

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

El anteproyecto remitido tiene por objeto regular, en el ámbito de la Administración General del Estado y de su sector público, la relación entre los grupos de interés y las personas titulares de puestos susceptibles de recibir influencia, para garantizar la transparencia en la toma de decisiones públicas y la prevención de situaciones de conflictos de interés.

Tal y como se señala en la Exposición de Motivos, con esta regulación se cubre un importante vacío normativo del ordenamiento jurídico estatal que se ha puesto de manifiesto, de forma reiterada, tanto por la propia sociedad civil como por instituciones comunitarias y organismos internacionales, citando como precedente el Libro verde sobre la iniciativa europea en favor de la transparencia que llevó a la creación del Registro de Transparencia en la Unión en el año 2011, así como las recomendaciones realizadas a España para la regulación de los grupos de Interés en el Informe Estado de Derecho de la Comisión Europea, en la Quinta Ronda de Evaluación del Grupo de Estados contra la Corrupción (GRECO) del Consejo de Europa así como en los informes bianuales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Asimismo, se cita el Objetivo 16 de la Agenda 2030, el componente 11 de la IV política palanca del Plan de Recuperación, Transformación y Resiliencia y el IV Plan de Gobierno Abierto 2020-2024.

## I

El marco normativo aplicable a los tratamientos de datos de carácter personal que puedan realizarse al amparo de la norma proyectada está

constituido, con carácter general, por 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

Dentro de la regulación de los grupos de interés, y a los efectos de las competencias de esta Agencia, destaca la creación de un Registro de grupos de interés de carácter público y obligatorio que va a implicar el tratamiento de datos de carácter personal, en la medida en que se tratan informaciones referidas a personas físicas identificadas o identificables (artículo 4 del RGPD), como pueden ser los datos personales de los grupos de interés que sean personas físicas, los representantes de las personas jurídicas, los sujetos para los cuales se realiza la actividad cuando sean personas físicas y las autoridades y personal público con el que se relacionen.

De este modo, el Registro de de grupos de interés de carácter público deberá cumplir con los principios de protección de datos personales contenidos en el artículo 5 del RGPD:

*1. Los datos personales serán:*

*a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*

*b) 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 («limitación de la finalidad»);*

*c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*

*d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);*

*e) 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 («limitación del plazo de conservación»);*

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

*2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).*

Con carácter previo, debe indicarse que el presente informe se ha elaborado partiendo de la consideración que para el cumplimiento de la finalidad perseguida por el anteproyecto, no resulta necesario el tratamiento de las categorías especiales de datos a las que se refiere el artículo 9.1. del RGPD, respecto de los cuales no se realiza referencia alguna ni en el texto ni en la MAIN.

Si se pretendiera el tratamiento de este tipo de datos personales debe recordarse que es requisito indispensable que, con carácter previo, concurra alguna de las causas que levanten la prohibición de su tratamiento conforme al artículo 9.2. del RGPD.

Por lo que, si previo el análisis de riesgos y la Evaluación de Impacto en la Protección de Datos a los que posteriormente nos referiremos, se considerara necesario que en determinados supuestos se trataran categorías especiales de datos personales, y siempre que se justifique oportunamente, su tratamiento únicamente podría realizarse conforme a lo previsto en la letra g) del artículo 9.2. del RGPD: el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

En este caso, debería recogerse expresamente en el anteproyecto dicha posibilidad, identificando qué tipos de datos personales incluidos en las categorías especiales de datos podrían ser objeto de tratamiento, y limitarlos a los estrictamente necesarios, previendo su supresión inmediata en cuanto no sean necesarios y estableciendo, en su caso, las garantías adicionales que

resulten del correspondiente análisis de riesgos para la adecuada protección de los intereses y derechos fundamentales del interesado.

