

N/REF: 069725/2018

Se remite a esta Agencia documentación sobre el proyecto europeo MADIA (Magnetic Diagnostic Assay for neurodegenerative diseases), incluido en el ámbito del programa Horizonte 2020 de la Unión Europea, a fin de que se determine si los tratamientos de datos personales que pudieran efectuarse en el marco de las actividades de investigación del mismo son conformes a la normativa de protección de datos de carácter personal.

El estudio tiene como objetivo hacer un registro de datos clínicos y moleculares de pacientes con enfermedades neurodegenerativas desarrollando una herramienta innovadora basada en el uso de la nanotecnología que permita analizar determinados biomarcadores en pacientes con dichas enfermedades y que al mismo tiempo sirva para el diagnóstico precoz de las mismas.

Según señala la consulta, en el proyecto participan diversas entidades públicas españolas y entidades de países miembros de la Unión Europea.

I

Con carácter previo debe señalarse que esta Agencia carece de competencia para emitir autorizaciones o aprobaciones de la conformidad de un tratamiento de datos a lo establecido en la normativa de protección de datos. No obstante, viene atendiendo las peticiones de informes que le dirigen los responsables de los ficheros a los efectos de facilitarles el conocimiento y la interpretación de la normativa de protección de datos de carácter personal, evitando así incumplimientos involuntarios de la legislación vigente. En el marco de esta actividad cabe examinar si los tratamientos de datos personales al que el proyecto objeto de consulta se refiere, que vayan a ser realizados por las entidades sujetas a la normativa de protección de datos aplicable en España, son conformes a lo previsto en la misma.

II

La primera cuestión que resulta del proyecto sujeto a informe es la relativa a la aplicación en el tiempo de la normativa de protección de datos, teniendo en cuenta que el proyecto, según se expone en la documentación aportada, se inicia en el año 2017 y finaliza en el año 2019.

A este respecto, debe considerarse que a partir de 25 de mayo de 2018 resulta plenamente aplicable el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Por consiguiente, se aplicaban hasta dicha fecha las normas que hasta entonces venían rigiendo la materia, esto es 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, y la normativa que en cada país la desarrollaba, normativa que en España venía constituida fundamentalmente por La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre y con posterioridad al 25 de mayo de 2018 el citado Reglamento General de Protección de datos. A ello cabe añadir que, a partir de 7 de diciembre de 2018, resulta aplicable lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En este sentido la disposición final quinta de dicha Ley incorpora un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad relativo al tratamiento de datos de la investigación en salud, cuyo artículo 105.bis dispone que *“El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.”*

Asimismo, en España la investigación biomédica se rige por su Ley especial, la Ley 14/2007, de 3 de julio, de Investigación biomédica cuyas previsiones resultarán también de aplicación en cuanto contengan especificaciones relativas al derecho a la protección de datos personales.

En consecuencia, en el presente informe se hará referencia a ambas normativas y a las obligaciones que, siendo exigibles conforme a la normativa anterior, se mantienen o modifican y a las nuevas exigencias que impone el Reglamento General de Protección de Datos, así como a la norma especial que en el derecho español regula la investigación biomédica.

III

En segundo lugar, debe examinarse la aplicabilidad de la normativa de protección de datos a los tratamientos de datos que puedan llevarse a cabo durante la ejecución del proyecto objeto de consulta.

Así en lo que respecta a la normativa aplicable con anterioridad a 25 de mayo de 2018, debe tenerse en cuenta que los artículos 1 y 2 de la Ley Orgánica 15/1999 extendían su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables.”*

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, precisaba que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

Dicha definición procede del artículo 2 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, según el cual se entenderán por datos personales *“toda información sobre una persona física identificada o identificable (el “interesado”); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».*

El Grupo de trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, en su Dictamen 4/2007 sobre el concepto de datos personales, tras poner de manifiesto que la Directiva maneja un concepto lato de datos personales, analiza los elementos de dicha definición, señalando respecto a la expresión “toda información” lo siguiente:

“Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas». Esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca, para evaluar la fiabilidad de los prestatarios («Fulano es un prestatario fiable»), el asegurador («no se espera que Fulano muera pronto») o el laboral («Fulano es un buen trabajador y merece un ascenso»).

Para que esas informaciones se consideren «datos personales», no es necesario que sean verídicas o estén probadas. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados.

Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada «datos sensibles» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo stricto sensu, pero también la información sobre cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).»

Como continuación de dicho análisis el Grupo de trabajo examina el término “sobre” indicando que “ya se ocupó anteriormente de la cuestión de cuándo puede considerarse que una información versa «sobre» una persona. En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa».

A ello cabe añadir que el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal define en su artículo 5.1.g) los datos de carácter personal relacionados con la salud como “las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.”

Por su parte, el artículo 3.o) de la Ley 14/2007, de 3 de julio, de Investigación biomédica define la muestra biológica como “cualquier material biológico de origen humano susceptible de conservación y que pueda albergar información sobre la dotación genética característica de una persona.” El artículo 5.1 de la misma norma dispone que “Se garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales que resulten de la actividad de investigación biomédica, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las mismas garantías serán de aplicación a las muestras biológicas que sean fuente de información de carácter personal.”

