de la Ley Orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD)

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

1.1. Artículo 1. Objeto de la ley.

La presente Ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al **Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016** (en adelante lo citaremos como: Reglamento UE 2016/679), relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.
El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento UE 2016/679 y en esta ley orgánica.

b) **Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución Española:**

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

1.2. Reglamento UE 2016/679 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.

Deroga la Directiva 95/46/CE conocida como "Reglamento general de protección de datos (RGPD)".

> *El artículo 4 del Reglamento UE 2016/679 trata de las **"Definiciones"** (Ver en el Anexo1 el listado completo de las mismas); interesa **destacar las que se refieren a los datos sanitarios** y son las siguientes:*
>
> ***1. 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.*

2. 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.*
3. 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.*

Y por ser un término tan "sanitario", añadimos:

4. 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.

1.3. LOPDGDD: Disposición derogatoria única. Derogación normativa.

1. Sin perjuicio de lo previsto en la *disposición adicional decimocuarta* y en la *disposición transitoria cuarta*, **queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), con efectos de 7 de diciembre de 2018.**

Disposición adicional decimocuarta
Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.

Las normas dictadas en aplicación del ***artículo 13 de la Directiva 95/46/CE*** *del Parlamento Europeo y del Consejo, de 24 de octubre de 1995*, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular **los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.**

ART. 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995
Artículo 13 Excepciones y limitaciones

1*. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6 ("Calidad de los datos personales que dispondrán los estados miembros"), en el articulo 10 ("Información en caso de obtención de datos recabados del propio interesado"), en el apartado 1 del artículo 11 ("Información cuando los datos no han sido recabados del propio interesado") , y en los artículos 12 ("Derecho de acceso") y 21 ("Publicidad de los tratamientos") cuando tal limitación constituya una medida necesaria para la salvaguardia de :*

a) la seguridad del Estado ;

b) la defensa;

c) la seguridad pública ;

d) la prevención , la investigación , la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada , aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

***2.** Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán , en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 ("Derecho de acceso") cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.*

Artículos 23 y 24 de la LOPD (Ley 15/1999)

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

***1**. Los responsables de los ficheros que contengan los datos a que se refieren los **apartados 2, 3 y 4 del artículo 22 "Ficheros de las Fuerzas y Cuerpos de Seguridad"** (ver pags. 8-9) **,** podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.*

***2**. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.*

***3.** El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.*

Artículo 24. Otras excepciones a los derechos de los afectados.

***1.** Lo dispuesto en los **apartados 1 y 2 del artículo 5 ("Derecho de información en la recogida de datos"**:*

> ***1**. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
>
> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
>
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
>
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
>
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
>
> *e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.*

2. *Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior, no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.*

2*. Lo dispuesto en el* ***artículo 15 "Derecho de acceso":***

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

3. *Lo dispuesto en el* ***apartado 1 del artículo 16 "Derecho de rectificación y cancelación"****:*

1. *El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días) no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.*

Disposición transitoria cuarta.
Tratamientos sometidos a la Directiva UE 2016/680.

Los tratamientos sometidos a la Directiva UE 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, **continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.**

Artículo 22 de la LOPD 1999:
Ficheros de las Fuerzas y Cuerpos de Seguridad.

1*. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.*

2. *La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.*

3. *La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia* ***los apartados 2 y 3 del artículo 7****, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de*

legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

Apartados 2 y 3 del artículo 7 "Datos especialmente protegidos":

2. *Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.*

3*. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente), podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.*

4. *Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.*

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento UE 2016/679 y en la presente ley orgánica.

2. Marco normativo de protección de datos: aspectos relevantes en materia sanitaria.

2.1 Bases jurídicas para el tratamiento de los datos de salud por las Administraciones Públicas.

---**La regulación está recogida en los artículos 8 y 9 de la LOPDGDD.**

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el **artículo 6.1.c) del Reglamento UE 2016/679**, cuando así lo prevea una norma de Derecho de la Unión Europea o **una norma con rango de ley**, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el **capítulo IV del Reglamento UE 2016/679**.

Artículo 6.1 c Reglamento UE 2016/679: Licitud del tratamiento

***1**.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

***c)** el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*

CAPÍTULO IV Reglamento UE 2016/679:
Responsable del tratamiento y encargado del tratamiento
Ver en en apartado 2.7 del texto

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el **artículo 6.1 e del Reglamento UE 2016/679**, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 6.1 e Reglamento UE 2016/679:
Licitud del tratamiento

***1**.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

***e)** el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

Artículo 9. Categorías especiales de datos.

1. A los efectos del **artículo 9.2.a) del Reglamento UE 2016/679**, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición

del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.
Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el **artículo 9.2 del Reglamento UE 2016/679**, cuando así proceda.

2. Los tratamientos de datos contemplados en las **letras g), h) e i) del artículo 9.2 del Reglamento UE 2016/679** fundados en el Derecho español **deberán estar amparados en una norma con rango de ley**, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 9 Reglamento UE 2016/679:
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 orientación 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 con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) 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, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, 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 o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) ***el tratamiento es necesario por razones de un interés público esencial****, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;*

h) ***el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social,*** *sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;*

i) ***el tratamiento es necesario por razones de interés público en el ámbito de la salud pública****, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,*

j) ***el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica*** *o histórica o fines estadísticos, de conformidad con el* ***artículo 89, apartado 1****, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.*

Artículo 89 Reglamento UE 2016/679:
Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

1.*El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.*

2*.Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los* ***artículos 15*** *(ver en pags. 14-15),* ***16*** *(ver en pag 16),* ***18*** *(ver en pag 17)* ***y 21*** *(ver en pag 19), sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.*

3.Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en ***artículos 15*** *(ver en pags. 14-15),* ***16*** *(ver en pag 16),* ***18*** *(ver en pag 17),* ***20*** *(ver en pag 18-19)* ***y 21*** *(ver en pag 19) sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.*

4.En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

3. *Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h),* ***cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad****, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.*

4. *Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.*

2.2. Ejercicio de derechos

2.2.1. El capítulo II de la LOPDGDD trata sobre el ejercicio de los derechos.

Artículo 12. Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los **artículos 15 a 22 del Reglamento UE 2016/679,** podrán ejercerse directamente o por medio de representante legal o voluntario.

El capítulo III del Reglamento UE 2016/679 con el título genérico "Derechos del interesado", que es la base del Capítulo II de la LOPDGDD, está estructurado del siguiente modo:

Sección 1: Transparencia y modalidades
- *Art. 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

Sección 2: Información y acceso a los datos personales.
- *Art. 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*
- *Art. 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*
- *Art. 15. Derechos de acceso del interesado.*

Sección 3: Rectificación y supresión
- *Art. 16. Derecho de rectificación*
- *Art. 17. Derecho de supresión ("el derecho al olvido")*
- *Art. 18. Derecho a la limitación del tratamiento*
- *Art. 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*
- *Art. 20. Derecho a la portabilidad de los datos*

Sección 4. Derecho de oposición y decisiones individuales automatizadas.
- *Art. 21. Derecho de oposición.*
- *Art. 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

Sección 5: Limitaciones
- *Art. 23. Limitaciones.*

2. El responsable del tratamiento estará obligado a **informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden.** Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el **Capítulo III del Reglamento UE 2016/679, se estará a lo dispuesto en aquellas.**

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los **artículos 12.5** (a continuación) **y 15.3** *(ver pag 15)* **del Reglamento UE 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica** *(ver pag. 16).*

Artículo 12.5 Reglamento UE 2016/679: Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

5. *La información facilitada en virtud de los artículos (del Reglamento UE) 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:*

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Artículo 13. Derecho de acceso.

1. El derecho de acceso del afectado se ejercitará de **acuerdo con lo establecido en el artículo 15 del Reglamento UE 2016/679.**
Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

Artículo 15 Reglamento UE 2016/679: Derecho de acceso del interesado

1*. 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 y a la siguiente información:*

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) 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;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) 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;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el ***artículo 22 Reglamento UE, apartados 1 y 4,*** *y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*

Artículo 22 Reglamento UE 2016/679:
Decisiones individuales automatizadas, incluida la elaboración de perfiles

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 el interesado y un responsable del tratamiento;

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,

o c) se basa en el consentimiento explícito del interesado.

3.En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4.*Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el* ***artículo 9, apartado 1, salvo que se aplique el artículo 9 Reglamento UE, apartado 2 letra a o g*** *(en pags. 11-12) y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*

2*. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las* ***garantías adecuadas en virtud del artículo 46 Reglamento UE relativas a la transferencia*** *(ver en pags. 23-24).*

3*. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.*

4*. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.*

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.
No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el **artículo 15.1 del Reglamento UE 2016/679** *(ver en pags 14-15)* que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el **artículo 12.5 del Reglamento UE 2016/679** (*ver en pag. 14)* se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el **artículo 16 del Reglamento UE 2016/679**, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 16 Reglamento UE 2016/679:
Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 15. Derecho de supresión.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el **artículo 17 del Reglamento UE 2016/679**.

Artículo 17 Reglamento UE 2016/679:
Derecho de supresión («el 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 datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento

c) el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento,

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información

***2.** Cuando haya hecho públicos los datos personales y esté obligado, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.*

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

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 impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;*

*c) **por razones de interés público en el ámbito de la salud pública***

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento,

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Este punto 3 constata que
el derecho de supresión ("olvido") de los datos sanitarios no es absoluto.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al **artículo 21.2 del Reglamento UE 2016/679** *(ver en pag 19)* el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento UE 2016/679.

Artículo 18 Reglamento UE 2016/679:
Derecho a la limitación del tratamiento

***1.** El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:*

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

*d) el interesado se haya opuesto al tratamiento en virtud del **artículo 21 del Reglamento UE, apartado 1** (ver en pag 19) mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.*

***2**. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, 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.*

***3.** Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.*

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 20 Reglamento UE 2016/679:
Derecho a la portabilidad de los 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 con arreglo a los **artículos del Reglamento UE, 6 apartado 1 letra a** o el **artículo 9, apartado 2 letra a** (pag. 11) , o en un contrato con arreglo al **artículo 6, apartado 1 letra b:***

Artículo 6.1 a y b Reglamento UE 2016/679:
Licitud del tratamiento

***1**.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

***a)** el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*

***b)** el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*

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.*

***3**. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del **artículo 17 del Reglamento UE** (ver en pags. 16-17). Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.*

***4**. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.*

Artículo 18. Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los **artículos 21 y 22** *(ver en pag. 15)* **del Reglamento UE 2016/679.**

Artículo 21 Reglamento UE 2016/679:
Derecho de oposición

***1.** El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el **artículo 6, apartado 1, letras e) o f)**, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.*

Artículo 6.1 e/f Reglamento UE 2016/679:
Licitud del tratamiento

***1**.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

***e)** el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

***f)** el tratamiento es 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.*

***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.*

***3.** Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.*

***4.** A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.*

***5**. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.*

***6**. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el **artículo 89 Reglamento UE 2016/679, apartado 1** (ver pag.12) el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.*

2.2.2. La LOPDGDD establece que **todas las actuaciones que se hayan de llevar a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de derechos, serán gratuitas**, con las salvedades previstas en los apartados **3 y 4 del artículo 13** (ver pag. 16) de la presente Ley Orgánica, a saber:

a) peticiones repetitivas reiteradas en el plazo de 6 meses sin causa legítima para ello,

b) elección por el interesado de un medio distinto al ofrecido que suponga un coste desproporcionado.

Afirma la imposibilidad de exigir al paciente contraprestación económica alguna por la obtención de copia de su historia clínica, más allá de las excepciones referidas anteriormente.

2.3. Tratamiento de datos de salud

La regulación que establece la LOPDGDD del tratamiento de los datos de salud se hace en:

A) **La disposición adicional decimoséptima** en relación a su vez, con

B) **la disposición final novena** de la misma.

2.3.A--Disposición adicional decimoséptima.
Tratamientos de datos de salud.

