

N/REF: 151979/2018

Se solicita de la Agencia Española de Protección de Datos una autorización o un informe sobre la conformidad a la normativa de protección de datos personales aplicable a los tratamientos de este carácter que pudieran efectuarse en el marco de las actividades de investigación del proyecto europeo My TRAC -My TRAVel Companion, incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

El objetivo principal de dicho proyecto es desarrollar una plataforma de servicios de transporte para el sector ferroviario con el fin de proporcionar una experiencia mejorada para los pasajeros. Para ello se va a utilizar una amplia gama de tecnologías, como inteligencia artificial emocional o simulación de elección por el usuario. Se creará una aplicación para teléfonos inteligentes que conectará información de diversas fuentes: operadores de transporte público respecto a horarios e información real (por ejemplo, retrasos, interrupciones); proveedores de movilidad como servicio (coches compartidos, servicios de taxi, etc.); conjuntos de datos relacionados con el servicio y el viaje (disponibilidad de estacionamientos, seguridad, densidad de la multitud en estaciones) y se relacionará esta información con las preferencias y el estado de ánimo de los usuarios. La aplicación proporcionará interfaces tanto para los usuarios como para los operadores, los primeros recibirán información para la planificación de viajes, adaptada a sus necesidades y estado de ánimo, y los segundos recibirán datos de comportamientos anonimizados y agregados para utilizar en tiempo real y en actividades de planificación estratégica.

Según señala la consulta, en el proyecto participan diversas entidades públicas y privadas españolas y de países miembros de la Unión Europea. El proyecto comporta la realización de un programa piloto en España.

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 objeto de informe es la relativa a la aplicación en el tiempo de la normativa de protección de datos, teniendo en cuenta que, según se expone en la documentación aportada, se inicia en 2017 y tiene una duración de 36 meses.

A este respecto, debe tenerse en cuenta 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. Con posterioridad al 25 de mayo de 2018 resulta de aplicación el citado Reglamento general de protección de datos y, a partir de 7 de diciembre de 2018, resulta también 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 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 y la Ley Orgánica 3/2018 que complementa el mismo.

III

En segundo lugar, debe examinarse la aplicabilidad de la normativa de protección de datos personales 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, extienden 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, precisa 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».

Por otra parte, para determinar que se entiende por persona identificada o identificable, señala del Grupo de Trabajo del artículo 29, en el mismo Dictamen 4/2007 lo siguiente:

“La Directiva requiere que la información se refiera a una persona física «identificada o identificable». Ello suscita las siguientes consideraciones. De modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»). Así pues, esta segunda alternativa es, en la práctica, la condición suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente. La identificación se logra normalmente a través de datos concretos que podemos llamar «identificadores» y que tienen una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc. o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc. La Directiva menciona esos «identificadores» en la definición de «datos personales» del artículo 2 cuando establece que «se declarará 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».

En lo que respecta a los términos “directa” o “indirectamente” identificable continúa señalando el Grupo de Trabajo del artículo 29 que:

“Esta idea se aclara aún más en los comentarios a los artículos de la propuesta modificada de la Comisión, en donde se afirma que «una persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.), que haga posible su identificación al estrecharse el grupo al que pertenece.”

Los términos de esta declaración indican claramente que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona - es decir, para aislarla – dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso.

Por su parte, cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean éstas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual Presidente del Gobierno de España»), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuestos a evitar cualquier quebrantamiento de la confidencialidad.”



El Reglamento (UE) 2016/679, esto es, el Reglamento general de protección de datos, define los datos personales en su artículo 4.1 como *“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.*

Dicha definición tiene en cuenta la aparición de nuevos datos identificativos de las personas, tal y como expresa su considerando 30 según el cual *“Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.”*

En el presente supuesto se van a tratar muy diferentes tipos de datos, la propia documentación aportada menciona los datos relativos a nombre, edad, género, localización del domicilio y localización del lugar de trabajo. También hace referencia a que pueden tratarse datos especialmente protegidos como emociones y estado de ánimo, considerando que podrían incluirse en la categoría de salud aunque no vayan a utilizarse con tal finalidad, y datos relativos a opiniones políticas o religiosas que los interesados puedan incluir en sus declaraciones en redes sociales conectadas con la aplicación. No obstante debe recordarse que también son datos de carácter personal, entre otros, los datos de localización, la identificación del dispositivo móvil, la frecuencia de acceso a la aplicación o a la plataforma, los datos recogidos por los sensores incluida la voz o la imagen de las personas si tales datos fueran recogidos, los datos contenidos en el dispositivo móvil que sea preciso utilizar para el funcionamiento de la aplicación y los perfiles que puedan obtenerse de los usuarios de la aplicación, no solamente el relativo a sus preferencias de los usuarios sino cualquier otro perfil que del comportamiento de las personas que utilizan las herramientas del proyecto se obtenga. A ello cabe añadir que entre las funcionalidades de la plataforma se hace referencia a la ayuda que pueda prestarse a personas discapacitadas, por lo que los datos de discapacidad que pudieran obtenerse son igualmente datos de carácter personal y además datos relacionados con la salud. También serán datos personales en cuanto estén asociados a una persona las razones por las que viajan. El tratamiento de cualquier clase de datos de carácter personal quedará sujeto a lo establecido en la normativa de protección de datos.