**Como se ha adelantado, esta Agencia considera que, con carácter general, no resultará necesario dicho tratamiento, por lo que debería recogerse expresamente en el texto de la norma que en ningún caso serán objeto de tratamiento en el Registro las categorías especiales de datos personales contempladas en el artículo 9.1. del RGPD.**

## II

Continuando con al análisis del principio de licitud, el Anteproyecto configura la inscripción en el Registro con carácter obligatorio, señalando en el artículo 6.1. que *“En el Registro de grupos de interés se inscribirán obligatoriamente las personas físicas y jurídicas, sea cual sea su forma o estatuto jurídico, así como las agrupaciones de personas que se conformen en plataformas, foros, redes u otras formas de actividad colectiva sin personalidad jurídica, que realicen la actividad de influencia”*. **Por lo tanto, la base jurídica que legitima el tratamiento es la contemplada en la letra c) del artículo 6.1 del RGPD: “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”**, cumpliéndose con el principio constitucional de reserva de ley que recuerda el artículo 8.1 de la LOPDGDD:

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

Por consiguiente, siendo un tratamiento de datos personales que va a realizar la Administración en cumplimiento de una obligación legal no procede la referencia al consentimiento de los afectados que se contiene en el artículo 7 del Anteproyecto, en el segundo párrafo del apartado 3:

*Quien suscriba la declaración responsable debe asegurar que posee y puede acreditar el consentimiento expreso de las personas físicas que van*

*a ejercer la actividad de influencia para que sus datos identificativos puedan hacerse públicos. Las personas que soliciten la inscripción de datos en el Registro estarán informadas del tratamiento otorgado a la información facilitada en los términos previstos en la normativa aplicable en materia de protección de datos de carácter personal.*

Para ello, debe partirse de la definición del consentimiento del interesado contenida en el artículo 4.11 del RGPD: 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, y que son objeto de un análisis detallado por el Comité Europeo de Protección de Datos en sus Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 4 de mayo de 2020.

A este respecto, tal y como viene destacando esta Agencia, con carácter general el consentimiento del interesado no permite legitimar los tratamientos de datos personales por parte de la Administración por presumirse que dicho consentimiento no es libre, máxime en los supuestos en los que existe una obligación legal. En este sentido, la necesidad de que el consentimiento sea libre implica, según el Considerando 42 del RGPD, que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno”. Además, como añade el Considerando 43, “Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”.

Por lo tanto, y sin perjuicio de que la intervención de las personas físicas que van a ejercer la actividad de influencia pueda ser voluntaria o derivar de otras relaciones jurídicas contractuales con la persona física o con la persona jurídica o entidad sin personalidad cuyo representante suscriba la declaración responsable, el tratamiento de sus datos personales en el Registro, incluida la publicidad de sus datos identificativos impuesta por la ley, no requiere el consentimiento de los afectados, sin perjuicio del deber de informar a los mismos en los términos establecidos en el artículo 13 del RGPD.

**Por todo ello, debería suprimirse en el apartado 3 del artículo 7 la referencia al consentimiento expreso, sustituyéndola por la mención de que quien suscriba la declaración responsable de asegurar que se ha informado a las personas físicas que van a ejercer la actividad de influencia respecto del tratamiento de sus datos personales en el Registro**

conforme a lo previsto en la normativa sobre protección de datos personales, incluido que sus datos identificativos van a hacerse públicos.

Asimismo, debería suprimirse la obligación que impone a las personas que actúan en nombre y representación de los grupos de interés el artículo 9.1. en la letra b): Aceptar que se haga pública la información proporcionada al Registro y la facilitada al personal público, así como la baja en el mismo, excepto aquélla que por motivos legales tenga prohibido o limitado su acceso

Todo ello sin perjuicio del deber de informar por el responsable del Registro a las personas que soliciten la inscripción en los mismos términos del artículo 13 del RGPD, tal y como se contempla en el último inciso del párrafo segundo del apartado 3 del artículo 7.

## II

Una vez identificada la base jurídica que legitima el tratamiento de los datos de carácter personal, derivada del cumplimiento de obligaciones legales al amparo del artículo 6.1.c) del RGPD, deben recordarse las previsiones que al respecto de la misma se contienen en los apartados 2 y 3 del propio artículo 6 del RGPD:

*2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.*

*3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:*

- a) el Derecho de la Unión, o*
- b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.*

*La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen*



*la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.*

En este mismo sentido, el ya citado artículo 8.1. de la LOPDGDD prevé específicamente que la ley que establezca la obligación “*podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679*”.

Estas previsiones deben ponerse en relación con la jurisprudencia del Tribunal Constitucional y del TJUE referida a la limitación del derecho fundamental a la protección de datos personales, tal y como viene señalando de manera reiterada esta Agencia.

De acuerdo con la misma, el derecho a la protección de datos personales es un derecho fundamental, cuyo contenido consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (STC76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre). Pero, además, estas sentencias señalaron igualmente la necesidad de que la injerencia esté prevista en una ley o norma de la Unión Europea, con respeto, en todo caso, al principio de proporcionalidad.