1. Se encuentran amparados en las **letras g), h), i) y j) del artículo 9.2 del Reglamento UE 2016/679** *(ver en pags. 11-12),* los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos **sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública**.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el **artículo 13 del Reglamento UE 2016/679**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.
Para los tratamientos previstos en esta letra, **se requerirá informe previo favorable del comité de ética de la investigación.**

Artículo 13 Reglamento UE 2016/679:
Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1*. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el ***artículo 6, apartado 1, letra f,*** *los intereses legítimos del responsable o de un tercero;*

Artículo 6 Reglamento UE 2016/679: Licitud del tratamiento
Apartado 1 letra f

> ***f)*** *el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan de datos personales, en particular cuando el interesado sea un niño.*

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, 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, o, en el caso de las transferencias indicadas en los ***artículos del Reglamento UE 46 o 47 o el artículo 49, apartado 1, párrafo segundo****, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.*

Artículo 46 Reglamento UE 2016/679:
Transferencias mediante garantías adecuadas

> ***1****.A falta de decisión con arreglo al* ***artículo 45 del Reglamento UE, apartado 3*** *(ver en Anexo 2, pag 54), el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.*
>
> ***2****.Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:*
>
> *a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;*
>
> *b) normas corporativas vinculantes de conformidad con el* ***artículo 47 del Reglamento UE*** *(ver más adelante);*
>
> *c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el* ***artículo 93 del Reglamento UE, apartado 2*** *(ver en Anexo 2, pags 54-55)*

*d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el **artículo 93 del Reglamento UE, apartado 2** (ver anexo 2 pags. 54-55).*

*e) un código de conducta aprobado con arreglo al **artículo 40 del Reglamento UE** (ver en Anexo 2, pags 57-60), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados,*

*f) un mecanismo de certificación aprobado con arreglo al **artículo 42 del Reglamento UE** (ver en Anexo 2, pags 60-62), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.*

***3**.Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:*

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional,

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

***4**.La autoridad de control aplicará el mecanismo de coherencia a que se refiere el **artículo 63 del Reglamento UE** (ver en Anexo 2, pag 62) en los casos indicados en el apartado 3 del presente artículo.*

***5**.Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el **artículo 26 apartado 2, de la Directiva 95/46/CE** (ver en Anexo 2, pag 63) seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del **artículo 26, apartado 4, de la Directiva 95/46/CE** (ver en Anexo 2 pag.64) permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.*

Artículo 47 Reglamento UE: Normas corporativas vinculantes

***1**.La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el **artículo 63 del Reglamento UE** (ver en Anexo 2 pag. 62), siempre que estas:*

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

***2**.Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:*

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

*e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el **artículo 22 del Reglamento UE** (ver en la pag. 15), el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el **artículo 79 del Reglamento UE** (ver en Anexo 2 pag. 58), y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;*

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o

parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los ***artículos del Reglamento UE 13*** *(ver en pag. 23)* ***y 14*** *(ver en Anexo 2 pag. 64);*

h) las funciones de todo delegado de protección de datos designado de conformidad con el ***artículo 37 del Reglamento UE*** *(ver en pag 42-43), o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;*

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes,

y n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3*.La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el* ***artículo 93 del Reglamento UE, apartado 2*** *(ver en Anexo 2 pag. 56-57).*

Artículo 49 Reglamento UE 2016/679:
Excepciones para situaciones específicas
apartado 1, párrafo segundo

Cuando una transferencia no pueda basarse en disposiciones de los artículos ***45*** *(ver en Anexo 2 pag. 56) o* ***46*** *(ver en pags. 23-24), incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los* ***artículos del Reglamento UE 13*** *(ver en pag 23) y* ***14*** *(ver Anexo 2, pag 64), el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.*

2. *Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:*

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) 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;

*c) cuando el tratamiento esté basado en los **artículos del Reglamento UE 6, apartado 1, letra a** (ver en pag 18), o **el artículo 9, apartado 2, letra a** (ver pag. 11), 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;*

d) el derecho a presentar una reclamación ante una autoridad de control;

e) 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 que no facilitar tales datos;

*f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el **artículo 22 del Reglamento UE, apartados 1 y 4** (ver en pag.15) y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*

***3**.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.*

***4.**Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.*

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.
El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

a) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

b) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo **89.2 del Reglamento UE 2016/679** (ver en pag.12)**,** podrán excepcionarse los derechos de los afectados previstos en los **artículos del Reglamento UE 2016/679**, **15** (Derecho de acceso, ver pag. 14-15), **16** (Derecho de

rectificación, ver pag. 16), **18** (Derecho a la limitación del tratamiento, ver en pags. 17-18), **20** (Derecho a la portabilidad, pags. 18-19 y **21** (Derecho de oposición, ver pag. 19) cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo **89 del Reglamento UE 2016/679** (ver en pag,12), se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el **artículo 35 del Reglamento UE 2016/679** o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

Artículo 35 reglamento UE
Evaluación de impacto relativa a la protección de datos

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.*

2*.El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.*

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 a que se refiere el ***artículo 9, apartado 1del Reglamento UE*** *(ver en pag. 11), o de los datos personales relativos a condenas e infracciones penales a que se refiere el* ***artículo 10 del mismo Reglamento:***

Artículo 10 Reglamento UE 2016/679
Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, 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. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

c) observación sistemática a gran escala de una zona de acceso público.

4**.La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el **artículo 68.

Artículo 68 Reglamento UE 2016/679
Comité Europeo de Protección de Datos

1.Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2.El Comité estará representado por su presidente.

3.El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4.Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5.La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

*6.En los casos a que se refiere el **artículo 65** (ver en Anexo 2 pag. 65-68) el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.*

***5.**La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.*

***6.**Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el **artículo 63** (ver en Anexo 2 pag.62) si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.*

***7.**La evaluación deberá incluir como mínimo:*

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1,

y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

***8.**El cumplimiento de los códigos de conducta aprobados a que se refiere **el artículo 40** (ver en Anexo 2 pag 57-60) por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.*

***9**.Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.*

***10**.Cuando el tratamiento de conformidad con el **artículo 6, apartado 1, letras c** o **e** (ver en pag 10), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.*

***11**.En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.*

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al **artículo 74 del Reglamento UE 536/2014**, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el **artículo 27.1 del Reglamento UE 2016/679** (ver adelante)**.**

Artículo 74 del Reglamento UE 536/2014 (sobre ensayos clínicos)

***1**.Si el promotor de un ensayo clínico no está establecido en la Unión Europea, tendrá un representante legal que sea una persona física o jurídica establecida en la Unión. Dicho representante legal se encargará de garantizar el cumplimiento de las obligaciones que incumben al promotor en virtud del presente Reglamento, y será el destinatario de todas las notificaciones al promotor previstas en el presente Reglamento. Toda notificación al representante legal será considerada notificación al promotor.*

***2**.Los Estados miembros podrán decidir no aplicar el apartado 1 en lo que respecta a los ensayos clínicos que vayan a realizarse únicamente en su territorio, o en su territorio y el de terceros países, siempre y cuando garanticen que el promotor designa al menos una persona de contacto en su territorio en relación con ese ensayo clínico que será el destinatario de todas las notificaciones al promotor previstas en el presente Reglamento.*

***3**.En lo que respecta a ensayos clínicos que vayan a realizarse en más de un Estado miembro, todos aquellos Estados miembros en los que vayan a realizarse podrán decidir no aplicar el apartado 1, siempre y cuando garanticen que el promotor designa al menos a una persona de contacto en la Unión en relación con ese ensayo clínico que será el destinatario de todas las comunicaciones al promotor previstas en el presente Reglamento.*

Artículo 27 Reglamento UE 2016/679
Representantes de responsables o encargados del tratamiento no establecidos en la Unión

***1**.Cuando sea de aplicación **el artículo 3, apartado 2**, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.*

Artículo 3 Reglamento UE
Ámbito territorial

2.El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.
En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el **artículo 37.5 del Reglamento UE 2016/679** (ver en pag 43)

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, **los comités de ética de la investigación**, en el ámbito de la salud, biomédico o del medicamento, **deberán integrar entre sus miembros un delegado de protección de datos** o, en su defecto, un experto con conocimientos suficientes del Reglamento UE 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

2.3.B--Disposición final novena.

Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002 y queda redactado como sigue:

Artículo 16. Usos de la historia clínica.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso.
El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el **apartado 2 de la Disposición adicional decimoséptima de la LOPDGDD** *(ver en pags. 22-30)*.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario **para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias** a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, **podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública**. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

Así, el **Artículo 41 de la Ley 33/2011 "Organización de los sistemas de información"**, la redacción de los dos primeros apartados no alberga dudas:

> ***1. Las autoridades sanitarias*** *con el fin de asegurar la mejor tutela de la salud de la población* ***podrán requerir****, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios* ***informes, protocolos u otros documentos con fines de información sanitaria.***
>
> ***2.*** *Las Administraciones sanitarias* ***no precisarán obtener el consentimiento*** *de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias,* ***cuando ello sea estrictamente necesario para la tutela de la salud de la población.***

2.4. Deberes de confidencialidad y secreto profesional.

La LOPDGDD establece el deber de confidencialidad:

Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el **artículo 5.1.f) del Reglamento UE 2016/679**.

El artículo 5.1.f del Reglamento UE: Principios relativos al tratamiento

1. los datos personales serán:

f) *tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*

2. La obligación general señalada en el apartado anterior será complementaria de los **deberes de secreto profesional** de conformidad con su normativa aplicable.
En el ámbito sanitario la relevancia del deber de secreto profesional es evidente:

--**obligaciones deontológicas** que deben asumir todos los profesionales sanitarios,

--**responsabilidades penales** a las que se enfrenta este colectivo por incurrir en la comisión de un delito de descubrimiento y revelación de secreto.
Está tipificado en los artículos 197 y siguientes del Código Penal, en los supuestos de accesos indebidos a la historia clínica, o revelación de secreto a terceros.

TÍTULO X
Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio
CAPÍTULO I
Del descubrimiento y revelación de secretos
Artículo 197.

Este artículo establece las penas para el delito de descubrimiento y revelación de secretos como una vulneración de la intimidad de otra persona sin su consentimiento. Destacamos de su redacción los puntos siguientes:

1*. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*

2*. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*

3. *Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.*

4. *Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:*
a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. *Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.*

(Este artículo tiene dos apartados más, 6 y 7 y además bis, ter, quater y quinquies).

Del artículo 9 del Reglamento UE 2016/679 (pags. 11-12) referido al tratamiento de categorías especiales de datos personales, destacamos aquí:

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 orientación sexuales de una persona física.*

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

h) ***el tratamiento es necesario para*** *fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;*

i) ***el tratamiento es necesario por razones de interés público en el ámbito de la salud pública****, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.*

2.5. Consentimiento de los menores de edad.

La LOPDGDD en su **artículo 7 "Consentimiento de los menores de edad",** indica la mayoría de edad en relación con la protección de datos de carácter personal:

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.
Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos **de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela**, con el alcance que determinen los titulares de la patria potestad o tutela.

El **artículo 12** de la LOPDGDD **"Disposiciones generales sobre ejercicio de los derechos"** , en el punto 6 (ver pag 14), establece que:

"En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los **menores de catorce años** los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica".

2.6 Tratamiento de datos de personas fallecidas.

Artículo 2 de la LOPDGDD.
Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier 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. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

Artículo 3 de la LOPDGDD:
"Datos de las personas fallecidas".

1. **Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.**
Como excepción, las personas a las que se refiere el párrafo anterior **no podrán acceder a los datos del causante**, ni solicitar su rectificación o supresión, **cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley**. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.
Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. **En caso de fallecimiento de menores**, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Destacamos que el Art. 18. "Derechos de acceso a la historia clínica", de la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica***, en su apartado 4 señala:***

> *"Los centros sanitarios y los facultativos de ejercicio individual sólo* ***facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho****, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso* ***el acceso de un tercero*** *a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros".*
>
> *Las personas vinculadas al paciente por razones familiares (considerando como tales al cónyuge, ascendientes y descendientes y hermanos) o de hecho, pueden acceder a la historia clínica salvo que el fallecido se hubiera opuesto y así se acredite, y en todo caso* ***siendo de aplicación las mismas limitaciones que regirían para el propio paciente si estuviese vivo****, a saber:*
>
> *a) la intimidad de terceras personas,*
>
> *b) anotaciones subjetivas,*
>
> *c) el conocido "privilegio terapéutico" de los profesionales sanitarios.*

2.7. Relación entre el responsable y el encargado del tratamiento.

2.7.1 Estas figuras están contempladas en el Reglamento de la UE, en el **artículo 4 "Definiciones"*:***

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;

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

2.7.2. El TÍTULO V de la LOPDGDD lleva por título "Responsable y encargado del tratamiento". En el CAPÍTULO I se encuentran las "Disposiciones generales. Medidas de responsabilidad activa" cuyo primer artículo es:

Artículo 28 LOPDGDD.
Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los **artículos 24** ("Responsabilidad del responsable del tratamiento") **y 25** "(Protección de datos desde el diseño y por defecto") **del Reglamento UE 2016/679**, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV, Evaluación de impacto relativa a la protección de datos (**Art 35**, pags. 27-28) y consulta previa (**Art 36**, pag. 45) del citado reglamento.