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 viene 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.

En este sentido, aunque como señala la consulta los datos personales queden almacenados en el dispositivo móvil de los usuarios y solamente se acceda a ellos cuando el interesado lo solicite a través de la aplicación, tal acceso constituye un tratamiento de datos que debe sujetarse a lo previsto en la normativa de protección de datos.

IV

En la consulta se hacen diversas referencias a que los datos personales a utilizar en el marco del proyecto serán anónimos. Sin embargo, la anonimización implica un procedimiento que no permita en ningún caso la reidentificación del usuario. Así, no resultaría aplicable la normativa de protección de datos cuando no sea posible identificar a las personas, por haberse sometido sus datos a un proceso de disociación; la Ley Orgánica 15/1999 describe éste 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”*

Cabe aquí recordar que el citado Grupo de Trabajo del artículo 29 en su Dictamen 5/2014, sobre técnicas de anonimización, señalaba que *“A la luz de*



la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación.”

Se recordaba en dicho Dictamen 5/2014 que ““El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».

Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso.

(...) Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos.”

En dicho Dictamen 5/2014 se ponía igualmente de manifiesto que “Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos.”

En el presente supuesto, no cabe pensar que los datos utilizados serán anónimos, puesto que siempre será posible la identificación de la persona por su conexión con el dispositivo móvil. También es posible identificar a la persona si esta permite una conexión a una red social de la que forme parte. Ello sin perjuicio de que del conjunto de los datos recabados (por ejemplo, a través de los datos de localización) pueda una persona resultar identificable.



Cuestión distinta es que tales datos puedan considerarse seudonimizarse. El concepto de seudonimización aparece expresamente recogido en el artículo 4.5) del Reglamento general de protección de datos 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.



V

Uno de los aspectos fundamentales que comporta el tratamiento de datos personales es determinar quién o quiénes son los responsables del mismo. Cabe así señalar, con carácter general, que la condición de responsable 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. 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.

Conforme a lo previsto en la Ley Orgánica 15/1999 en su artículo 3.d) es responsable del fichero o tratamiento la *“persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*.

El Reglamento general de protección de datos define al responsable del tratamiento como en su artículo 4.7 como *“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”*

Por otra parte, cabe mencionar que el Reglamento general de protección de datos regula por primera vez la figura del corresponsable estableciendo al efecto en su artículo 26 lo siguiente:

“1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.



2. *El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.*

3. *Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.”*

Debe además hacerse referencia a la figura del encargado del tratamiento, definida en el artículo 3 g) de la Ley Orgánica 15/1999 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*”. También el Reglamento general de protección de datos se refiere al encargado del tratamiento o encargado como “*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*”.

En este sentido cabe recordar que la figura del encargado del tratamiento 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 criterio definidor de la condición de responsable del tratamiento viene dado por la potestad de determinar los fines y los medios del tratamiento, en tanto que el encargado debe limitar su actuación a seguir las instrucciones del responsable, reputándosele responsable en caso de que determine fines y medios, esto es, si utiliza para fines propios los datos personales que el responsable le haya comunicado para que lleve a cabo el tratamiento objeto de encargo o establezca relaciones con los afectados por el tratamiento sin que conste que actúa por cuenta de otro, sin perjuicio de que pueda incurrir en una infracción de la normativa de protección de datos con dicha actuación.

En lo que respecta al régimen jurídico del encargado del tratamiento debe aquí tenerse en cuenta que la disposición transitoria quinta de la Ley Orgánica 3/2018 prevé que “*Los contratos de encargo 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 jurídico 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.

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.