Por su parte, el Reglamento (UE) 2016/679, esto es, el Reglamento general de protección de datos, define los datos en su artículo 4.1, entendiendo por tales “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.” Asimismo, conforme al número 15 del mismo artículo 4 se consideran datos relativos a la salud los “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”

De este modo, en el presente supuesto, tanto con la normativa anterior como con la actual, tiene la condición de dato de carácter personal cualquier clase de información asociada a las personas físicas que participan en las actividades previstas en el proyecto y tienen la condición de datos de salud, los relativos a la salud física o mental de las personas cuyas muestras biológicas se recaban, extendiéndose las garantías previstas en la normativa de protección de datos a dichas muestras biológicas en tanto son fuente de información de carácter personal.

IV

Teniendo en cuenta que en el proyecto se señala que los datos clínicos de los pacientes serán recogidos por el investigador de forma codificada y que solamente el equipo de investigación y las autoridades sanitarias tendrán acceso a todos los datos recogidos para el estudio, añadiendo que solamente se puede transmitir información a terceras partes que no permita la identificación, debe aquí recordarse la diferencia entre un proceso de seudonimización y un proceso de disociación o anonimización, ya que éste último determina la inaplicación de la normativa de protección de datos.

En este sentido, la Ley Orgánica 15/1999 describía el proceso de disociación en su artículo 3 f) como *“Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable”*

En lo que respecta a la seudonimización cabe recordar que el aludido Grupo de Trabajo del Artículo 29, en su Dictamen 5/2014 sobre técnicas de anonimización, define la seudonimización como “la sustitución de un atributo (normalmente un atributo único) por otro en un registro” señalando que “por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización.”

En este sentido señalaba el Dictamen 4/2007 del Grupo de Trabajo del artículo 29 respecto de un mecanismo de seudonimización habitual como son los datos cifrados que *“Los datos cifrados son un ejemplo clásico de*

«seudonimización». La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado.»

Así, a título de ejemplo, indicaba el Dictamen 4/2007 que *“Si a cada persona física se le ha asignado un único código, siempre existe un riesgo de identificación en caso de que sea posible acceder a la clave utilizada para el cifrado. Por lo tanto, los riesgos de un acceso ilegal desde el exterior, la probabilidad de que alguien de la organización remitente - a pesar de estar sujeto al secreto profesional -proporcione la clave y por ende la vía para una identificación indirecta, son factores que deben tenerse en cuenta para determinar si las personas pueden ser identificadas teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona y, por lo tanto, si la información debe considerarse como «datos personales».*

El concepto de seudonimización aparece expresamente recogido en el artículo 4.5) del Reglamento europeo que define la «seudonimización» como *“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”*

El considerando 26 de dicho Reglamento recuerda que *“Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.”*

Y en el considerando 28, viene a poner de manifiesto la diferencia entre anonimización y seudonimización al señalar que *“La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la*

introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.”

Debe así tenerse en cuenta la diferencia entre ambos conceptos, de modo que si bien la seudonimización debe valorarse positivamente como una medida de seguridad que tal y como señala el Reglamento General de Protección de Datos contribuye a reducir los riesgos para los interesados, no excluye la aplicación de la normativa de protección de datos de modo que todas las obligaciones y deberes que ésta impone continúan siendo exigibles. A diferencia de la seudonimización, la anonimización implica un procedimiento que no permita en ningún caso la reidentificación del usuario, solo así quedará excluido de la aplicación de la normativa de protección de datos.

De este modo, si la información relativa a las personas se encuentra asociada a un seudónimo, esta operación de seudonimización, por sí misma, no constituye un procedimiento de disociación puesto que a partir de la información de que se tiene conocimiento será posible realizar la operación inversa a la seudonimización, lo que da lugar a que la aplicación de la normativa de protección de datos no quede excluida.

Siguiendo tales criterios, la Ley 14/2007, de 3 de julio, de Investigación biomédica, define en su artículo 3.i) *el dato anonimizado o irreversiblemente disociado, como el dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiéndose por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados*. Mientras que conforme a su letra k) será un dato codificado o reversiblemente disociado el *“dato no asociado a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa.”* Y de la misma manera, diferencia entre la *“muestra biológica anonimizada o irreversiblemente disociada”* que será, conforme a la letra p de dicho artículo 3, la *“muestra que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable”* y la muestra biológica codificada o reversiblemente disociada, descrita en la letra r del citado artículo 3 como *“muestra no asociada a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa.”*

De este modo, resultará también aplicación la normativa de protección de datos a las muestras codificadas o reversiblemente disociadas, como en el caso presente, toda vez que a partir de la información de que se tiene conocimiento será posible realizar la “operación inversa” a la codificación.