Artículo 24 Reglamento UE 2016/679
Responsabilidad del responsable del tratamiento

1*.Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

2*.Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.*

3*.La adhesión a códigos de conducta aprobados a tenor del **artículo 40** (ver en Anexo 2 pag 57-60) o a un mecanismo de certificación aprobado a tenor del **artículo 42** (ver en Anexo 2 pag 60-62) podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*

Artículo 25 Reglamento UE 2016/679
Protección de datos desde el diseño y por defecto

1*.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la 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, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*

2*.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*

3.*Podrá utilizarse un mecanismo de certificación aprobado con arreglo al* ***artículo 42*** *(ver en Anexo 2 pag 60-62) como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.*

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular**, los mayores riesgos que podrían producirse en los siguientes supuestos**:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, **pérdida de confidencialidad de datos sujetos al secreto profesional**, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los **artículos 9 "Tratamiento de categorías especiales de datos personales"** (pags. 11-12) y **10 "Tratamiento de datos personales relativos a condenas e infracciones penales" del Reglamento UE** (ver pag 28) *y* los **artículos 9 "Categorías especiales de datos"** (pag 10) y **10 "Tratamiento de datos de naturaleza penal" de esta ley orgánica** o de los datos relacionados con la comisión de infracciones administrativas.

Artículo 10 LOPDGDD.
Tratamiento de datos de naturaleza penal.

1. *El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.*

2. *El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el* ***artículo 10 del Reglamento UE 2016/679*** *(ver pag 28), podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.*

3. *Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.*

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

2.7.3. En la LOPDGDD, en su **Disposición adicional primera (“Medidas de seguridad en el ámbito del sector público”)** se definen funciones de seguridad del responsable o del encargado del tratamiento.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el **artículo 32 del Reglamento UE 2016/679, titulado “Seguridad del tratamiento”**.

Artículo 32 del Reglamento UE 2016/679
“Seguridad del tratamiento”.

1.*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas,* ***el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo****, que en su caso incluya, entre otros:*

a) la seudonimización y el cifrado de datos personales;

*b) **la capacidad de garantizar la confidencialidad**, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

***2**. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.*

***3.** La adhesión a un código de conducta aprobado a tenor del **artículo 40 del Reglamento UE "Códigos de conducta"** (ver en Anexo 2 pag 57-60) o a un mecanismo de certificación aprobado a tenor del **artículo 42 Reglamento UE "Certificación"** (ver en Anexo 2 pag. 60-62) podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*

***4. El responsable y el encargado del tratamiento** tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.*

2. Los responsables enumerados en el **artículo 77.1 de esta ley orgánica** deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.
En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Artículo 77.1. LOPDGDD
Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.
f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2.8 Delegado de Protección de Datos (DPD).

El Cap III de la LOPDGG se refiere completamente al DPD, con los siguientes artículos:

Artículo 34 LOPDGDD.
Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el **artículo 37 del Reglamento UE 2016/679** (ver adelante) y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l**) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.**
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 37 del Reglamento (UE) 2016/679
Designación del delegado de protección de datos

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** (ver en pag 11-12) y de datos relativos a condenas e infracciones penales a que se refiere el **artículo 10** (ver en pag 38)*

***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 del Reglamento UE** (ver adelante en esta pag. y siguiente)*

***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.*

Artículo 35 LOPDGDD.
Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el **artículo 37.5 del Reglamento UE 2016/679** (ver antes, ese apartado **cita al art 39 reglamento UE**) para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 39 del Reglamento UE 2016/679: funciones del DPD

***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 "Evaluación de impacto relativa a la protección de datos"*** *(ver en pags. 27-28)****.***

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 a que se refiere el ***artículo 36 ("Consulta previa"),*** *y realizar consultas, en su caso, sobre cualquier otro asunto.*

Artículo 36 Reglamento UE 2016/679
Consulta previa

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*** *(pag 27-28) muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.*

2.*Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el* ***artículo 58*** *(ver en Anexo 2 pag. 61-62). Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.*

3.*Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:*

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en ***el artículo 35*** *(pags 27-28)*

y f) cualquier otra información que solicite la autoridad de control.

4*.Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria*

5*.No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.*

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.*

Artículo 36 LOPDGDD.
Posición del delegado de protección de datos.

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en **el artículo 5 ("Deber de confidencialidad") de esta ley orgánica** (ver pag 32)**.**

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37 LOPDGDD.
Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.
En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.
Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII ("Procedimientos en caso de posible vulneración de la normativa de protección de datos") de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

3. RESUMEN Y CONCLUSIONES

1.La LOPDGDD se ocupa del conjunto de datos personales.

Como en esta revisión nos interesa el contenido relacionado con la sanidad, **las referencias sanitarias directas** se encuentran en la disposición adicional decimoséptima y en la disposición final novena de la Ley *(ver apartado 2.3 del presente texto).* El Reglamento UE 2016/679 aporta muchos temas de interés sanitario y que hemos transcrito en el texto, al tratarse de referencias que están en el articulado de la LOPDGDD.
Los supuestos de tratamientos de datos por razones de salud, deberán estar amparados en una norma con rango de ley, lo que a su vez comporta que la vigencia de buena parte de las abundantes previsiones reglamentarias existentes en esta materia queden en entredicho.

2. Las bases jurídicas para el tratamiento de datos relacionados con la salud figura en los artículos 8 y 9 la LOPDGDD (pags 10-11) , complementado por los artículos 6 (en pags. 6,18 y 19) y 9 (en pag 11) del Reglamento UE 2016/679. Quedan bien delimitados las categorías especiales de datos personales y junto a la prohibición de su tratamiento, también se especifican las razones que permiten el manejo de dichos datos especiales.

3. En lo que respecta al ejercicio de los derechos, el Capítulo II de la LOPDGDD con el articulado que lo integra (pags 13-20), está basado en el Capítulo III del Reglamento UE 2016/679. Los derechos se aplican a todas las materias que incorporan tratamiento de datos, tanto sanitarias como de otros ámbitos. Destacamos que el conocido como "derecho al olvido" no es universal para todo tipo de datos; en el caso de los datos sanitarios la supresión completa no es un derecho absoluto.

4. La disposición adicional decimoséptima (pags 22-30) **analiza el tratamiento de datos con fines de investigación en salud,** estableciendo como regla general, que el tratamiento de datos con estas finalidades exige que el interesado haya otorgado su consentimiento. En todo caso, para llevar a cabo un tratamiento con fines de investigación en salud pública, el legislador obliga a realizar una evaluación de impacto que determine los riesgos derivados del tratamiento, someter la investigación científica a normas de calidad, y adoptar medidas dirigidas a garantizar que los investigadores no accedan a datos de identificación.
La citada disposición adicional distingue entre:
a) Tratamiento de datos sanitarios por autoridades sanitarias con competencias en vigilancia de la salud pública.
b) Reutilización de datos personales con fines de investigación.
c) Seudonimización de datos personales con fines de investigación en salud.

5. La disposición final novena (pag 31) **modifica el apartado 3 del artículo 16 de la Ley 41/2002 de 14 de noviembre.** Con esta nueva redacción, *el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación, o de docencia, obliga a preservar los datos de identificación personal del paciente separados de los datos de carácter clínico asistencial,* de manera que, como regla general, queda asegurado el anonimato salvo que el propio paciente haya dado su consentimiento para no separarlos.

6. El tratamiento de los datos personales, incluidos los datos de carácter sanitario, están sometidos al **deber de confidencialidad** (pags 32-33)por parte tanto de los responsables y

encargados del tratamiento, como de todas las personas que intervengan en cualquier fase de éste.
En el tratamiento de datos para fines de medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario, gestión de sistemas y servicios de asistencia sanitaria, o razones de interés público en el ámbito de la salud pública, dicho tratamiento ha ser realizado por un profesional sujeto a la obligación de secreto profesional o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros.

7. El tratamiento de los datos personales de un menor de edad (pag 34), únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años.
Los titulares de la patria potestad podrán ejercitar en nombre y representación de los **menores de catorce años** los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

8. En lo que respecta al tratamiento de datos personales de personas fallecidas (pags 35-36), las personas vinculadas a la fallecida por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.
Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

9. Las figuras de los **responsables o encargados del tratamiento** (pags 37-41) de los datos están bien definidos por el Reglamento UE 2016/679. En la LOPDGDD se definen las obligaciones generales de ambos, tomando como base el articulado relacionado del citado Reglamento y se destaca en el texto de la ley los riesgos que pue den producirse en muchos supuestos que contravienen el uso correcto en el tratamiento de datos.

10. El capítulo III de la LOPDGDD se refiere al Delegado de Protección de Datos (pags 42-46) con cuatro artículos (del 34 al 37 y completados con otros del Reglamento UE) y se refieren a su designación, entre otras numerosas entidades, a los centros sanitarios legalmente obligados al mantenimiento de historias clínicas; a su cualificación; a su posición dentro de la entidad que se trate y finalmente a su intervención en caso de reclamación ante las autoridades de protección de datos.
Es destacable que en el ejercicio de sus funciones el DPD tendrá acceso a los datos personales y procesos de tratamiento sin los límites que establecen el deber de confidencialidad o secreto. Si aprecia una vulneración relevante en materia de protección de datos ha de comunicarlo a los órganos de administración y dirección del responsable o del encargado del tratamiento.

4. BIBLIOGRAFÍA

1. Constitución Española de 1978. Publicada en: Boletín Oficial del Estado número 311, de 29/12/1978.
Última modificación: 27 de septiembre de 2011
Disponible en:
https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

2. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
Última modificación: 23 de junio de 2010
Disponible en:
https://www.boe.es/buscar/pdf/1982/BOE-A-1982-11196-consolidado.pdf

3. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.
Disponible en:
https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

El Artículo 94 del Reglamento UE 2016/679 deroga a la Directiva 95/46/CE:
1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.
2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

4. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Última modificación: 2 de marzo de 2019
Disponible en:
https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

5. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Publicada en: BOE número 298, de 14/12/1999. Última modificación: 6 de diciembre de 2018.
Norma derogada, con efectos de 7 de diciembre de 2018, sin perjuicio de lo previsto en las disposiciones adicional 14 y transitoria 4 de la Ley Orgánica 3/2018, de 5 de diciembre, según establece su disposición derogatoria única (los artículos 22, 23 y 24 siguen en vigor). Ref. BOE-A-2018-16673
Disponible en:
https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

6. Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)
Disponible en:
https://www.boe.es/doue/2002/201/L00037-00047.pdf

7. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
Última modificación: 6 de diciembre de 2018.
Disponible en:
https://www.boe.es/buscar/pdf/2002/BOE-A-2002-22188-consolidado.pdf

8. Ley 14/2007, de 3 de julio, de Investigación biomédica.
Última modificación: 2 de junio de 2011
Disponible en:
https://www.boe.es/buscar/pdf/2007/BOE-A-2007-12945-consolidado.pdf

9. Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD).
Publicada en: Boletín Oficial del Estado número 17, de 19/01/2008.
Última modificación: 8 de marzo de 2012.
Disponible en:
https://boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

Este Real Decreto 1720/2007 no está derogado en su totalidad, sino únicamente aquellas disposiciones que "contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la LOPDGDD."
Tampoco estarán derogadas aquellas disposiciones del Real Decreto 1720/2007 que desarrollen los artículos 22, 23 y 24 de la LOPD 15/1999 que siguen en vigor conforme a la disposición derogatoria única de la LOPDGDD.

10. Ley 33/2011, de 4 de octubre, General de Salud Pública.
Última modificación: 28 de marzo de 2014
Disponible en:
https://www.boe.es/buscar/pdf/2011/BOE-A-2011-15623-consolidado.pdf

11. 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).
Disponible en:
https://www.boe.es/doue/2016/119/L00001-00088.pdf

12. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Publicado en: «BOE» núm. 294, de 6 de diciembre de 2018.
Referencia: BOE-A-2018-16673. Última modificación: 25 de junio de 2019.
Disponible en:
https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

13. Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
Disponible en:
https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751
Norma derogada, con efectos de 7 de diciembre de 2018, por la disposición derogatoria única de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales.. Ref. BOE-A-2018-16673

14. Lomas Hernández V. Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre,
de Protección de Datos Personales y Garantía de los Derechos Digitales desde la perspectiva sanitaria. Rev Esp Soc Informatica y Salud 2019;134: 7-11.
Disponible en (nº completo de la revista):
https://seis.es/is-134-abril-2019/
15. Autoritat Catalana de Protecció de Dades (APDCAT). Guia de protección de datos para pacientes y personas usuarias de los servicios de salud. Junio 2020
Disponible en:
https://docs.google.com/viewerng/viewer?url=https://apdcat.gencat.cat/web/.content/03-documentacio/documents/Guia-proteccio-de-dades-pacients-v14-CAST.pdf&chrome=false&dov=1

5. ANEXOS
5.1. DEFINICIONES

El Reglamento UE 2016/679 en su **Artículo 4 "Definiciones"**, enumera las siguientes:

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;

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 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;

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 presente 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 presente Reglamento;

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

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

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

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

22) Autoridad de control interesada:
la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control;

23) Tratamiento transfronterizo:
a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro,

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

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

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

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

5.2. CITAS DE TERCER NIVEL EN EL ARTICULADO DEL DOCUMENTO.

1. Del artículo 46 Reglamento UE (pags 23-24 texto):

a) **Artículo 45** Reglamento UE, Transferencias basadas en una decisión de adecuación, **apartado 3** (citado en pag. 23 del texto):

3.La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el **apartado 2 del presente artículo**. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el **apartado 2, letra b**, del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el **artículo 93**, **apartado 2** (ve adelante).