En concreto, el Tribunal Constitucional, en la STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

*- En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). En la*

*STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:*

*Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)."*

*Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites" (STC 292/2000, FJ 15).*

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

*"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el*



*interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6)."*

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

La STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:

*En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

*65 Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice:

*Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del*

*ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].*

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos,

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

*176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].*

Como ya mencionamos más arriba en este informe, la STC 76/2019, tan reiterada, dispone:

*Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites» (STC 292/2000, FJ 15).*

Con el fin de dar adecuado cumplimiento a la normativa y jurisprudencia citada, esta Agencia viene recomendando repetidamente en sus informes que

el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto etc.) quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”.

*g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma*

Dicha EIPD no se ha llevado a cabo por el órgano proponente de la disposición general. Su realización permitiría que los responsables o encargados del tratamiento no tendrían la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general.

Esta Agencia recuerda, asimismo, que el citado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta “los riesgos que se derivan del tratamiento de los datos personales” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que, con la participación del delegado de protección de datos (DPD), se lleven a cabo y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el Anteproyecto de ley establece (ver art. 35.7.d) RGPD).

Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo “desde el diseño” del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma.

Por todo ello, si bien el texto remitido contiene una mención expresa a la aplicación al Registro de lo establecido en la normativa de protección de datos de carácter personal, la misma no es suficiente, dada su generalidad y la aplicación directa de dicha normativa, para entender cumplidos los requisitos legales y jurisprudenciales exigibles a las limitaciones del derecho fundamental, sino que deberá valorarse si el propio texto incorporar previsiones y garantías específicas a este respecto, tal y como se analizará posteriormente, sin perjuicio de las que pudieran resultar de los análisis referidos.

### III

Por otro lado, la aplicación de la normativa sobre protección de datos de carácter personal requiere, tal y como venimos señalando, de la correcta atribución de responsabilidades, identificando el sujeto que va a ostentar la condición de responsable del tratamiento, que el artículo 4.7 del RGPD define 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.*

En el presente caso, tratándose de la actuación de organismos públicos, debe atenderse a las normas jurídicas que atribuyen las correspondientes competencias, criterio recogido asimismo en las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable del tratamiento y encargado en el RGPD, al referirse a los supuestos de control emanado de disposiciones legales:

*22. En algunos casos, el control puede inferirse de una competencia legal explícita; p. ej., cuando la designación del responsable del tratamiento o los criterios específicos de su nombramiento se establecen en el Derecho nacional o de la UE. En este sentido, el artículo 4, punto 7, establece que «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». A pesar de que el artículo 4, punto 7, solo hace referencia al «responsable del tratamiento» en singular, el CEPD también considera posible que el Derecho de la Unión o de los Estados miembros designe más de un responsable del tratamiento, incluso en calidad de corresponsables del tratamiento.*

*23. Cuando el responsable del tratamiento se haya identificado expresamente en la normativa, esto se considerará determinante a la hora de establecer quién actúa como tal. Se presupone, por tanto, que el legislador ha designado como responsable del tratamiento al ente con verdadera capacidad para ejercer el control. En algunos países, el Derecho nacional establece que las autoridades públicas son responsables del tratamiento de datos personales en el marco de sus obligaciones.*

*24. No obstante, es más frecuente el caso en que la legislación, más que nombrar directamente al responsable del tratamiento o fijar los criterios para su nombramiento, establezca un cometido o imponga a alguien el deber de recoger y tratar determinados datos. En tales casos, el objetivo del tratamiento suele venir determinado por la ley. El responsable del tratamiento será normalmente el designado por la ley para cumplir este fin, este cometido público. Este sería, por ejemplo, el caso de un ente al que se le encargaran ciertos cometidos públicos (por ejemplo, la seguridad social) que no se pudieran cumplir sin recoger al menos algunos datos personales, y que, por tanto, creara una base de datos o un registro para realizar dichas tareas. En este caso, aunque indirectamente, la legislación establece quién es el responsable del tratamiento. Con mayor frecuencia, la ley puede imponer a entes públicos o privados la obligación de conservar o facilitar determinados datos. Estos entes se considerarían en principio los responsables del tratamiento necesario para cumplir esta obligación.*

Por consiguiente, para la identificación de la condición de responsable del tratamiento de los datos personales debe atenderse a la atribución competencial que se realiza en el anteproyecto, cuyo artículo 5.2. dispone lo siguiente:

*2. La OCI, a la que se adscribe el Registro de grupos de interés, será la responsable de la gobernanza y gestión del mismo, teniendo, asimismo, atribuidas las potestades de seguimiento y control previstas en esta ley*

*De acuerdo con lo establecido en el artículo 19.1 de la ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, la OCI actuará con plena autonomía funcional en el ejercicio de las funciones atribuidas en esta ley.*

**Consecuentemente, corresponderá a la OCI la condición de responsable del tratamiento, lo que debería recogerse expresamente en la norma proyectada.**

#### IV



Sin perjuicio de lo anterior, procede analizar la regulación contenida en la norma con el objeto de identificar aquellos preceptos que inciden en el tratamiento de los datos de carácter personal, así como las posibles precisiones y garantías que el mismo establezca.

En primer término, la **necesidad del tratamiento** de los datos personales encuentra su justificación en la propia Exposición de Motivos a la que ya nos hemos referido al principio del presente informe. Asimismo, como una medida que permite garantizar la proporcionalidad del tratamiento, el artículo 4, en su número 5, excluye de la consideración de grupos de interés a “Las personas físicas que actúen en condición estrictamente personal, respecto de asuntos de índole particular carentes de relevancia económica o social significativa”.

La **finalidad del tratamiento** se recoge expresamente en el apartado 1 del artículo 5: “garantizar la transparencia y la integridad de las actividades que desarrollan dichos grupos en sus relaciones con las personas miembros del Gobierno, el personal que ostenta la condición de alto cargo, el personal directivo y demás personal público”.

En cuanto al cumplimiento del **principio de minimización de datos** personales y conforme a la doctrina jurisprudencial citada, que requiere que las limitaciones del derecho fundamental se recojan en la propia ley que legitima el tratamiento, directamente o mediante remisión a otra norma legal, sin que sea suficiente las habilitaciones reglamentarias genéricas, esta Agencia considera necesario que se identifiquen en la ley, al menos, las **categorías de datos** personales que pueden ser objeto de tratamiento, y que deberán ser adecuados, pertinentes y limitados a lo necesario para la finalidad perseguida. A estos efectos, se considera insuficiente la remisión que se contiene en el apartado 3 del artículo 5 al desarrollo reglamentario: “Reglamentariamente se establecerán las normas relativas a la organización y el funcionamiento del mismo, que deberán incluir, como mínimo, una clasificación de los sujetos inscritos y la información objeto de inscripción”.

Dicha previsión debe ponerse en relación con el contenido del artículo 7, referido al procedimiento de inscripción, cuyo apartado 2 indica la información que debe facilitarse y que, en el caso de personas físicas, incluidos los representantes de las personas jurídicas así como los sujetos para los que se

realiza la actividad que tengan dicha condición, implicará el tratamiento de sus datos personales:

2. La solicitud de inscripción deberá incluir, al menos, información relativa al nombre y domicilio o razón social del grupo de interés, tipo de organización, datos de contacto, descripción de su finalidad u objeto social, ámbitos de interés y financiación. Asimismo, incluirá información financiera, referida al último ejercicio contable cerrado, indicando la parte imputable a la actividad de influencia y, en su caso, el importe y el origen de los fondos recibidos de las administraciones e instituciones públicas.

En el supuesto de personas jurídicas y agrupaciones también se incluirá el cargo de la persona que actúe en su nombre y representación y, en su caso, se deberá indicar si forman parte del grupo de interés otras entidades o federaciones o si el grupo de interés forma parte, a su vez, de algunas de éstas.

Si se realiza la actividad de influencia por cuenta de terceros, también se deberá indicar la identidad de los sujetos para los cuales se realiza la actividad y las cantidades económicas que reciben por este concepto.

A este respecto, se considera que la enumeración de la información en la ley debe ser taxativa, de modo que las categorías de datos personales, referida a los datos identificativos y de contacto, datos referidos a la actividad profesional y datos financieros, no pueda ampliarse reglamentariamente, sin perjuicio del posible desarrollo reglamentario de los datos concretos que puedan ser objeto de tratamiento, respetando siempre el principio de minimización de datos.

Por ello, se propone la siguiente redacción del párrafo segundo del artículo 5.3:

“Reglamentariamente se establecerán las normas relativas a la organización y el funcionamiento del mismo, que deberán incluir, como mínimo, una clasificación de los sujetos inscritos y la información objeto de inscripción, que en el caso de datos personales, **quedará limitada a los datos identificativos y de contacto, datos referidos a la actividad profesional y datos financieros que se determinen**”.