Debe, también hacerse referencia al concepto de tratamiento de datos personales, toda vez que de lo expuesto en el proyecto se desprende la

realización de diversos posibles tratamientos. A este respecto, conforme al artículo 3.c) de la Ley Orgánica 15/1999 un tratamiento de datos venía constituido por las *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.”*

El artículo 4.2 del Reglamento General de Protección de datos define el tratamiento como *“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”*

Por consiguiente, la realización de alguna o varias de estas operaciones respecto de datos personales, esto es, de cualquier información asociada a una persona física identificada o identificable, dará lugar a un tratamiento de datos personales. Debe así tenerse en cuenta que la recogida de datos no constituye el único tratamiento posible, sino que otras operaciones (por ejemplo, conservación o comunicaciones de datos) constituyen también tratamientos de datos y son igualmente determinantes, de la aplicabilidad de la normativa de protección de datos.

V

Tomando en consideración que en el proyecto participan entidades españolas y de otros Estados miembros de la Unión Europea, debe hacerse una referencia a la determinación de la normativa aplicable con anterioridad a la plena aplicación del Reglamento general de protección de datos.

El artículo 4 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 disponía al respecto:

- 1 *Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:*
 - a *el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos*

establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable”

Para determinar la legislación aplicable resulta necesario hacer referencia a las figuras de responsable y encargado del tratamiento. El artículo 2 de la Directiva 95/46 define en su letra d) al responsable del tratamiento como *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; (...)”* Debe así diferenciarse el responsable del fichero o tratamiento del responsable del proyecto o de una fase del mismo ya que a dicha condición de responsable del fichero o tratamiento se anudan determinadas consecuencias jurídicas distintas a las propias de quien está a cargo de un determinado trabajo.

Cabe así señalar, con carácter general, que la condición de responsable del fichero es consecuencia del hecho de que una persona o entidad, debidamente legitimada, haya decidido tratar datos personales para sus propios fines, correspondiéndole por ello asumir las obligaciones impuestas por la normativa de protección de datos y las responsabilidades que de su incumplimiento pudieran derivarse. En el derecho español la Ley Orgánica 15/1999, definía al responsable del fichero o tratamiento como la *“persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*.

Por su parte, el encargado del tratamiento venía definido en el artículo 2.e) de la Directiva como *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.”*

Cabe así recordar que esta figura obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos por parte del responsable a quien le presta tal servicio, sino que el tratamiento de los datos se realiza por el encargado en nombre y por cuenta del responsable como si fuera este mismo quien lo lleva a cabo. El artículo 3 g) de la Ley Orgánica 15/1999, define así al encargado como *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”*.

Debe tenerse en cuenta que, para que pueda hablarse de encargado del tratamiento la Directiva 95/46/CE, venía a exigir los siguientes requisitos en su artículo 17, números 3 y 4:

“3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.”

De este modo, si las entidades participantes en el proyecto establecidas en un Estado miembro actuaban en calidad de responsables debían ajustar los tratamientos de datos que efectuasen a lo previsto en la normativa de protección de datos que les resultaba de aplicación de conformidad con lo establecido en el artículo 4 de la Directiva 95/46/CE, esto es, los tratamientos de datos personales en el marco de las actividades de cada establecimiento debían adecuarse a la legislación nacional en que cada establecimiento se encuentre.

En el caso de que las entidades participantes en el proyecto actuaran como encargados del tratamiento, les resultaba de aplicación la normativa de protección de datos que correspondía al responsable por cuya cuenta actuaban, excepto en lo que respecta a la adopción de medidas de seguridad, en que se aplicaba la normativa del Estado miembro en que tuviese su establecimiento el encargado del tratamiento.

En lo que respecta a la aplicación de la normativa de protección de datos española el artículo 3.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, disponía que *“Se regirá por el presente reglamento todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.”*

En consecuencia, conforme a la normativa vigente antes de 25 de mayo de 2018, se encontraba sujeta a lo establecido en la normativa española, en su condición de responsable, la entidad española que recababa en España datos clínicos y muestras de pacientes y de personas sanas a los que se utiliza como sujetos control. También quedarían sujetas a dicha normativa otras entidades españolas participantes en el proyecto que actuaran en calidad de responsables del tratamiento. Igualmente quedaban sometidas a la normativa española de protección de datos y demás aplicable las entidades que actuaran como encargadas de tratamiento de responsables sujetos a la normativa española, excepto en la aplicación de las medidas de seguridad que serían las

del país en que tenga su establecimiento el encargado. No obstante, si alguna entidad española actuase como encargado del tratamiento de un responsable al que deba aplicarse la normativa de protección de datos de otro país de la Unión Europea, seguiría la ley nacional del responsable, salvo en lo que respecta a las medidas de seguridad que serían las establecidas en la normativa española.

VI

Hasta 25 de mayo de 2018, las entidades españolas que tuviesen la condición de responsables del tratamiento debían dar cumplimiento a las obligaciones impuestas al responsable por la Ley Orgánica 15/1999. A partir de dicha fecha deben dar cumplimiento a las nuevas obligaciones establecidas en el Reglamento General de protección de datos, igualmente deben tenerse en cuenta las especificaciones contenidas en la Ley Orgánica 3/2018 cuya vigencia comenzó el 7 de diciembre de dicho año.