Cabe aquí recordar lo señalado por el Grupo de Trabajo del artículo 29 en su informe 02/2013 sobre las aplicaciones de los dispositivos inteligentes, en el que se indicaba que el desarrollador de la aplicación es un responsable del fichero o tratamiento, en tanto que decide la medida en que la aplicación accederá y procesará las distintas categorías de datos personales en el dispositivo y o a través de recursos informáticos remotos, de modo que, de conformidad con las definiciones legales de responsable antes vistas, determina los fines y los medios del tratamiento de datos personales en los dispositivos inteligentes. Por consiguiente, le incumben todas las obligaciones exigibles al responsable del fichero o tratamiento. La categoría de desarrollador de la aplicación incluye tanto a las personas que crean una aplicación y la distribuyen como a las entidades públicas o privadas que subcontratan el desarrollo de la aplicación.

En el presente supuesto se desprende de la documentación aportada en la consulta que la aplicación se desarrolla como una parte del proyecto, por lo que debe determinarse respecto de cada miembro del consorcio la posición que ocupa, esto es, su carácter de responsable, corresponsable o encargado del tratamiento, toda vez de que ella resultan diferentes obligaciones y responsabilidades.

Teniendo en cuenta 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”*

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 efectúen a lo previsto en la normativa de protección



de datos que les resultase 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 encontrase.

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, dispone 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.”*

Por consiguiente, los tratamientos de datos realizados por responsables cuyo establecimiento se encuentre en territorio español quedaban sujetos a lo dispuesto en la Ley Orgánica 15/1999. Este era el caso de las entidades españolas participantes en el proyecto si actuaban en calidad de responsables, pero sería igualmente el caso de cualquier otra entidad participante si tuviera un establecimiento en España y efectuase un tratamiento de datos en el marco de las actividades del mismo. También quedaban sometidas a la normativa española de protección de datos 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 tuviesen su establecimiento. No obstante, si alguna entidad española actuase como encargado del tratamiento de un responsable al que debiera aplicarse la normativa de protección de datos de otro país de la Unión Europea, seguía la ley nacional del responsable, salvo en lo que respecta a las medidas de seguridad que serían las establecidas en la normativa española.

VII

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.

Dentro de las obligaciones impuestas a los responsables del tratamiento resulta fundamental la relativa a la legitimación para el tratamiento de datos.

En el marco de la Ley Orgánica 15/1999, las bases legitimadoras para el tratamiento de los datos que no tuvieran el carácter de especialmente protegidos se encuentran en su artículo 6, cuyo número primero exige el consentimiento inequívoco del afectado salvo que la Ley disponga otra cosa. No obstante, su artículo 7 establece un régimen especial para el tratamiento de datos especialmente protegidos, en sus números 2 y 3, disponiendo que:

“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.”

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 debía ser expreso cuando se tratase de datos relativos a la salud y debía recabarse por escrito cuando se pretendía el tratamiento de los datos a que se refiere el artículo 7.2 de dicha Ley.

Esta Agencia ha venido describiendo en sus informes dichas características entendiendo 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 especialmente protegidos, 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 consentimiento obtenido durante la vigencia de la Ley Orgánica 15/1999 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, debía 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 tras la plena vigencia del Reglamento general de protección de datos, debe acudirse a lo previsto en su artículo 6 que enumera las bases legitimadoras del mismo, siendo la primera de ellas que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

Ahora bien, teniendo en cuenta que en el presente supuesto pueden llegar a tratarse datos relacionados con la salud o datos que revelen la ideología o creencias de las personas, debe recordarse 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 orientación 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 las contenidas en las letras 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”* y e) *“el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.”*

A este respecto la Ley Orgánica 3/2018 dispone en su artículo 9.1 que *“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.”

Dicho precepto se corresponde con lo que venía estableciendo el artículo 7.4 de la Ley Orgánica 15/1999, a cuyo tenor *“quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual”*. Por consiguiente, no será posible, ni aun contando con el consentimiento de los afectados un tratamiento cuya finalidad principal sea la identificación de los datos a que se refiere el artículo 9.2.a) de la Ley Orgánica 3/2018.

Fuera de tal supuesto, expresamente prohibido por la Ley Orgánica 3/2018, el tratamiento de los datos en el presente supuesto encuentra su base legal en el consentimiento del interesado, conforme a lo previsto en el artículo 6.1.a del Reglamento general de protección de datos. Dicha norma 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 “explícito”.

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 del 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 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 lo que respecta al carácter de inequívoco, tal y como se establece en el artículo 6 del Reglamento general de protección de datos, 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. No obstante, cabe el uso de otros medios, el aludido documento de directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 menciona algunos que pueden ser utilizados en el contexto digital, tales como, entre otros, rellenar un impreso electrónico, enviar un correo electrónico, cargar un documento escaneado con su firma o utilizar una firma electrónica.

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 general de protección de datos 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.”