Artículo 45 Reglamento UE apartado 2

2.Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:
a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros,

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

b) Artículo 93 apartado 2 reglamento UE. Procedimiento de Comité (varias citas: pags 23-24 y otras)

1.La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del **Reglamento UE nº 182/2011**.

Artículo 3 Reglamento UE 182/2011
Disposiciones comunes

1. Las disposiciones comunes establecidas en el presente artículo se aplicarán a todos los procedimientos mencionados en los **artículos 4 a 8.**

2. La Comisión estará asistida por un comité compuesto por representantes de los Estados miembros. El comité estará presidido por un representante de la Comisión. El presidente no participará en las votaciones del comité.

3. El presidente presentará al comité el proyecto de acto de ejecución que la Comisión deba adoptar. Salvo en casos debidamente justificados, el presidente convocará una reunión en un plazo no inferior a 14 días a partir de la presentación al comité del proyecto de acto de ejecución y del proyecto de orden del día. El comité emitirá su dictamen sobre el proyecto de acto de ejecución en un plazo que el presidente podrá fijar en función de la urgencia del asunto. Los plazos deberán ser proporcionados y brindar a los miembros del comité la oportunidad de examinar con la suficiente antelación y de forma efectiva el proyecto de acto de ejecución y de expresar sus opiniones.

2.Cuando se haga referencia al presente apartado, se aplicará **el artículo 5 del Reglamento UE nº 182/2011.**

Artículo 5 Reglamento UE 182/2011
Procedimiento de examen

1. Cuando se aplique el procedimiento de examen, el comité emitirá su dictamen por la mayoría prevista en el artículo 16, apartados 4 y 5, del Tratado de la Unión Europea y, cuando proceda, en el artículo 238, apartado 3, del TFUE, para los actos que deban adoptarse a partir de una propuesta de la Comisión. Los votos de los representantes de los Estados miembros en el comité se ponderarán del modo establecido en dichos artículos.

2. Cuando el comité emita un dictamen favorable, la Comisión adoptará el proyecto de acto de ejecución.

3. Sin perjuicio de lo dispuesto en el artículo 7, si el comité emite un dictamen no favorable, la Comisión no adoptará el proyecto de acto de ejecución. Cuando se considere necesario un acto de ejecución, el presidente podrá, bien presentar al mismo comité una versión modificada del proyecto de acto de ejecución en el plazo de dos meses a partir de la emisión del dictamen no favorable, bien presentar al comité de apelación para una nueva deliberación el proyecto de acto de ejecución en el plazo de un mes a partir de dicha emisión.

4. En ausencia de dictamen, la Comisión podrá adoptar el proyecto de acto de ejecución, salvo en los casos contemplados en el párrafo segundo. Si la Comisión no adopta el proyecto de acto de ejecución, el presidente podrá presentar al comité una versión modificada del mismo. Sin perjuicio de lo dispuesto en el artículo 7, la Comisión no adoptará el proyecto de acto de ejecución cuando:

a) dicho acto se refiera a la fiscalidad, los servicios financieros, la protección de la salud o la seguridad de las personas, los animales o las plantas, o medidas de salvaguardia multilaterales definitivas;

b) el acto de base establezca que el proyecto de acto de ejecución no podrá ser adoptado si no se ha emitido un dictamen, o

c) se oponga a ello una mayoría simple de los miembros que componen el comité. En cualquiera de los casos mencionados en el párrafo segundo, cuando se considere necesario un acto de ejecución, el presidente podrá, bien presentar al mismo comité una versión modificada del mismo en el plazo de dos meses a partir de la votación, bien presentar al comité de apelación para una nueva deliberación el proyecto de acto de ejecución en el plazo de un mes a partir de la votación.

5. No obstante lo dispuesto en el apartado 4, se aplicará el siguiente procedimiento para la adopción de proyectos de medidas antidumping o compensatorias definitivas en los casos en que el comité no haya emitido un dictamen y una mayoría simple de los miembros que lo componen se oponga al proyecto de acto de ejecución. La Comisión realizará consultas con los Estados miembros. A los 14 días como muy pronto y al mes como muy tarde de la reunión del comité, la Comisión informará a los miembros de los resultados de esas consultas y presentará un proyecto de acto de ejecución al comité de apelación. No obstante lo dispuesto en el artículo 3, apartado 7, el comité de apelación se reunirá a los 14 días como muy pronto y al mes como muy tarde de la presentación del proyecto de acto de ejecución. El comité de apelación emitirá su dictamen con arreglo al artículo 6. Los plazos establecidos en el presente apartado se entenderán sin perjuicio de la obligación de respetar los plazos fijados en los actos de base pertinentes.

3.Cuando se haga referencia al presente apartado, se aplicará el **artículo 8** del Reglamento (UE) nº 182/2011, **en relación con su artículo 5** (ver antes).

c) Artículo 40 Reglamento UE. Códigos de conducta (citado en pag. 24 del texto)

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, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los **artículos 24** (pags. 37-38) **y 25** (pag. 38) y las medidas para garantizar la seguridad del tratamiento a que se refiere el **artículo 32** (ver pag. 39-40);

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales,

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los **artículos 77 y 79**.

Artículo 77 Reglamento UE 2019/679
Derecho a presentar una reclamación ante una autoridad de control

1.Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2.La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del **artículo 78**.

Artículo 79 Reglamento UE 2016/679
Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

1.Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del **artículo 77**, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2.Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

3.Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del **artículo 46, apartado 2, letra e** (ver en pag. 24) 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.

4.El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el **artículo 41, apartado 1** (ver pag siguiente), efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de

tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al **artículo 51 o 56** (ver pag siguiente)

Artículo 41 Reglamento UE 2016/679
Supervisión de códigos de conducta aprobados

1.Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

Artículo 51 Reglamento UE 2016/679
Autoridad de control

1.Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») 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, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63. 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.

Artículo 56 Reglamento UE 2016/679
Competencia de la autoridad de control principal

1.Sin perjuicio de lo dispuesto en el **artículo 55** (ver adelante), la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el **artículo 60** (ver pag.66-67)

2.No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3.En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4.En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el **artículo 60** (ver pag. 66-67). La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el **artículo 60, apartado 3** (ver pag 66).

5.En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los **artículos 61 y 62.**

6.La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado

5.Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al **artículo 55** (ver adelante)**.** La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

Artículo 55 Reglamento UE 2016/679
Competencia

1.Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.

2.Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el **artículo 56** (ver pag. anterior)

3.Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

6.Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7.Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del **artículo 55** (ver anterior) lo presentará por el procedimiento mencionado en el **artículo 63** (ver en pag. 62)**,** antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8.Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9.La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el **artículo 93, apartado 2** (ver pag 56-57)

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11.El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

d) Artículo 42 Certificación (citado en pag 24 del texto)

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.

2.Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del **artículo 46, apartado 2, letra f** (ver pag. 24) 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.

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

4.La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin

perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del **artículo 55** (pag 59-60) **o 56** (ver en pag. 59).

5.La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el **artículo 43** (ver adelante) o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el **artículo 58, apartado 3** (ver adelante), o por el Comité de conformidad con el **artículo 63** (pag. 62). Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

Artículo 43 Reglamento UE 2016/679
Organismo de certificación

1.Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del **artículo 55** (pag 59-60) o **56** (pag 59) ;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.o 765/2008 del Parlamento Europeo y del Consejo (1) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2.Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el **artículo 42, apartado 5** (ver al inicio de la pag) y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el **artículo 63** (pag 62)

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

……..Este art. sigue con apartados del 3 al 9…..

Artículo 58.3 Reglamento UE
Poderes

3.Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el **artículo 36** (en pag 45 del texto);

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el **artículo 36, apartado 5** (pag 45 del texto) si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el **artículo 40, apartado 5** (pag. 59)

e) acreditar los organismos de certificación con arreglo al **artículo 43** (pag 61)

f) expedir certificaciones y aprobar criterios de certificación con arreglo al **artículo 42, apartado 5** (esta pag. al inicio)

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

6.Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el **artículo 43** (pag 61), o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

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** (pag 61), 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.

8.El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

e) Artículo 63: Mecanismo de coherencia (citado en pag 24 del texto)

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

f) Artículo 26 Directiva 95/46/UE: Excepciones (citado en pag 24 del texto)

1. No obstante lo dispuesto en el **artículo 25** y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el **apartado 2 del artículo 25**,

Artículo 25 Directiva 95/46/UE
Principios

1 . Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2 . El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos , la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final , las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3 . Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4 . Cuando la Comisión compruebe , con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5 . La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4 .

6 . La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el **apartado 2 del artículo 31** , (pag. 63) que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del

presente artículo o, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas .

siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista , o, b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado v el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado,

o, c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero,

o, d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial ,

o, e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado ,

o, f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado **2 del artículo 25** (ver antes), cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2. En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el **apartado 2 del artículo 31**. Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 31 Directiva 95/46/UE
El Comité

1 . La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión .

2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate. El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación .
La Comisión adoptará las medidas que serán de aplicación inmediata . Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:
— la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;
— el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guion .

4. Cuando la Comisión decida, según el procedimiento establecido en el **apartado 2 del artículo 31**, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

2. Del artículo 47 Reglamento UE (pag 24-25 del texto)

Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado (citado en pag. 25 del texto)

1.Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los **artículos 46** (pags 23-24) **o 47** (pags. 24-25) **o el artículo 49 apartado 1**, **párrafo segundo** (pag 25), referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el **artículo 6, apartado 1, letra f** (pag 19)**,** los intereses legítimos del responsable del tratamiento o de un tercero;

c) 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, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el **artículo 6, apartado 1, letra a** (pag 18)**,** o el **artículo 9, apartado 2, letra a** (pag 11)**,** la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el **artículo 22, apartados 1 y 4** (pag 15)**,** y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3.El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado,

o c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5.Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el **artículo 89, apartado 1** (pag 12), o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado,

o d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

3. Del artículo 68 Reglamento UE (pag 28 del texto)

Artículo 65 Reglamento UE citado en pag 28 del texto

Artículo 65 Reglamento UE
Resolución de conflictos por el Comité

1.Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el **artículo 60, apartado 4** (pag 66) una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de

decisión de la autoridad principal, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

Artículo 60, Reglamento UE
Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas

1.La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2.La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3.La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4.En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el **artículo 63** (pag 62).

5.En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6.En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7.La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8.No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9.En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10.Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11.En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12.La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el **artículo 64, apartado 1**, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

Artículo 64 apartado 1 Reglamento UE
Dictamen del Comité

1.El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el **artículo 40, apartado 7** (pag 58), cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo con arreglo al **artículo 41, apartado 3** (pag 57) , o un organismo de certificación conforme al artículo **43, apartado 3** (pag 59) ;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el **artículo 46, apartado 2, letra d** (pag 23)**,** y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el **artículo 46, apartado 3, letra a** (pag 24)**;**

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del **artículo 47** (pag 24-25).

2.La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3.Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4.Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5.El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6.La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un

mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del tratamiento y al interesado, respectivamente.

La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el **artículo 60, apartados 7, 8 y 9** (ver pag 66)**.**

La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

5.3. PREGUNTAS RELACIONADAS CON LA PROTECCIÓN DE DATOS

Seleccionadas de la "Guía de protección de datos para pacientes y personas usuarias de los servicios de salud" de la APDCAT (cita bibliográfica, 15), con corrección del lenguaje para ser inclusivo y adaptación a las características locales.