Entre las obligaciones impuestas a los responsables del tratamiento por la Ley Orgánica 15/1999 y las nuevas obligaciones impuestas por la normativa actualmente vigente deben destacarse las siguientes:

-En primer lugar, conforme a lo establecido en la Ley Orgánica 15/1999, debía notificarse la creación del fichero a efectos de su inscripción en el Registro General de Protección de Datos de esta Agencia, no obstante, dicha obligación dejó de ser exigible a partir de 25 de mayo de 2018.

En la actualidad el artículo 31 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) obliga a los responsables del tratamiento a mantener un registro de las actividades de tratamiento bajo su responsabilidad, y a los encargados a mantener registros de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable. Debe tenerse en cuenta que el número 5 de dicho artículo establece una excepción al cumplimiento de dichas obligaciones siempre y cuando se cumplan dos condiciones: la primera de ellas que se trate de una empresa u organización que emplee a menos de 250 personas y, la segunda, que el tratamiento que realice no entrañen un riesgo para los derechos y libertades de los interesados, no incluya categorías especiales de datos personales a los que se refiere el artículo 9 del Reglamento ni datos personales relativos a condenas o infracción penales a que se refiere el artículo 10 de la misma norma, ni dicho tratamiento sea ocasional. De este modo, aunque el responsable diera empleo a menos de 250 personas, el carácter habitual, aun cuando sea temporal, del tratamiento de datos personales precisos para llevar

a cabo el proyecto, impide aplicar dicha excepción debiendo llevar a cabo dicho registro en los términos establecidos en el precepto transcrito.

A ello cabe añadir que el artículo 31.2 de la Ley Orgánica 3/2018 exige a los sujetos enumerados en su artículo 77.1 -entre las que se encuentran las Administraciones de las Comunidades Autónomas, los organismos públicos y entidades de Derecho Público vinculadas o dependientes de las Administraciones Públicas y las Universidades Públicas- a hacer público un inventario de sus actividades de tratamiento accesible por medios electrónicos, en el que debe constar la información establecida en el artículo 30 del Reglamento General de Protección de Datos y su base legal.

- En segundo lugar, debe tenerse en cuenta que el requisito capital para que un tratamiento de datos personales sea conforme a lo establecido en la normativa de protección de datos es que el mismo se encuentre legitimado en lo previsto en dicha normativa.

Tratándose en el presente supuesto del tratamiento de datos de salud, cabe recordar que el artículo 7.3 de la Ley Orgánica 15/1999 disponía que *“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.”*

A ello debe añadirse que Ley 14/2007, de 3 de julio, de Investigación biomédica hace referencia al consentimiento en diversos preceptos, así en su artículo 4 relativo al consentimiento informado y derecho a la información, se dispone en su número primero que *“Se respetará la libre autonomía de las personas que puedan participar en una investigación biomédica o que puedan aportar a ella sus muestras biológicas, para lo que será preciso que hayan prestado previamente su consentimiento expreso y escrito una vez recibida la información adecuada.”* Añadiendo en su párrafo segundo que *“La información se proporcionará por escrito y comprenderá la naturaleza, importancia, implicaciones y riesgos de la investigación, en los términos que establece esta Ley. Asimismo, el artículo 45 al regular los principios rectores específicos reitera en su letra d) que “deberá obtenerse previamente el consentimiento escrito del sujeto fuente o en su caso de sus representantes legales para el tratamiento de muestras con fines de investigación o de datos genéticos de carácter personal.”* Por su parte el artículo 58.1 establece que *“La obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud. Dicho consentimiento será revocable.”*

De este modo, durante la vigencia de la Ley Orgánica 15/1999 el responsable debía recabar, de las personas físicas que participasen en el estudio, su consentimiento para el tratamiento de sus datos personales, consentimiento que debía reunir las características de “libre, inequívoco, específico e informado” conforme a lo previsto en el artículo 3.h) de la Ley Orgánica 15/1999 a lo que debe añadirse que el consentimiento debe ser expreso por tratarse de datos de salud y por escrito cuando se pretende la obtención de muestras biológicas.

Esta Agencia ha venido describiendo en sus informes dichas características de manera que se entiende por consentimiento libre aquel que ha sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil. El consentimiento específico viene referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999. Para que pueda hablarse de consentimiento inequívoco se exige la realización de una acción u omisión que implique la existencia del consentimiento.

En lo que se refiere al capital requisito del consentimiento expreso en el caso de los datos relativos a la salud, la Audiencia Nacional ha señalado en sentencia de 24 de marzo de 2006 lo siguiente “*Por consentimiento expreso hemos de entender aquél que se obtiene de una declaración clara e inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos mediante la expresión de su voluntad de forma que permita su constancia y prueba indubitada. La existencia de consentimiento expreso, referido a la cesión y uso de estos datos especialmente sensibles no debe admitir duda ni entenderse o interpretarse en varios sentidos, o poder dar ocasión a juicios diversos*”

En cuanto al requisito de la información, supone que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se efectúa. En este sentido el artículo 5 de la Ley Orgánica 15/1999 venía a exigir que “*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*”.