En el presente supuesto en que se persigue el desarrollo de una aplicación, el deber de información es esencial, puesto que debe darse tal información antes de la instalación de la misma. En este sentido, el usuario de la aplicación tiene derecho a saber qué tipo de datos personales están siendo tratados y con qué finalidad se van a usar.

Señala el Grupo de Trabajo del artículo 29 en el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, que el responsable del tratamiento debe informar a los usuarios potenciales como mínimo de la identidad y datos de contacto del responsable, de las categorías exactas de datos personales que el desarrollador de aplicaciones recogerá y tratará, de los objetivos precisos y si los datos se comunicasen a terceros la forma en que los usuarios pueden ejercer sus derechos (retirar el consentimiento y eliminar datos).

Debe tenerse en cuenta, también como se señala en las directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Trabajo del artículo 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.

Ser informado de qué datos se están tratando es especialmente importante habida cuenta del amplio acceso que las aplicaciones suelen tener a sensores y estructuras del dispositivo, donde muchas veces ese acceso no es obvio. Cabe así mencionar, dentro de los datos personales a que pueden



acceder las aplicaciones, los relativos a localización, contactos, identificadores únicos del dispositivo y del cliente (IIEEM; IIAM; IUD y número de teléfono móvil), identidad del interesado, identidad del teléfono (los usuarios tienden a llamar a su móvil con su verdadero nombre) registros de llamadas, SMS y mensajería instantánea, historial de navegación, correo electrónico, fotografías y vídeos, credenciales de autenticación para los servicios de la sociedad de la información, datos biométricos (en modelos de reconocimiento facial y huellas dactilares), etc.

El Grupo de Trabajo del artículo 29 recuerda que el consentimiento solamente es válido si la persona ha sido previamente informada sobre los principales elementos del tratamiento de datos, por lo que facilitar dicha información únicamente después de que el tratamiento de datos personales se haya iniciado carece de validez jurídica.

En cuanto a la forma, señala el aludido Dictamen 02/2013 que la información debe estar a disposición de los usuarios antes de instalar la aplicación y debe seguir siendo accesible dentro de la aplicación tras su instalación. El Grupo de Trabajo del artículo 29 recomienda que la información esté también disponible y fácilmente localizable por ejemplo dentro de la tienda de aplicaciones y preferiblemente en los sitios web del desarrollador responsable de la aplicación. Por otra parte, teniendo en cuenta las limitaciones que puede presentar la cantidad de información que puede presentarse en una pantalla pequeña, el aludido Grupo de Trabajo recomienda que la información se facilita por capas, así en un primer aviso se facilita la información mínima exigible conforme al marco jurídico español y se pone a disposición del interesado información complementaria a través de enlaces al conjunto de la política de privacidad.

Respecto a los consentimientos recabados con anterioridad a la plena aplicabilidad del Reglamento general de protección de datos dispone el considerando 171 de dicha norma 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.”

Debe también recordarse 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.

VIII

Debe tenerse en cuenta que todo tratamiento de datos debe ser respetuoso de los principios propios de la materia de protección de datos. Estos principios venían recogidos bajo el título de calidad de datos en el artículo 4 de la Ley Orgánica 15/1999 y en la actualidad se recogen en el artículo 5 del Reglamento general de protección de datos.

Debe destacarse en primer lugar el principio de licitud, lealtad y transparencia. El artículo 5.1.a del Reglamento general, de protección de datos dispone que los datos personales serán tratados *“de manera, lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia)”*.

Son diversos los considerandos del Reglamento que hacen referencia a dicho principio, así el considerando 39 señala que *“Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.”* En este mismo sentido el considerando 60 recuerda que *“Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales.(...)”*

El segundo párrafo del considerando 71 precisa que *“A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar*

medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.”

Dicho principio tiene especial incidencia en el presente supuesto en que los datos se obtienen a través de una aplicación y, tal y como la documentación aportada se indica, en los casos en que el interesado lo permita, se recabarán datos de la red social que éste determine. A este respecto, ya se ha hecho referencia al derecho a la información del interesado, pero debe ponerse especial énfasis en que este debe conocer qué datos van a tratarse y consentir su tratamiento. Por otra parte, una recogida lícita y leal impide que se lleve a cabo un acceso a la red social de manera que no pueda diferenciarse de la que haga el propio interesado, lo que permitiría un acceso indiscriminado a todos los datos de éste, y, en tanto no existen límites, el acceso a los de los terceros que con él se relacionan. No obstante, podría resultar lícito un tratamiento limitado a los datos hechos manifiestamente públicos por el interesado en una red social siempre y cuando se contase igualmente con el consentimiento del afectado para tal tratamiento y se de cumplimiento a los demás principios recogidos en el artículo 5 del Reglamento.