1. Derechos de los pacientes con respecto a sus datos

Cualquier persona tiene derecho a ser informada sobre lo que se hará con sus datos de salud, en el momento en que se recogen.
Aparte de ello, ya sea ella misma o a través de sus representantes, puede ejercer los derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos personales, enviando una solicitud al responsable o centro sanitario donde la hayan atendido.
Los centros sanitarios deben responder siempre a la solicitud de las personas en el plazo de un mes, cualquiera que sea el sentido de la respuesta.
Los centros sanitarios deben tener en cuenta el criterio médico de los profesionales que atienden a la persona enferma, a la hora de decidir, por ejemplo, si se entrega una determinada información (por ejemplo, si se trata de anotaciones subjetivas), si se elimina o si se modifica información de una historia clínica, a petición de la misma.

2. El derecho de la persona afectada a ser informado sobre el uso de sus datos

Cuando los datos se recogen de la misma persona, ya sea porque ella los declara o porque se obtienen a raíz de una exploración o prueba médica, es necesario informarle de lo siguiente:
• Si es imprescindible o no facilitar los datos.

• Quién es el responsable del tratamiento (el hospital, SVS, laboratorio de análisis clínicos, un centro de investigación, etc.).

• Los datos de contacto del delegado de protección de datos (DPD).

• Para qué se utilizarán los datos (asistencia sanitaria, investigación biomédica, prevención de riesgos laborales, etc.) y qué les permite hacerlo (el consentimiento del paciente, una ley, la atención sanitaria de los hijos en el colegio, etc.).

• Qué datos se tratarán (identificativos, de características personales, de salud, económico-financieros i de seguros, profesionales y de ocupación laboral, etc.).

• Los destinatarios de los datos (Administración pública, otros centros sanitarios, etc.).

• Si los datos se transferirán a países fuera del Espacio Económico Europeo, y en virtud de qué instrumento.

• Cuánto tiempo se conservarán los datos. Si no se puede concretar el plazo, hay que informar de los criterios que se utilizarán para establecerlo.

• Qué derechos tiene, incluido, si procede, el derecho a retirar el consentimiento en cualquier momento.

• Si con los datos se tomará algún tipo de decisión automatizada, incluida la elaboración de perfiles. Debe incluirse información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de este tratamiento para la persona afectada.

3. ¿El derecho de información previsto en la normativa de protección de datos es el mismo que el consentimiento informado en el ámbito sanitario?

No. Se trata de dos derechos de información diferentes:

• El consentimiento informado en el ámbito sanitario hace referencia al deber de recoger el consentimiento de las personas que deben someterse a determinadas intervenciones más o menos invasivas sobre su cuerpo (exploraciones, análisis clínicos, biopsias, intervenciones quirúrgicas, curas, tratamientos médicos, etc.).
Es necesario explicar a la propia persona en qué consistirá la actuación para que pueda decidir y autorizar si se somete a ella o no.

• El derecho de información que prevé la legislación de protección de datos personales es un derecho de todas las personas enfermas. Los centros sanitarios no tienen que solicitar el consentimiento para tratar los datos que les faciliten las mismas para atenderles, pero sí tienen la obligación de explicarles cómo utilizarán sus datos.

4. El derecho a obtener información sobre la propia salud: derecho de acceso

La normativa de protección de datos personales reconoce el derecho de la persona afectada acceder a su historia clínica en cualquier momento, así como a obtener una copia gratuita de los datos o documentos que allí figuran (documentación en soporte papel, electrónico, audiovisual, etc.). Además, también tiene derecho a obtener la siguiente información:

• Los fines del tratamiento.
• Las categorías de datos personales de que se trata.
• Los destinatarios o las categorías de destinatarios a quienes se han comunicado o se comunicarán los datos personales, en particular destinatarios en terceros países o en organizaciones internacionales.
• El plazo previsto de conservación de los datos personales. Si ello no es posible, los criterios utilizados para determinarlo.
• El derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos personales o la limitación del tratamiento de datos o a oponerse a él.
• El derecho a presentar una reclamación ante la Delegación de Protección de Datos de la Generalitat Valenciana (GVA).
• El origen de los datos, cuando no se han obtenido del propio paciente.
• La existencia de decisiones automatizadas, incluida la elaboración de perfiles, (información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de este tratamiento para el paciente).
• Cuando se transfieren datos personales a un tercer país o a una organización internacional, las garantías adecuadas relativas a la transferencia.

En ocasiones, la información sobre nuestra salud puede estar contenida en la historia clínica de otra persona, lo que nos daría la posibilidad de acceder a dicha información, ya que se trataría de nuestros propios datos. Este es el caso, por ejemplo, de la información sobre los hijos recién nacidos que se recoge en la historia clínica de la madre biológica, o de la historia clínica que se abre en los centros de reproducción asistida, que contienen información de diferentes personas que deben poder acceder a su propia información.

5. ¿El derecho de acceso previsto en la normativa de protección de datos permite conocer qué profesionales han accedido a la historia clínica?

El derecho de acceso previsto en la normativa de protección de datos no prevé que se deba dar esta información. Sólo prevé que hay que facilitarlo cuando la información se ha comunicado a otras entidades o personas externas.
Sin embargo, algunos centros lo han establecido como una buena práctica. Además, en el caso de las administraciones públicas, la normativa sobre acceso a la información pública también puede permitir a los pacientes acceder a ella, dado su interés legítimo en conocerla.

6. ¿Se puede excluir información del derecho de acceso a la historia clínica?

En ocasiones la persona afectada no debe conocer todo lo que incluye su historia clínica, ya sea por su propio interés o por el de otras personas:

a) El acceso de la persona a su información de salud se puede limitar cuando los profesionales que lo atienden consideren que hay un estado de necesidad terapéutica (por ejemplo, si el personal médico cree que el conocimiento de determinadas informaciones sobre la propia enfermedad puede ser gravemente perjudicial para la persona y contraproducente para su recuperación). En estos casos, el personal médico debe hacer constar esta circunstancia en la historia clínica y tiene que informar a las personas vinculadas a la afectada por razones familiares o de hecho.

b) El o la paciente no puede ejercer el derecho de acceso a la documentación de la historia clínica en perjuicio del derecho de terceras personas a la confidencialidad de sus datos.
A menudo, las personas cercanas al/la paciente aportan informaciones en interés terapéutico del/ de la paciente que el/la médico puede incorporar a la historia clínica. Estas personas tienen derecho a que, si procede, se proteja la confidencialidad de esta información y, por tanto, la persona enferma no llegue a conocerla. Por ejemplo, si un familiar comunica al personal médico la sospecha de que el /la paciente consume drogas o alcohol o que no se toma la medicación prescrita.

c) El personal facultativo puede limitar el acceso del paciente a las anotaciones subjetivas que ha incorporado a la historia clínica. Las anotaciones subjetivas son impresiones o valoraciones personales que los profesionales sanitarios consideran de interés para la atención sanitaria del / de la paciente, no sustentadas directamente en datos objetivos o en pruebas médicas que lo corroboren. Sería el caso de sospechas de incumplimientos terapéuticos o de tratamientos no declarados, de hábitos no reconocidos, que los síntomas referidos son inciertos o exagerados o que la persona afectada no dice la verdad; también de

observación de comportamientos insólitos o de hábitos sociales poco habituales que dificulten la relación con los profesionales, o actitudes o comportamientos del entorno del paciente que dificulten esta relación, etc.
Si la autoridad judicial solicita conocer el contenido de las anotaciones subjetivas, el centro sanitario o en su caso, el personal responsable de la atención, deberá entregárselas. El resto de profesionales asistenciales que tienen que tratar al /la paciente también deben poder conocerlas.

7. ¿Tengo derecho a conocer mis orígenes biológicos, aunque ello suponga acceder a información de la madre biológica?

Sí. El derecho a conocer los propios orígenes biológicos incluye el derecho a conocer la identidad de los progenitores biológicos. Este derecho se reconoce a los niños y a los adolescentes desamparados (personas adoptadas, tuteladas o extuteladas por la Administración) una vez han alcanzado la mayoría de edad o se han emancipado. Los solicitantes deben poder acceder a determinada información de la historia clínica de la madre biológica que pueda ser relevante para su propia salud.

8. ¿Puede el hospital facilitar mi historia clínica a mi abogado para presentar una reclamación?

Para obtenerla, el abogado que representa a un /una paciente debe acreditar su identidad y la habilitación frente al centro sanitario, ya sea a través de un formulario del centro o bien aportando poderes notariales otorgados por el paciente. A parte de esta cuestión, ningún centro sanitario puede denegar el derecho de acceso a una persona por el hecho de que quiera reclamar contra el hospital, ni dicha persona tiene la obligación de explicar al centro sanitario el motivo de su solicitud de acceso.

9. ¿Puede un pariente biológico acceder a mi historia clínica?

A menudo, la información sobre la salud de una persona no sólo afecta a dicha persona, sino también a sus parientes biológicos. Por ejemplo, la información genética relacionada con una enfermedad hereditaria es información de toda la "familia genética" de la persona afectada. Ello puede justificar que, en caso de riesgo para la salud del familiar biológico, éstos puedan acceder a algunos datos de la historia clínica de la persona con la enfermedad.

10. El derecho a que se rectifiquen o se supriman datos de nuestra historia clínica: derecho de rectificación y derecho de supresión.

Cualquier persona tiene derecho a pedir al responsable que modifique algún dato erróneo o que haya quedado obsoleto. Es el llamado derecho de rectificación.
En determinados supuestos también se puede solicitar que se suprima una información o dato personal. Por ejemplo, si el tratamiento es ilícito, si ya se ha alcanzado la finalidad perseguida o se ha retirado el consentimiento, cuando ésta es la única base jurídica del tratamiento (derecho de supresión o derecho al olvido).
El ejercicio de los derechos de rectificación o de supresión suele presentar poca complejidad, si lo que se quiere modificar es una dirección o un teléfono debido a un cambio de domicilio, o bien los datos bancarios, información laboral o profesional, etc.

Sin embargo, en el ámbito sanitario, la petición de cambiar o suprimir datos clínico-asistenciales (la referencia a un episodio clínico concreto o a una intervención quirúrgica de hace unos años, etc.) requiere que los/las profesionales sanitarios analicen las circunstancias de cada caso, siempre desde el criterio médico, para valorar si este cambio puede condicionar o perjudicar la asistencia sanitaria la persona.
Los centros sanitarios deben analizar las circunstancias de cada caso, desde la perspectiva del criterio del personal médico y del interés terapéutico de la persona que ha recibido la atención.

La ley obliga al responsable a bloquear los datos que se han rectificado o suprimido. Esto significa guardarlos fuera de los circuitos habituales de trabajo, de manera que nadie los pueda consultar o utilizar. Sólo deben permanecer a disposición de las autoridades judiciales, de las administraciones públicas competentes o de las autoridades de protección de datos para exigir las responsabilidades que procedan. Una vez que han prescrito las posibles responsabilidades legales la información del paciente ya puede ser destruida físicamente.

11. Recientemente me trataron en un Centro de Salud lejos de mi residencia, y no creo que me vuelvan a atender en el futuro. ¿Puedo solicitar ya la supresión de todos mis datos?

No. Aunque no se prevea que en el futuro se vuelva a recibir asistencia en este centro, la ley obliga a conservar parte de la información durante cinco o quince años, o incluso un período superior según el documento de que se trate, a contar desde la fecha de la atención recibida. Cuando se trata de centros de la red pública asistencial, durante este período la información puede estar a disposición de otros centros asistenciales de la red a través de la historia electrónica.

12. ¿Puedo solicitar la supresión de cualquier información que aparezca en mi historial médico sobre mi tratamiento de reproducción asistida y donación de óvulos?

No. La ley reconoce a la infancia y adolescencia el derecho a conocer su origen genético y a solicitar a las administraciones públicas competentes la documentación que les permita demostrar su identidad. Esto significa que es necesario mantener la información sobre la donación de embriones en la historia clínica de la madre y, en consecuencia, esta información no puede ser eliminada. De todos modos, la madre puede solicitar que nadie más, aparte de los niños y niñas, acceda a esta información.

13. Cuando hay una causa de supresión, ¿los datos deben ser destruidos físicamente en ese momento?

No. En caso de rectificación o supresión de datos, la normativa de protección de datos impone el deber de bloquearlos. Esto implica la identificación y reserva de los datos fuera de los circuitos de trabajo ordinarios y la adopción de medidas que impidan el tratamiento para que sólo estén a disposición de los jueces y tribunales, del Ministerio Fiscal o de las administraciones públicas competentes; en particular de las autoridades de protección de datos, para exigir posibles responsabilidades derivada del tratamiento y sólo hasta que dichas responsabilidades prescriban.

14. En un informe incluido en mi historia clínica hay un error en la fecha de una intervención quirúrgica y en el equipo médico que me asistió. ¿Puedo solicitar que lo modifiquen?