Por consiguiente, el modelo de consentimiento debía adecuarse a dichos requerimientos, esto es, la identificación del responsable del tratamiento (que cómo se ha indicado no es el investigador, sin perjuicio de que se le señale como la persona ante la que puede ejercitar sus derechos), la finalidad del tratamiento y la posibilidad de ejercer los derechos a que se refiere la letra d) de dicho precepto. Asimismo, debían indicarse quienes eran los posibles

destinatarios de la información (en el presente supuesto, a título de ejemplo, otros socios del proyecto en caso de que se les comunicasen datos personales) recabando el consentimiento de los interesados para tal comunicación de datos.

En lo que respecta a la legitimación para el tratamiento de datos en el Reglamento General de Protección de datos, debe tomarse en consideración que su artículo 9.1 prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. No obstante, en su número segundo excepciona dicha prohibición cuando concurra alguna de las circunstancias que enumera, de las que interesa aquí la contenida en la letra j) según la cual: *“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.”*

A este respecto, la Ley Orgánica 3/2018 en su disposición adicional decimoséptima, se refiere a los tratamientos de salud previendo que se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las leyes que relaciona, entre las que se encuentra la Ley 14/2007, de 3 de julio, de Investigación biomédica. Debe aquí reiterarse que la citada Ley 14/2007 requiere en diversos preceptos el consentimiento escrito del sujeto fuente para obtener muestras biológicas con fines de investigación biomédica.

Por su parte, el número 2 de la disposición adicional decimoséptima de la Ley Orgánica 3/2018 establece que *“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.”*

El Reglamento general de protección de datos define el consentimiento en su artículo 4.11 como “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.” A ello cabe añadir, que en lo respecta a categorías especiales de datos, el artículo 9.1.a) de la misma norma exige que el consentimiento tenga el carácter de “explicito”.

En lo que respecta a dichos requisitos, deben tenerse en cuenta las directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas por el Grupo de Trabajo del artículo 29 y respaldadas por el Comité Europeo de Protección de Datos, creado por el citado Reglamento y al que se le atribuyen diversas funciones entre las que figura la garantía de la aplicación coherente del mismo.

Conforme a tales directrices, el consentimiento libre implica una elección y control real de los sujetos a quien pertenecen los datos, sin que el consentimiento pueda ser un fundamento válido cuando existe una situación de desequilibrio de poder en la relación entre el responsable y el interesado. En este sentido cabe destacar la previsión contenida en el artículo 4.4 de la Ley 14/2007 que expresamente determina que *“La falta de consentimiento o la revocación del consentimiento previamente otorgado no supondrá perjuicio alguno en la asistencia sanitaria del sujeto.”*

En cuanto a la nota de especificidad, señalan las citadas directrices que el artículo 6.1.a del Reglamento General de Protección de datos confirma que el consentimiento debe darse “para uno o varios fines específicos”. Asimismo, el consentimiento debe ser específico para cada fin. En este sentido, cabe mencionar que el artículo 60 de la Ley 14/2007 dispone que:

“1. El consentimiento sobre la utilización de la muestra biológica se otorgará, bien en el acto de obtención de la muestra, bien con posterioridad, de forma específica para una investigación concreta.

2. El consentimiento específico podrá prever el empleo de la muestra para otras líneas de investigación relacionadas con la inicialmente propuesta, incluidas las realizadas por terceros. Si no fuera este el caso, se solicitará al sujeto fuente que otorgue, si lo estima procedente, un nuevo consentimiento.”

En lo que respecta al carácter de inequívoco se establece en el artículo 6 del Reglamento de protección de datos que requiere una declaración del interesado o una clara acción afirmativa. En el presente supuesto, además de inequívoco, el consentimiento debe ser “explícito” por tratarse de categorías especiales de datos personales. Señalan las directrices a que se viene haciendo referencia que el término explícito se refiere a la manera en que el interesado expresa el consentimiento, siendo una manera evidente de garantizar que el consentimiento es explícito confirmar dicho consentimiento en una declaración escrita. Cómo se ha venido señalando son numerosos los preceptos de la Ley 14/2007 en los que se hace referencia a que el consentimiento conste por escrito.

En lo que respecta al requisito de la información, debe tenerse en cuenta que la información exigible conforme a lo previsto en los artículos 13 y 14 del Reglamento es mayor que la exigida conforme a la Ley Orgánica 15/1999. De este modo cuando se recabe el consentimiento de los participantes en el ensayo con posterioridad a 25 de mayo de 2018, deberá darse la información conforme a lo previsto en dichos preceptos del Reglamento General de Protección de datos.

En lo que respecta a la información que debe proporcionarse al interesado dispone el artículo 13 del Reglamento General de Protección de Datos lo siguiente:

“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;

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 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.