De entre los principios propios de la materia de protección de datos, cabe destacar igualmente el principio de finalidad, recogido en el artículo 4.2 de la Ley Orgánica 15/1999, según el 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*”. Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto venía considerando la expresión “finalidades incompatibles” como sinónimo de “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”*.

La limitación de la finalidad está vinculada al principio de proporcionalidad, consagrado en el artículo 4.1 de la Ley Orgánica 15/1999 conforme al cual *“Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.”* De la misma manera el artículo 5 del Reglamento general de protección de datos exige que los datos sean *“adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)”*

De este modo solamente deberán recabarse aquellos datos que sean precisos para llevar a cabo las actividades especificadas y para las que se ha obtenido consentimiento de los interesados. Dicho principio tiene una especial incidencia en lo que respecta a la aplicación para móviles, dado que, como se ha señalado, son muchos los datos contenidos en un terminal móvil al que las aplicaciones puede acceder, debiendo solicitarse el acceso en cada momento por el interesado y accederse solamente a los datos estrictamente necesarios para el funcionamiento de la aplicación.

Igualmente, dentro de los aludidos principios debe hacerse referencia al relativo a la conservación de los datos, disponiendo el número 5 del artículo 4 de la Ley Orgánica 15/1999 que *“Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.”*

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.”

A dicho principio se refiere igualmente el Reglamento general de protección de datos bajo el nombre de principio de limitación de plazo de conservación, en su artículo 5 letra e) 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; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado.”

En el presente caso se señala que los datos solamente se tratan en el momento en que se solicita el servicio, quedando almacenados en el dispositivo móvil del interesado y almacenándose solamente en la plataforma datos anónimos y agregados. En este sentido se indica que los participantes podrán dejar de participar en el piloto borrando su cuenta. Tal y como señala el Grupo de Trabajo del artículo 29, en el aludido informe 02/2013 sobre las aplicaciones de los dispositivos inteligentes debe ser posible en todo caso la desinstalación de la aplicación.

IX

Respecto a otras obligaciones del responsable cabe mencionar 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 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.

- Dentro de las obligaciones del responsable debe destacarse, en segundo 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.”

En este sentido, y siguiendo nuevamente lo indicado por el Grupo de Trabajo del artículo 29 en el Dictamen 02/2013, cabe mencionar que los desarrolladores de aplicaciones deben diseñar un entorno favorable a la seguridad, con herramientas que impidan la propagación de aplicaciones maliciosas y permitan la instalación y la desinstalación sencilla de la aplicación. Señala también que *“la responsabilidad de los desarrolladores de aplicaciones*



en cuanto a la seguridad de sus productos no termina con la puesta en el mercado de una versión operativa. Las aplicaciones, como cualquier producto de software, pueden sufrir deficiencias de seguridad y tener puntos vulnerables, por lo que los desarrolladores deben elaborar soluciones o parches para los mismos y suministrárselos a aquellas partes que pueden ponerlas a disposición de los usuarios o hacerlo ellos mismos.”

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 o las autoridades autonómicas de protección de datos personales correspondientes), 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, debe mencionarse aquí en primer lugar la mencionada en el artículo 25 relativa a la protección de datos desde el diseño y por defecto, lo cual exige la evaluación continua de los riesgos actuales y futuros para la protección de datos y la aplicación de medidas correctoras eficaces.

- Debe hacerse referencia también a la obligación de realizar una evaluación de impacto relativa a la protección de datos, prevista en el artículo 35 del Reglamento. 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.”

En la página web de la Agencia Española de Protección de Datos se encuentra publicado el listado de tratamientos de datos personales en los que es obligatoria la realización de una evaluación de impacto. En este sentido y siguiendo las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento “entraña probablemente un alto riesgo” a efectos del Reglamento (UE) 2016/679, será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de los establecidos en la citada lista. Debe tenerse en cuenta que la lista incluye, entre otros, los siguientes tratamientos:

- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
- Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación



financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

- Tratamientos que impliquen el uso de datos a gran escala.
- Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

Teniendo en cuenta que en el presente supuesto concurren varios de los criterios señalados en la citada lista, en el presente supuesto parece necesario realizar la correspondiente evaluación de impacto.

Por último, debe resaltarse que, entre las nuevas obligaciones del responsable establecidas en el Reglamento general de protección de datos, figura también la de designar, en su caso, un delegado de protección de datos. Prevé a este respecto el artículo 37 del aludido Reglamento, lo siguiente:

“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, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.”