Es importante que la historia clínica refleje adecuadamente y de manera veraz las circunstancias relevantes de los procesos de atención a pacientes. Los errores en la fecha de la intervención o en la identificación del personal médico responsable pueden afectar negativamente al tratamiento de atención actual y futuro (por ejemplo, el personal facultativo pueden prevenir si la recuperación de la persona enferma entra en normalidad, o puede impedirle contrastar la información con los el personal sanitario que le asistió). Por lo tanto, la información se debe rectificar. Si no se hace, la persona puede acudir a la Delegación de Protección de Datos GVA y presentar una reclamación de tutela de derechos.

15. El derecho a llevar los datos a otro proveedor de servicios de salud: derecho de portabilidad.

La normativa de protección de datos reconoce el derecho a solicitar al personal responsable la información que la persona paciente ha facilitado previamente, en un formato estructurado, de uso común y lectura mecánica que permita su entrega a diferente personal responsable (derecho a la portabilidad de los datos).
La ley contempla esta posibilidad sólo si el tratamiento de los datos se basa en el consentimiento de la persona o en la ejecución de un contrato, y cuando la información está automatizada.
Sin embargo, no puede aplicarse cuando los datos se utilizan en el marco de una misión realizada en interés público, como es el caso de la red asistencial pública.
Si en los documentos que se transfieren a petición de la persona existen datos de otras personas (profesionales que han atendido, personal administrativo del centro médico, familiares de la persona paciente, etc.), esta información debe ser excluida de la documentación que se proporciona.

16. El derecho a limitar el tratamiento de datos: derecho de limitación

En determinados casos en que exista un conflicto entre una persona y un centro sanitario, dicha persona podrá ejercer el derecho a limitar el tratamiento, es decir, podrá solicitar que sus datos personales no sean tratados:
• Mientras el centro decide sobre la exactitud de los datos o si es apropiado ejercer el derecho de oposición.

• Cuando la persona desea que los datos se conserven incluso si el tratamiento puede ser ilícito o innecesario.

• Cuando quien es responsable del tratamiento ya no necesita los datos, pero la persona los necesita para llevar a cabo reclamaciones o defenderse de ellas.

Los datos afectados por la limitación sólo pueden continuar utilizándose si a quien le afectan lo autoriza, o bien para presentar reclamaciones o proteger los derechos de otras personas afectadas.

17. El derecho a oponerse a que se utilicen nuestros datos: derecho de oposición

Una persona puede manifestar la voluntad, por razones relacionadas con su situación particular, de que ciertos datos sanitarios no estén disponibles para diferentes profesionales sanitarios, que sólo puedan acceder a ellos profesionales de su propio centro asistencial, que no se utilizan para determinadas finalidades, que no se lleven a cabo otros tratamientos, etc. Quienes son responsables de la información deben cesar en el tratamiento a menos que demuestren razones legítimas imperiosas que deben prevalecer.
Dada la finalidad asistencial de la historia clínica, conviene no dificultar ni poner en peligro la atención sanitaria de la persona enferma.

18. Hace años sufrí una grave enfermedad mental grave. Me preocupa que esta información esté disponible para cualquier profesional del sistema sanitario. ¿Puedo oponerme a que todo el conjunto de profesionales accedan a ella? ¿Puedo exigir que se suprima de mi historia clínica cualquier referencia a este episodio?

La normativa sanitaria establece que los datos de la historia clínica sólo deben ser accesibles, con finalidades asistenciales, para el personal sanitario que deba tratar a la persona enferma y han de proteger y respetar la confidencialidad de dicha información.
Mediante el derecho de oposición la persona paciente podrá solicitar, por motivos relacionados con su situación particular, que no todo el personal profesional tenga acceso a este episodio de salud.
Sin embargo, este derecho puede ser limitado, si el centro sanitario puede demostrar que hay razones legítimas imperiosas que deben prevalecer (por ejemplo, si puede poner en peligro la asistencia sanitaria que recibe la persona o el buen funcionamiento del sistema de salud).
La concesión del derecho de oposición no implica necesariamente la supresión de la información, sino que, debido a la exigencia de la Ley de autonomía del paciente, hay que conservarla durante determinados períodos.

19. ¿Cómo podemos ejercer nuestros derechos?

Hay que dirigirse al personal responsable del tratamiento o al centro sanitario y explicar qué se solicita (acceder a información, rectificar o suprimir un dato, oponerse a un tratamiento en particular, etc.).
Se puede hacer directamente o por representación de un familiar, alguien de la abogacía o cualquier otra persona que actúe en nombre del interesado. La persona representante debe identificarse y acreditar que puede actuar en nombre de a quien representa.
El plazo de respuesta es de un mes, prorrogable a dos meses más, dependiendo de la complejidad y el número de solicitudes.
El responsable o centro sanitario podrá solicitar información adicional para poder identificar correctamente a quien lo solicita.
Si la solicitud es denegada, hay que indicar que la persona puede reclamar ante la Delegación de Protección de Datos GVA o a los órganos judiciales. También puede reclamar ante quien ejerza como delegado de protección de datos de la entidad.
El ejercicio de los derechos es gratuito, salvo que las solicitudes sean manifiestamente infundadas o repetitivas. En el caso del derecho de acceso se considera que la solicitud es

repetitiva si se ejerce más de una vez cada seis meses, a menos que exista una causa legítima, o si se solicitan varias copias de un documento. Si ello genera gastos para el centro sanitario, se puede cobrar un precio razonable.

20. ¿Puedo acceder la historia clínica de otra persona con poder notarial?

Sí. El Código Civil ofrece la posibilidad de otorgar poderes notariales a otra persona para actuar legalmente en nombre y representación del paciente. Pueden ser poderes especiales para ejercer los derechos relativos a los datos personales o poderes generales en los que también se haga referencia a otros ámbitos de actuación o de interés del titular.
También se puede acceder con una autorización firmada por la persona.
Por lo general, los centros sanitarios tienen formularios a disposición de quienes los soliciten.

21. La información personal es confidencial

La persona da a conocer al personal sanitario aspectos de su salud y de su vida personal y familiar que proporcionan mucha información sobre su situación, estilo de vida y hábitos que, en muchas ocasiones, pueden afectar a su intimidad y a la de terceras personas. Dicho personal es confidente necesario de la persona paciente y deben proteger esa confianza. Respetar el secreto profesional no es sólo un deber ético, sino una obligación legal.
En un centro sanitario hay diferentes perfiles de profesionales (personal administrativo, comerciales, informáticos, personal sanitario, personal investigador, el profesorado, estudiantes de ciencias de la salud, etc.). Cada uno de ellos debe acceder sólo a la información de las personas necesaria para llevar a cabo las tareas que se les encomienden. Quienes son profesionales de la salud están sujetos al secreto profesional. Diferentes profesionales que participen en el proceso asistencial pueden estar sujetos a una obligación de secreto equivalente. En cualquier caso, la normativa de protección de datos obliga a todas las personas implicadas en el tratamiento de la información a mantener la confidencialidad. La información no puede ser compartida o difundida con otras personas o entidades ajenas fuera de las circunstancias autorizadas.
En algunos casos excepcionales, el personal sanitario pueda estar obligado a tener que romper el secreto profesional cuando la ley lo prevé. Así, por ejemplo, cuando la ley lo prevea, el deber de denuncia puede obligarles a comunicar a jueces y tribunales, al Ministerio Fiscal o a las administraciones competentes hechos que conozcan en el ejercicio de sus funciones y que puedan ser delito.

22. Los centros y profesionales de la salud deben proteger nuestra información

Los centros sanitarios están obligados a adoptar las medidas necesarias para garantizar los derechos de las personas enfermas y la seguridad de los datos (confidencialidad, integridad y disponibilidad), a partir de un análisis de los riesgos del tratamiento en cada caso.
Una de las medidas que debe implementarse es un registro de los accesos a la historia clínica.
En este registro, para cada acceso deben constar los siguientes datos:
• Fecha en la que se accedió a la información.
• Centro sanitario desde el que se ha accedido.
• Identidad y categoría profesional de quien accede.

• Información consultada.

23. ¿El centro médico que me ha atendido puede proporcionarme información que solicito por teléfono sobre mi estado de salud o los resultados de las pruebas que me han realizado?

La comunicación de datos de salud por teléfono conlleva el riesgo de facilitar la información a un tercero que intenta suplantar la identidad de la persona enferma. Por este motivo, es necesario evitarlo, a menos que se hayan implementado protocolos para identificar de forma segura a quien solicita la información.

24. ¿Qué sucede cuando un centro sanitario no protege adecuadamente nuestra información?

El centro puede cometer una infracción de la normativa de protección de datos. La Delegación de Protección de Datos GVA puede imponer multas económicas a entidades privadas, o una amonestación y, si procede, imponer medidas correctoras a las entidades públicas.

Además, si un profesional sanitario revela información sobre una persona que conoce por su trabajo o sus relaciones laborales, puede cometer una infracción disciplinaria o, incluso, un delito contra la intimidad.

25. Soy personal de plantilla ya la vez paciente de un hospital. ¿Puede el personal del centro acceder a información sobre mi intervención quirúrgica?

No. A menos que estas personas estuvieran involucradas en la asistencia médica directa, el acceso sería indebido y vulneraría el principio de confidencialidad. El mero hecho de trabajar en un centro sanitario no permite el acceso a la dicha información, sin su consentimiento. El centro debe proporcionar las instrucciones apropiadas a todo el personal de plantilla sobre esta cuestión. La persona afectada puede reclamar ante la Delegación de Protección de Datos GVA o a las autoridades judiciales.

26. ¿Puede la familia de la persona paciente conocer su estado de salud?

Únicamente la persona enferma puede decidir si quiere que le informen sobre su estado de salud o si no lo quiere. También si prefiere que se informe a familiares, o que no reciban información de los médicos que lo atienden.
La ley permite que se comuniquen datos de salud de pacientes a las personas vinculadas, ya sea por motivos familiares o de hecho, que lo acompañan en el proceso asistencial, salvo que la persona paciente se oponga a ello.
En caso de incapacidad física o psíquica de pacientes, se debe informar a familiares o a las personas vinculadas. Por ejemplo, si una persona ingresa en un centro hospitalario en un estado de incapacidad física o psíquica, es necesario proporcionar información a familiares o personas más cercanas para que puedan tomar decisiones en su nombre.

27. He llamado a un hospital para pedir información sobre un familiar ingresado y no me la han proporcionado. ¿Han actuado correctamente?

Sí. Antes de proporcionar cualquier dato sobre el estado de salud de una persona ingresada, los centros sanitarios deben asegurarse de la identidad de la persona que llama, su relación con ella y, en su caso, de las indicaciones que esta le haya dado. De lo contrario, pueden vulnerar la intimidad de la persona ingresada.
Constituye una buena práctica que el centro pregunte qué personas de su confianza pueden recibir información, por ejemplo, sobre su evolución después de una intervención quirúrgica.

28.El hospital donde está ingresado un familiar ¿debe facilitarme su número de habitación?

El hospital puede proporcionar el número de la habitación (que es un dato que forma parte de la historia clínica) sólo a las personas vinculadas por motivos familiares o de hecho que lo acompañan durante el proceso asistencial. Para el resto de visitas, debe autorizarlo la propia persona paciente.

29. Tengo un familiar hospitalizado en un centro sanitario, que no tiene capacidad para decidir por sí mismo sobre su tratamiento médico. ¿Quién puede acceder a su información para decidir qué hay que hacer?

Cuando a criterio médico una persona enferma hospitalizada no tiene capacidad suficiente para tomar decisiones sobre su salud (por ejemplo, por un accidente grave o por una enfermedad mental), las personas que le representan o están vinculados a ella por motivos familiares o de hecho pueden acceder a su información.

30. ¿Puedo solicitar la historia clínica de un familiar difunto?

Sí. Las personas vinculadas por razones familiares o de hecho con la titular fallecida de la historia clínica pueden solicitar acceso a su información personal. Ello, a menos que existiera una prohibición expresa por parte de la persona que ha fallecido. El acceso de un tercero a la historia clínica motivado por un riesgo para la propia salud debe limitarse a los datos pertinentes. No hay que facilitar información que afecte a la intimidad de la persona fallecida ni a las anotaciones subjetivas del personal sanitario, o que perjudiquen a terceros.

31. ¿Quién puede tratar los datos de salud y para qué?