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 el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), 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 automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, 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.

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."

Debe tenerse en cuenta, también como se señala en las directrices del grupo del 29, respecto de la información relativa a la identidad del responsable que en caso de que múltiples responsables (conjuntos) del tratamiento vayan a recurrir al consentimiento o si los datos se van a transferir o van a ser procesados por otros responsables del tratamiento que desean basarse en el consentimiento original, se deberá nombrar a todas estas organizaciones. No es necesario nombrar a los encargados como parte de los requisitos del consentimiento, aunque, con el fin de cumplir lo dispuesto en los artículos 13 y 14 del RGPD, los responsables deberán facilitar una lista completa de los receptores o categorías de receptores de los datos que incluya a los encargados del tratamiento.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, consagra respecto del deber

de información, el principio de información por capas disponiendo en su artículo 11 que:

“1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de las que procedieran los datos.”

Por consiguiente, los consentimientos que se recaben con posterioridad al 25 de mayo de 2018, deberán incluir la información a que se refiere el artículo 13 del Reglamento General de Protección de datos, si bien cabe acudir a la posibilidad de que la información se proporcione mediante el sistema a que se refiere el artículo 11 de la Ley Orgánica 3/2018.

Respecto a los consentimientos recabados con anterioridad a dicha fecha dispone el considerando 171 del Reglamento que *“Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento.”*

Por otra parte, tanto con la normativa anterior como con la actual el consentimiento es revocable en cualquier momento. Así resultaba de lo previsto en los artículos 6.3 y 11.4 de la Ley Orgánica 15/1999, pudiendo el interesado exigir el cese en el tratamiento de sus datos mediante su pura y simple manifestación de voluntad. Por su parte, el artículo 7.3 del Reglamento general de protección de datos dispone que *“El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.”*

El artículo 4 de la Ley 14/2007 señala que *“3. Las personas que participen en una investigación biomédica podrán revocar su consentimiento en cualquier momento, sin perjuicio de las limitaciones que establece esta Ley. Las personas o entidades que hayan recibido dicho consentimiento dispondrán las medidas que sean necesarias para el efectivo ejercicio de este derecho.”* Por su parte el artículo 59 e) de la misma norma exige respecto de la información previa a la utilización de la muestra biológica, cuando no vaya a ser sometida a un proceso de anonimización, que debe facilitarse al interesado por escrito, información sobre el *“derecho de revocación del consentimiento y sus efectos, incluida la posibilidad de la destrucción o de la anonimización de la muestra y de que tales efectos no se extenderán a los datos resultantes de las investigaciones que ya se hayan llevado a cabo.”* Por su parte el artículo 60.3 dispone que *“El consentimiento podrá ser revocado, totalmente o para determinados fines, en cualquier momento. Cuando la revocación se refiera a cualquier uso de la muestra, se procederá a su inmediata destrucción, sin perjuicio de la conservación de los datos resultantes de las investigaciones que se hubiesen realizado con carácter previo.”*

A este respecto, el Reglamento General de Protección de datos en su artículo 17 prevé que *“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:(...) b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico”*

Sin embargo, el apartado 3 del artículo 17, establece diversas excepciones a la aplicación de lo previsto en los apartados anteriores del citado artículo,

entre las cuales cabe mencionar las contenidas en las letras b, c y d) de dicho precepto que a continuación se reproduce:

“b) 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 de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, 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.”

De este modo, la limitación del derecho de supresión establecida en la Ley 14/2007, no entra en contradicción con lo dispuesto en el artículo 17 del Reglamento General de Protección de Datos, quedando enmarcada en las posibles excepciones a la obligación de suprimir los datos que dicho Reglamento prevé.

Por otra parte, cabe señalar que tanto con la normativa anterior, artículo 12 del Reglamento de desarrollo de la Ley Orgánica 15/1999, como con la actual, artículo 7 de Reglamento General de Protección de datos, corresponde al responsable del tratamiento la prueba de la existencia del consentimiento del interesado para el tratamiento de sus datos personales.

- Dentro de las obligaciones del responsable debe destacarse, en tercer lugar, el deber de implantar las debidas medidas de seguridad. En este sentido cabe recordar que el artículo 9 de la Ley Orgánica 15/1999 disponía que *“El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.”* El número 2 de dicho precepto establecía la prohibición de registrar en datos de carácter personal en ficheros *“que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.”*

El Reglamento general de protección de datos adopta un enfoque diferente al establecido en la Ley Orgánica 15/1999 y su normativa de desarrollo en lo que respecta a las medidas de seguridad que el responsable debe implementar. Señala el considerando 83 de dicha norma que *“A fin de*

mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.”

Y en su artículo 32, números 1 y 2, dispone lo siguiente respecto de la 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.”

Asimismo, debe tenerse en cuenta que una vez el Reglamento General de Protección de datos es plenamente aplicable incumbe a todos los responsables la obligación de notificar, en su caso, las violaciones de seguridad de los datos a la autoridad de control (esto es, en el caso español a la Agencia Española de protección de datos), disponiendo al respecto el artículo 33 de dicho Reglamento que:

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

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

La notificación contemplada en el apartado 1 deberá, como mínimo:

- a describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
- b comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
- c describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
- d describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los*

datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.”