Para recoger y tratar datos personales, se necesita una base legal. En algunos casos, la base legal puede ser el consentimiento de la persona de que se trata; en otros, podrá ser cualquiera otra de las bases jurídicas previstas en el artículo 6 del Reglamento UE 679/2016. Además, en el caso de los datos de salud debe concurrir alguna de las excepciones previstas en el artículo 9.2 del Reglamento.
Los centros de la red asistencial pública, dada la misión de interés público que tienen encomendada, pueden tratar los datos de sus pacientes con el fin de proporcionarles asistencia sin necesidad de solicitarles el consentimiento. En los centros que no forman

parte de esta red, la base jurídica puede ser, por ejemplo, la necesidad de tratamiento para cumplir un contrato.
En los casos en que la base legal sea el consentimiento de la persona afectada, este consentimiento debe ser explícito. Esto no implica que el consentimiento deba proporcionarse siempre por escrito, pero la práctica habitual y más recomendable es que quede constancia por escrito o en otros soportes, como la grabación de audio o vídeo.

32. ¿Es suficiente consentir una sola vez para tratar mis datos para diferentes finalidades?

No. En el caso de los datos de salud, el consentimiento debe ser explícito con respecto a cada una de las finalidades. Es decir, debemos poder dar el consentimiento por separado sobre cada una, incluso aunque sea en un mismo documento, inequívocamente y después de haber sido informados sobre el tratamiento de los datos.
Por ejemplo, si un centro sanitario solicita el consentimiento para participar en un estudio clínico, el consentimiento dado por la persona es sólo para ese fin. Si, además, el centro desea enviarle publicidad sobre varias cuestiones, o quiere proponerle participar en un reportaje para una revista científica, etc., la persona debe dar el consentimiento para cada finalidad por separado.
El consentimiento puede proporcionarse a través de una declaración escrita, incluyendo medios electrónicos, o una declaración verbal. Un documento (en papel o electrónico) que ya tenga las casillas marcadas nunca es un consentimiento válido.

33. Tratamiento de datos para finalidades asistenciales

Esta es la finalidad principal de la historia clínica.
Los centros sanitarios y profesionales sanitarios de la red de salud pública no necesitan el consentimiento de sus pacientes para tratar los datos con el fin de proporcionarles atención sanitaria, ya que la ley les permite hacerlo.
En el caso de los centros privados, la contratación de sus servicios también permitiría el tratamiento de los datos de sus pacientes.
El acceso a una historia clínica con fines asistenciales sólo corresponde al personal que atiende a pacientes, ya sea individualmente o como parte de un equipo de profesionales. Los y las trabajadoras sociales que forman parte de los equipos de atención primaria también pueden acceder a la información de salud de pacientes, siempre que sea necesario para atenderles.

34. ¿Cualquier médico del Centro de Salud donde me atienden habitualmente puede ver mi información de salud?

No. El acceso a una historia clínica sin el consentimiento de las personas asistidas o sin una razón de salud que lo justifique, supone una vulneración del principio de confidencialidad de la información de dichas personas. Por lo tanto, el personal médico que, a pesar de trabajar en el mismo centro de salud, hospital, centro sociosanitario, residencia, etc., no están implicados en el tratamiento asistencial de las personas a su cargo, no deben acceder a los datos personales.

35. Sufro una enfermedad crónica y no puedo desplazarme, por lo que mi centro asistencial me ha ofrecido atenderme con sistemas de telemedicina. ¿Es seguro?

La introducción de sistemas de atención a distancia es cada vez más común, para controlar a pacientes crónicos, hacer el seguimiento de un tratamiento o cuando dichos pacientes no pueden trasladarse al centro asistencial.
La telemedicina permite controlar los síntomas y la evolución de la enfermedad, indicar qué medicación deben tomar, y controlar su salud física y mental. En algunos casos, esto puede incluir la entrega de dispositivos a dichos pacientes para que puedan utilizarlos en su domicilio (aparatos para medir la frecuencia cardíaca, la temperatura, la presión arterial, etc.).
Los servicios de salud que utilizan estas tecnologías deben garantizar un nivel de protección equivalente al que se ofrece en la atención presencial.
Por esta razón, deben aplicar las medidas técnicas y organizativas adecuadas que aseguren la confidencialidad, integridad y disponibilidad de la información, y que eviten los accesos indebidos a esta información.

36. Podemos utilizar soluciones basadas en inteligencia artificial para hacer un diagnóstico médico?

El uso de la inteligencia artificial es cada vez más común en la prestación de servicios de asistencia sanitaria y en investigación en salud; por ejemplo, la diagnosis basada en análisis de imágenes, para tratar información de historias clínicas a gran escala, realizar análisis genéticos y desarrollar vacunas y medicamentos, o hacer cribajes y detectar enfermedades de manera más eficaz.
La inteligencia artificial puede ofrecer ventajas, como permitir una detección más precisa y rápida de enfermedades en una persona, o ayudar en la investigación médica. Pero también supone un tratamiento ingente de información personal, que los responsables tienen que articular adecuadamente.
A estos efectos es esencial la anonimización y el principio de minimización de datos, es decir, que sólo se utilicen los datos estrictamente necesarios. En cualquier caso, la persona tiene derecho a ser informada y a que se garantice la intervención humana en el diagnóstico.
En este campo, la inteligencia artificial debe entenderse como un apoyo al personal asistencial y no como un sistema que pueda tomar decisiones directas sobre la salud de pacientes sin la intervención profesional.

37. Tratamiento de datos para finalidades de administración y gestión de servicios.

El personal de un centro sanitario que se encarga de las tareas de administración y gestión del centro puede acceder a los datos de la historia clínica relacionadas con estas funciones. Son, por ejemplo, los necesarios para programar una visita o para facturar un servicio a las personas asistidas.
Este personal sólo tiene que acceder a los datos imprescindibles para realizar los trámites necesarios.

38. ¿El hospital donde he sido tratado por un accidente de tráfico puede comunicar mis datos a la compañía de seguros de mi vehículo sin mi consentimiento?

Sí. Cuando se trata de un seguro obligatorio, la ley permite a los centros sanitarios reclamar a las compañías de seguros el importe de la asistencia sanitaria prestada a las personas aseguradas de estas compañías. Para ello, la entidad debe poder comunicar datos de pacientes para acreditar que se ha prestado la asistencia sanitaria reclamada.

39. Si he presentado una reclamación contra el hospital donde me han atendido, ¿el hospital puede comunicar mis datos a un abogado externo?

Sí. Si los datos son necesarios para ejercer el derecho de defensa o el cumplimiento del contrato de seguro, el hospital podrá comunicar los datos de salud de la persona atendida a sus abogados o a la compañía de seguros del mismo hospital o de profesionales denunciados.

40. ¿Puede un centro sanitario instalar cámaras de videovigilancia?

Sí, siempre que previamente haya constatado la necesidad de hacerlo para proteger la seguridad de trabajadores, pacientes y acompañantes, instalaciones o bienes que contengan.
Los responsables de los centros sanitarios, ya sean públicos o privados, deben velar por la intimidad de pacientes y sus familias y garantizar la proporcionalidad de la captación. Las cámaras no deben instalarse en espacios donde puedan vulnerar la intimidad de las personas que reciben tratamiento en el centro.
Se debe informar de que hay cámaras instaladas y cumplir con el resto de las previsiones establecidas en la normativa de protección de datos.

41. Tratamiento de datos con finalidades epidemiológicas y de salud pública.

La epidemiología es el estudio de la distribución y los determinantes de los estados o eventos (en particular de enfermedades) relacionados con la salud y la aplicación de estos estudios al control de enfermedades y otros problemas de salud. Forma parte de la medicina preventiva y ayuda en el diseño y desarrollo de políticas de salud pública.
En el tratamiento de la información con fines epidemiológicos o de salud pública es necesario evitar la identificación de las personas afectadas, salvo que sea necesario para que las autoridades sanitarias para la prevención de un riesgo o peligro grave para la salud de la población o que las personas hayan dado su consentimiento previamente.
Cuando se detectan casos relacionados con enfermedades de declaración obligatoria o brotes epidémicos, hay obligación de comunicarlo a las autoridades sanitarias. Tanto el personal especializado como las autoridades sanitarias deben asegurarse de que esta información no sea la causa de discriminación o daños de ningún tipo para las personas afectadas.
Las autoridades sanitarias también pueden tratar los datos cuando sea necesario para garantizar la calidad y la seguridad de la asistencia sanitaria, los medicamentos y los productos sanitarios.

42. ¿Puede un centro asistencial comunicar sin mi permiso, a mis familiares o a la empresa en la que trabajo, que se me ha detectado una enfermedad contagiosa?

Si se trata de una enfermedad de declaración obligatoria, la ley permite a la administración sanitaria comunicar al centro de trabajo, al colegio o a las personas relacionadas con el paciente índice, su identidad (si es esencial) y la enfermedad que padece, para comprobar si se han producido contagios. En el lugar de trabajo o en los centros escolares, la información debe llegar al número mínimo de personas que permita a las autoridades sanitarias tomar las medidas adecuadas.

43. Si se declara una epidemia, ¿pueden las autoridades en materia de salud pública utilizar nuestros datos sin nuestro consentimiento?

Sí. Es lícito que las autoridades en materia de salud pública traten nuestros datos de salud, cuando sea necesario por razones de interés público; por ejemplo, controlar la propagación de epidemias o pandemias y, en última instancia, cuando se producen crisis sanitarias o amenazas transfronterizas que representan un grave peligro para la salud de la población. El tratamiento también es lícito cuando se trata de proteger el interés vital del titular de la información u otras personas.
Si existe riesgo de transmisión, las autoridades competentes en materia de salud pública deben adoptar las medidas necesarias para controlar a las personas afectadas, a las de su entorno inmediato y a quienes estén o hayan estado en contacto con ellas. Para ello, pueden tratar los datos necesarios.

44. En los casos de epidemias que representan un riesgo para la población en general, ¿pueden las autoridades de salud pública informar a las personas de mi entorno sobre mi estado de salud?

En estas situaciones, las autoridades de salud pública pueden habilitar sistemas para contactar y alertar a las personas que han estado en contacto con una persona infectada, con el fin de proteger los intereses vitales y evitar que estas personas propaguen la enfermedad.
Siempre que sea posible, las autoridades deberán informar únicamente sobre la posibilidad de que se haya producido o que se pueda producir el contagio, sin difundir la identidad de la persona fuente de contagio.

45. En caso de epidemia, ¿puede cualquier administración pública o establecimiento controlar la temperatura en el momento de acceder a un recinto para detectar posibles casos sospechosos?

En general, establecer una medida de este tipo sin el consentimiento de las personas afectadas no tiene fundamento jurídico, excepto que lo establezcan las autoridades competentes en materia de salud pública.
Ello sin perjuicio de la habilitación de la que disponen los servicios de prevención de las empresas para adoptar medidas de vigilancia de la salud adecuadas respecto de las personas

de su plantilla, si el estado de salud de alguna de ellas puede suponer un peligro para el resto de personas trabajadoras o para las que se relacionan con la empresa.

46. ¿Es apropiado que los servicios de salud utilicen apps para hacer un seguimiento o atención si se declara una epidemia?

Sí, siempre que estas apps o webs que recogen o tratan los datos de la ciudadanía cumplan con los requisitos de la normativa de protección de datos.
Estas aplicaciones pueden permitir conocer si una persona presenta síntomas de contagio, datos sobre su estado psicológico, etc., y proporcionarle la ayuda adecuada y los recursos de salud adecuados.
También se pueden utilizar para estudios epidemiológicos y estadísticos con datos agregados obtenidos de las personas que los utilizan (por ejemplo, datos de geolocalización agregados para detectar áreas geográficas con mayor riesgo e incidencia de la epidemia, a fin de permitir a las autoridades establecer medidas de control).
Antes de empezar a usar la app hay que disponer de información suficiente. Es importante leer y entender la política de privacidad y saber quién es responsable de ello; qué datos se pueden tratar o comunicar; para qué finalidad se utilizarán; qué derechos tienen las personas usuarias y dónde se pueden ejercer, así como el tiempo de conservación y la ubicación de los datos que se tratan.
La gestión eficaz de una situación de crisis sanitaria, como la causada por la covid-19, puede implicar que las autoridades públicas adopten medidas excepcionales para evitar que se propague entre la población.
Para ello, las aplicaciones de seguimiento de los síntomas y la localización de contactos pueden ser una herramienta adecuada, siempre que se ofrezcan garantías adecuadas para salvaguardar los derechos y libertades fundamentales de quienes los usan, especialmente el derecho a la protección de los datos personales.
El consentimiento informado de las personas que deciden instalarse estas apps puede ser una base legal adecuada. Sin embargo, para cumplir con el resto de los principios relativos a la protección de datos, la aplicación no debe permitir que se revele la identidad de las personas que han estado en contacto y el lugar o el momento en que se ha producido, sino sólo que durante un tiempo relevante ha habido contacto con una persona contagiada o sospechosa de estarlo.
Esto, además de implementar las medidas de seguridad adecuadas y garantizar que los datos sólo se utilizarán para este fin y que la información se destruirá una vez que la situación epidémica haya desaparecido.