- Como se ha señalado el Reglamento General de Protección de Datos, impone nuevas obligaciones a los responsables del tratamiento, tales como la realización de una evaluación de impacto relativa a la protección de datos, prevista en su artículo 35. El número primero de dicho precepto dispone que *“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.”*

Por su parte, el número 4 de dicho precepto prevé que *“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.”*

La Ley Orgánica 3/2018 dispone en cuanto a las obligaciones anteriores lo siguiente:

“1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 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 del citado reglamento.

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 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

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.”

Asimismo, la disposición adicional decimoséptima de dicha Ley Orgánica 3/2018, en su número 2, letra f) dispone que “Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, 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.”

Por último, dentro de las obligaciones del responsable, cabe destacar que el número segundo, letra h) de la citada disposición adicional decimoséptima hace referencia al delegado de protección de datos, disponiendo que *“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.”*

VII

Si alguna de las entidades sujetas a la normativa de protección de datos española efectuase una comunicación de los datos personales objeto de tratamiento en el proyecto a terceros, incluida cualquiera de las demás entidades que participan en el mismo o procediesen a su difusión por cualquier procedimiento, dicha comunicación o difusión constituirá una cesión de datos personales.

La cesión de datos personales venía definida en la Ley Orgánica 15/1999 en su artículo 3 i) como *“Toda revelación de datos realizada a una persona distinta del interesado”*. Tal cesión debía sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de dicha Ley Orgánica, según el cual solo podía verificarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario, exigiendo, para que pudiera tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarían los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretendían comunicar (artículo 11.3), y que debía recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

De la misma manera, y en el marco de aplicación del Reglamento General de Protección de datos, tal y como se señalaba en el documento de directrices del Grupo del artículo 29, respecto de la información relativa a la identidad del responsable, debe tenerse en cuenta que, en caso de que múltiples responsables (conjuntos) del tratamiento vayan a recurrir al consentimiento o si los datos se van a transferir o van a ser procesados por

otros responsables del tratamiento que desean basarse en el consentimiento original, se deberá nombrar a todas estas organizaciones en la información que se aporte al recabar el consentimiento.

No obstante, en lo que respecta a las demás entidades participantes en el proyecto cabe recordar la posibilidad de que puedan actuar en condición de encargados del tratamiento del responsable, en tal caso no será preciso el consentimiento del interesado, en tanto no se produce una cesión de datos. Ello sin perjuicio de la existencia de otros encargados del tratamiento que pudieran actuar en nombre del responsable. El artículo 12 de la Ley Orgánica 15/1999 regula la figura del encargado del tratamiento, disponiendo que *“No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.”* El Reglamento General de Protección de Datos contempla también la figura del encargado del tratamiento al que define en su artículo 4.8) como *“la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”* y cuyo régimen jurídico regula en su artículo 28. Igualmente, la Ley Orgánica 3/2018 en su artículo 33.1 dispone que *“El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.”*

Debe aquí tenerse en cuenta que la disposición transitoria quinta de dicha Ley Orgánica 3/2018 prevé que *“Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.”*

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.”

En lo que respecta al régimen de encargado del tratamiento previsto en la Ley Orgánica 15/1999, cabe recordar que para que la relación entre responsable y encargado del tratamiento pueda darse y sea ajustada a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la misma, considerando los siguientes aspectos:

En primer lugar, el acceso a los datos por el tercero debe efectuarse con la exclusiva finalidad de prestar un servicio al responsable del fichero, debiendo asimismo encontrarse dicha relación de servicios contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo

12.2 de la Ley Orgánica 15/1999, impone que *“la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”*.

En este sentido, debe además recordarse que uno de los requisitos determinantes de la condición de encargado de tratamiento es la inexistencia de una relación directa entre el afectado por el tratamiento de datos, tal y como establece el último párrafo del número primero del artículo 20 del Reglamento de desarrollo de la Ley Orgánica 15/1999 según el cual *“se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado”*. El encargado debe obrar en todo caso en nombre y por cuenta del responsable como si como si la relación fuese entre éste y el afectado. De este modo, si se establece dicha relación directa utilizando el encargado para sus propios fines los datos personales recabados por el responsable, carecería de tal condición deviniendo responsable y la comunicación de datos al mismo una cesión que requerirá el consentimiento de los interesados.

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley Orgánica 15/1999, de forma que *“una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”*.

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la citada Ley, de que *“En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”*.

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la aludida Ley Orgánica podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento de desarrollo de dicha Ley al disponer *“no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del*

responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.”

Por su parte, el artículo 22 del aludido Reglamento de desarrollo de la Ley Orgánica 15/1999, dispone respecto de la conservación de los datos lo siguiente:

“1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.”