47. Tratamiento de datos con finalidades de inspección sanitaria

Los profesionales que realizan tareas de inspección para la Administración sanitaria pueden acceder, debidamente acreditados, a los historiales clínicos de las personas atendidas, para comprobar la calidad de la asistencia que reciben, que cumplen con los derechos de las mismas o cualquier otra obligación del centro en relación con pacientes o la administración sanitaria. Siempre que sea posible, estos datos deben tratarse de forma anonimizada o seudonimizada.

48. Tratamiento de datos con finalidades de investigación en salud

Los datos de salud que se recogen para atender a pacientes se pueden utilizar más adelante con fines de investigación en los siguientes casos:
• Cuando la persona da el consentimiento explícito para participar en un proyecto de investigación médica o en un área de investigación.
La participación en un ensayo clínico o en un estudio sobre una enfermedad puede incluir procedimientos médicos invasivos (muestras de sangre, ensayo de medicamentos, etc.). La inclusión en el estudio debe ser gratuita, voluntaria, libre y no discriminatoria para la persona participante en el estudio.

• Cuando las autoridades sanitarias realizan estudios en situaciones de excepcional relevancia y gravedad para la salud pública.

• Cuando se haya dado el consentimiento para que los datos se utilicen para un estudio inicial y se deseen reutilizar para otra investigación relacionada con el área de la investigación inicial.
En este caso, es necesario informar a las personas afectadas y contar con un informe favorable del comité de ética.

• Cuando se utilizan datos personales seudonimizados, es decir, sin identificar a la persona.
La seudonimización consiste en sustituir los datos identificativos por un código o clave que terceros no puedan relacionar con la persona titular de los datos. La información seudonimizada sigue siendo información personal. La información debe ser entregada seudonimizada al equipo de investigación.
Es necesario tener un compromiso previo de confidencialidad y de no reidentificación de las personas, tomar las medidas adecuadas para evitar accesos indebidos a la información y tener un informe previo del comité de ética de la investigación o en su defecto de la persona que ejerce de delegada de la protección de datos o, si no lo hay, de un experta en protección de datos. A menudo también será necesario llevar a cabo una evaluación de impacto relativa a la protección de datos.

49. ¿Se pueden utilizar mis datos de salud para la investigación médica sin mi consentimiento?

Aunque en algunos casos este tratamiento se puede producir sobre la base del consentimiento prestado por la persona, la ley también acepta otros supuestos, como, por ejemplo, que se traten datos de salud seudonimizados con fines de investigación en salud. Esto, siempre que en este último caso, el personal responsable proteja la información con las medidas de seguridad adecuadas para no poner en peligro los derechos de las personas afectadas (separación funcional al hacer la seudonimización, compromisos de confidencialidad y de no reidentificación, medidas de seguridad específicas, informe del comité de ética, etc.).

50. Sufro de una enfermedad rara y el equipo médico me propone participar en un estudio de investigación. ¿Estoy obligado a participar en él?

No. La participación activa de una persona en los estudios de investigación es siempre voluntaria, y las condiciones o la calidad del tratamiento médico que recibe no pueden depender de que participe o no en el estudio.

Si acepta participar, antes de su inicio, deberá recibir toda la información que necesite sobre las características e implicaciones del estudio y del tratamiento que se realizará de sus datos.

51. ¿Cuándo pueden ser reidentificadas las personas que participan en una investigación?

Si en una investigación médica realizada con datos seudonimizados, se detecta un peligro real y específico para la seguridad o la salud de una o más personas, una amenaza grave a sus derechos, o si es necesario garantizar una atención sanitaria adecuada, las personas afectadas pueden ser reidentificadas.
Si declaró que no quería conocer los resultados del estudio, hay que respetar su voluntad. Sin embargo, si por criterio médico se considera que, como resultado de lo que se ha descubierto en el estudio, la salud o la seguridad de sus familiares biológicos corre un peligro real y específico, o existe una amenaza grave para sus derechos o es necesario para garantizar una atención sanitaria adecuada, hay que informarle.

52. Tratamiento de datos con finalidades de docencia

El acceso a la historia clínica con fines de docencia debe realizarse protegiendo el anonimato de las personas, a menos que se tenga su consentimiento.
El alumnado de especialidades en ciencias de la salud pueden acceder a la historia clínica con datos personales anonimizados o a historias clínicas simuladas por quien imparte la docencia. Esto garantiza que el aprendizaje se realiza respetando la intimidad de las personas y la confidencialidad de los datos de salud.
El personal médico residente en formación son personal asistencial del centro sanitario, por lo que pueden acceder a la historia clínica de las personas que atienden.
Los centros sanitarios deben informar al alumnado y residentes de especialidades en ciencias de la salud, sobre las medidas de protección de datos personales y requerirles que cumplan los compromisos que les corresponden: deber de confidencialidad, custodia de información, política de permisos, medidas a implementar al utilizar dispositivos electrónicos, portátiles, memorias USB, compromiso de no reidentificación, etc.

53. Me ha pedido permiso para grabar imágenes de la intervención quirúrgica al que debo someterme, con fines de docencia universitaria. ¿Es correcto?

Sí. En este caso, la grabación de una intervención quirúrgica no responde a una finalidad asistencial, sino que tiene finalidades de docencia, de manera que la persona afectada puede autorizar el tratamiento de las imágenes. La grabación no se puede hacer si dicha persona no da su consentimiento. Para utilizar las imágenes u otros datos en la docencia o en publicaciones científicas, no debe ser identificable la persona intervenida.

54. ¿Puede el alumnado en formación estar presente en las visitas hospitalarias?

Las personas ingresadas, o sus representantes pueden autorizar que dicho alumnado pueda estar presente en su proceso asistencial (por ejemplo, en una exploración o revisión médica). El personal médico debe limitar la presencia del personal en formación cuando se considere inapropiado por la situación clínica, emocional o social del paciente.

55. Tratamiento de los datos de salud en el ámbito laboral

La legislación laboral reconoce el derecho de las personas trabajadoras a una protección efectiva en el ámbito de la salud y la seguridad en el trabajo. Al mismo tiempo, establece que en su trabajo están obligados a respetar las medidas de salud y seguridad establecidas. Esta normativa también prevé situaciones que generan ayudas, permisos o prestaciones para las y los trabajadores y sus familias (para cuidar de niños o familiares con enfermedades específicas, por la hospitalización de familiares, cambios o adaptación de puestos de trabajo por razones de salud o rehabilitación de trabajadores, etc.).
Del mismo modo, el Estatuto de los Trabajadores prevé que la empresa, mediante el reconocimiento por parte del personal médico, puede verificar el estado de salud de quienes han alegado razones de salud para justificar las ausencias en el lugar de trabajo.
Por otro lado, este marco normativo obliga a las empresas a contar con un servicio de prevención de riesgos laborales que se responsabilice de las actividades de prevención y protección de estos riesgos.
Cuando los y las trabajadoras se someten voluntariamente a revisiones médicas facilitadas por la empresa, el personal sanitario deben tratar sus datos de salud con el fin de elaborar un informe sobre su aptitud para desarrollar su trabajo. En estos casos, la empresa puede saber si la persona es apta o no apta para su trabajo y, también, la información relacionada con la necesidad de introducir o mejorar las medidas de protección y prevención. Sin embargo, no debe conocer otra información o datos concretos sobre la salud de las personas trabajadoras.
En resumen, la relación laboral de una persona trabajadora o funcionaria con su empresa o con la Administración pública puede hacer necesario que la empresa conozca y trate determinados datos personales suyos, incluidos los de salud y, en algunos casos, incluso de sus familiares.

56. Me encuentro en una situación de incapacidad temporal (IT). ¿Qué información debe constar en el formulario que debo entregar a mi empresa para comunicar o confirmar la baja?

Cuando una persona trabajadora se encuentra en una situación de baja por enfermedad, en la copia del formulario destinado a la empresa (para ser remitido al INSS o a una mutua), deben constar algunos datos de salud (fecha de la baja y alta médica, duración probable de la baja, si se trata de una enfermedad común o accidente no laboral y, si procede, si se trata de una recaída). Sin embargo, ni la descripción de la limitación de la capacidad ni el diagnóstico deben comunicarse al empresario a tal efecto.

57. En caso de una emergencia sanitaria o epidemia, ¿la empresa en la que trabajo tiene derecho a conocer si estoy infectada o puedo estarlo por tener algún síntoma, e informar de ello a las autoridades de salud pública?

En aplicación de las normas de salud pública y prevención de riesgos laborales, las empresas deben velar por la salud de sus personas trabajadoras. En caso de epidemia o crisis sanitaria, las empresas pueden tratar los datos estrictamente necesarios de su personal empleado (por ejemplo, para saber quiénes están afectados por la enfermedad, si deben mantenerse

aislados, etc.) con el fin de evitar contagios, hay que aplicar correctamente dentro de la empresa las medidas de control adecuadas sobre la epidemia y comunicar posibles casos de contagio a las autoridades, de modo que puedan hacer los estudios de contactos para controlar la epidemia.
En cualquier caso, tanto los datos de salud que la empresa debe conocer, como los que se comunican a las autoridades deben ser únicamente los estrictamente necesarios para este fin.

58. Comunicación de datos a jueces y tribunales

La ley prevé que los jueces y tribunales puedan acceder a los datos de la historia clínica con fines judiciales.
Si un órgano judicial se dirige a un centro o a profesionales sanitarios y solicita datos de salud de una persona paciente, el centro debe atender necesariamente a esta solicitud y proporcionar los datos sin necesidad del consentimiento de la propia persona. Sin embargo, si el centro tiene dudas sobre qué información debe enviarse, o si la información solicitada puede no ser pertinente, puede solicitar las aclaraciones necesarias a la autoridad judicial.

59. Comunicaciones de datos a las fuerzas y cuerpos de seguridad

Los centros sanitarios deben comunicar los datos de salud del paciente a los cuerpos policiales en funciones de policía judicial que los requieran, sin necesidad de que la persona consienta, en los siguientes casos:
• Cuando sea absolutamente necesario para los fines de una investigación específica.
• Cuando sea necesario proteger el interés vital de la persona.
• Cuando son datos que la persona ha hecho manifiestamente públicos.
• Cuando una ley lo autoriza.
También es necesario comunicar datos que no sean de salud u otras categorías especiales de datos a los cuerpos policiales (por ejemplo, datos de identificación o residencia), sin necesidad de vincular esta cesión a una investigación específica, cuando sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

60. Los datos de salud de los menores de edad

La posibilidad de consentir el tratamiento de los datos personales de los menores de 14 años y el ejercicio de sus derechos corresponde a las personas titulares de la patria potestad.
Los menores que sean mayores de 14 años y que no estén incapacitados, deben poder acceder a su información y ejercer sus derechos.
Los padres o representantes legales del menor también pueden hacerlo hasta que sea mayor de edad, ya que no necesitan su consentimiento para acceder a los datos de salud de los hijos. Las dos posibilidades deben entenderse como compatibles y no excluyentes entre sí.
Si hay un conflicto entre los padres o representantes legales y el menor, el acceso de los padres a los datos de salud del hijo puede limitarse por aplicación del principio de protección del interés superior del menor. Deben tenerse en cuenta las circunstancias específicas de cada caso.

61. La Administración está tramitando un procedimiento de desamparo de mi hijo de dos años. ¿Puedo acceder a su historia clínica?

Si la patria potestad se suspende como resultado de un procedimiento de desamparo, también queda suspendida la posibilidad de que los padres ejerzan el derecho de acceso a la historia clínica del menor.

62. ¿Qué pasa si hay un conflicto con la custodia de los hijos?

En caso de separación o divorcio de los padres, el centro sanitario puede solicitar la resolución judicial que ha decidido sobre la patria potestad y la situación de los hijos menores, para garantizar que el progenitor que solicita el acceso a la historia clínica tenga la representación legal del menor.

63. Tengo atribuida temporalmente la custodia de mis nietos. Los servicios sociales han pedido al Centro de Salud información de salud de los niños y también mía. ¿Pueden hacerlo?

Los centros sanitarios pueden tener que comunicar a los servicios sociales datos de salud de menores atendidos y tutelados por la Administración pública competente en protección de menores, así como datos de salud de los familiares que los atienden. Sin embargo, sólo puede compartir los datos necesarios para verificar que los menores están bien atendidos y para tomar las decisiones necesarias en su interés.