En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica 15/1999, con la excepción antes señalada respecto de la adopción de medidas de seguridad cuando el encargado tenga su establecimiento en otro Estado miembro de la Unión Europea.

En cuanto al régimen jurídico establecido en el Reglamento General de Protección de Datos, interesa aquí reproducir lo establecido en su artículo 28.3 según el cual *“El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:*

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

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

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

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

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

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros."

Por su parte la Ley Orgánica 3/2018 dispone, en el mismo sentido que lo hacía la Ley Orgánica 15/1999, en su artículo 33.2 que *"Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.*

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades."

El número tercero de dicho artículo 33 prevé que el responsable del tratamiento determine si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, salvo cuando exista una previsión legal que obligue a su conservación, devueltos al responsable o entregados, en su caso, a un nuevo encargado. Conforme al número cuarto del mismo artículo 33, el encargado del tratamiento podrá conservar, debidamente

bloqueados, los datos en cuanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

VIII

Debe tenerse en cuenta que todo tratamiento de datos debe ser respetuoso de los principios propios de la materia de protección de datos. De tales principios, recogidos bajo el título de calidad de datos en el artículo 4 de la Ley Orgánica 15/1999, cabe destacar el denominado principio de finalidad, consagrado en el artículo 4.2 de dicha Ley y conforme al cual *“Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”*. Dicho principio había sido objeto de una interpretación sistemática por la Audiencia Nacional, considerando que la expresión “finalidades incompatibles” era equivalente a “finalidades distintas”.

El Reglamento general de protección de datos recoge dicho principio bajo la denominación de principio de limitación de la finalidad en el artículo 5.1.b) conforme al cual los datos serán *“recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales”*.

En este sentido el artículo 60 de la Ley 14/2007, como anteriormente se ha señalado hace referencia al principio de limitación de la finalidad, disponiendo en su número primero que el consentimiento sobre la utilización de la muestra biológica se otorgará de forma específica para una investigación concreta. En su número segundo dispone que “El consentimiento específico podrá prever el empleo de la muestra para otras líneas de investigación relacionadas con la inicialmente propuesta, incluidas las realizadas por terceros. Si no fuera este el caso, se solicitará al sujeto fuente que otorgue, si lo estima procedente, un nuevo consentimiento.”

Debe señalarse aquí que la disposición adicional decimoséptima de la Ley Orgánica 3/2018, en su número 2, letra c) toma en consideración lo señalado en el artículo 33 del Reglamento según el cual *“Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con*

finde 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”, permitiendo considerar como 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 estos casos se exigen las siguientes garantías:

-En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del 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 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 dichos tratamientos se requerirá informe previo favorable del comité de ética de la investigación.”

En este sentido, la disposición transitoria sexta de la Ley Orgánica 3/2018, relativa a la reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de dicha Ley dispone que:

“Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.”

Debe hacerse también referencia al principio de limitación de la conservación, descrito en la letra e) del artículo 5 del Reglamento General de Protección de datos según el cual los datos serán “*mantenidos de forma que*

se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales”

A este respecto la normativa especial contenida en la Ley 14/2007, dispone en su artículo 61 que *“1. En el caso de que la muestra sea conservada, el sujeto fuente será informado por escrito de las condiciones de conservación, objetivos, usos futuros, cesión a terceros y condiciones para poder retirarlas o pedir su destrucción. No obstante, las muestras biológicas utilizadas en investigación biomédica se conservarán únicamente en tanto sean necesarias para los fines que justificaron su recogida, salvo que el sujeto fuente haya otorgado su consentimiento explícito para otros usos posteriores.*

2. Lo indicado en el apartado anterior se entiende aplicable en tanto los datos de identificación de la muestra no hayan sido sometidos a su anonimización de conformidad con lo previsto en esta Ley.”

En el presente caso se señala que los datos serán guardados de forma codificada y protegidos por el investigador principal y las muestras serán depositadas en una colección privada con la finalidad de que puedan ser utilizadas para futuros estudios vinculados con la misma línea de investigación, lo que resulta conforme con lo establecido en el artículo 61 de la Ley 14/2007 antes mencionado y con lo previsto en el artículo 27 del Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica, cuyo artículo 27 señala respecto del destino de las muestras una vez finalizada la investigación o el proyecto de investigación concreto lo siguiente:

“El consentimiento específico otorgado por el sujeto fuente para que su muestra se incorpore a una colección para fines de investigación biomédica conservada fuera del ámbito organizativo de un biobanco, o se utilice en un proyecto de investigación concreto, preverá una de las siguientes opciones:

a) La destrucción de la muestra una vez finalizado el proyecto o la investigación.

b) La anonimización de la muestra biológica para usos posteriores.

c) La posterior cesión gratuita de la muestra a un biobanco, siempre que se facilite información sobre el mismo y sobre las posibles finalidades de uso de la muestra.

d) La posterior utilización de la muestra integrada en una colección para una línea de investigación relacionada con la inicialmente propuesta, incluso por un tercero mediante cesión gratuita, con la advertencia de que se solicitará el consentimiento específico del sujeto fuente para ello.”