Por otro lado, en cuanto al **acceso a los datos de carácter personal** y teniendo en cuenta que el registro es de carácter público, dicha circunstancia deberá tenerse en cuenta, igualmente, respecto de los datos de carácter personal que se pretendan publicar, teniendo en cuenta las limitaciones que

podrían derivar de la normativa sobre protección de datos personales derivada del incremento del riesgo para los derechos y libertades de los afectados que pueda derivarse de dicha publicidad. En este sentido, procede recordar la especial protección que la LOPDGDD otorga al documento nacional de identidad u otros documentos equivalentes, tal y como se refleja en su disposición adicional séptima, con el objeto de evitar que pueda hacerse público el nombre y apellidos y el número completo de dichos documentos.

Asimismo, la normativa sobre protección de datos personales deberá tenerse debidamente en cuenta respecto de otro tipo de información que vaya a hacerse pública y que pueda contener datos de carácter personal, como es el supuesto contemplado en la letra d) del apartado 2 del artículo 6:

*d) Las actuaciones desarrolladas por los grupos de interés, especialmente las reuniones y audiencias mantenidas con el personal público, así como las comunicaciones, los informes y otras contribuciones relacionadas con las materias tratadas.*

A este respecto, deberán aplicarse los principios recogidos en el artículo 5 del RGPD a los tratamientos de datos personales que puedan contenerse en las comunicaciones, informes y otras contribuciones a los que se refiere el precepto, singularmente los principios de limitación de la finalidad y minimización de datos.

**De este modo, debería diferenciarse entre aquellos datos personales que se van a hacer públicos y aquellos otros que, por aplicación de la normativa sobre protección de datos personales, no tengan tal carácter, de modo que el acceso a estos últimos solo pueda tener lugar en los términos previstos en dicha normativa.**

Otro de los principios fundamentales recogidos en el artículo 5 del RGPD es el de **exactitud de los datos**, y para cuyo adecuado cumplimiento se establecen previsiones específicas en el texto remitido, que se valoran positivamente. En este sentido, el artículo 7.4. señala que “La información declarada en la solicitud de inscripción, en particular la de carácter financiero, deberá actualizarse por el grupo de interés anualmente.” Y el artículo 9.1.a) establece como primera obligación de las personas que actúen en nombre y representación de los grupos de interés la de “Comunicar y mantener actualizados los datos identificativos del grupo de interés y de sus miembros que realicen actividades de influencia, facilitándolos en los modelos electrónicos que se establezcan reglamentariamente”. Asimismo, se incluyen las correspondientes sanciones en el artículo 13, que en su apartado 1.c) tipifica como infracción muy grave el “Inscribirse en el Registro de grupos de interés con datos o documentos falsos, u omitir deliberadamente datos y

*documentos que deberían ser aportados al Registro”; en el apartado 2.d) como infracción grave el “No actualizar la información aportada al Registro cuando corresponda, siempre y cuando se esté realizando efectivamente la actividad de influencia” y el apartado 3 como infracción leve “el retraso superior a 5 días hábiles, sin justificación acreditada, en la actualización de la información que ha de inscribirse en el Registro de grupos de interés, tras el requerimiento que se formule al efecto por la OCI”.*

En cuanto al **principio de conservación de los datos**, el artículo 7, al regular el procedimiento de inscripción en el Registro, señala en el último inciso del párrafo primero de su apartado 4 que *“Se entenderá caducada la inscripción, transcurrido el plazo de dos años desde la última actualización o modificación, sin perjuicio de que se pueda mantener la información en el Registro a fin de facilitar la trazabilidad en el tiempo de las actuaciones desarrolladas por el grupo de interés”.*

Con dicha previsión se estaría estableciendo una previsión de permanencia indefinida de los datos en el Registro, cuestión sobre la que se pronunció esta Agencia en el Informe 74/2018, referente al Borrador de Real Decreto por el que se aprueba el reglamento de desarrollo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, señalando lo siguiente:

*Dentro igualmente de las disposiciones relacionadas con la aplicación de los límites derivados del artículo 15 de la Ley 19/2013 y la normativa de protección de datos de carácter personal debe ahora hacerse referencia al artículo 10 del Reglamento que sería objeto de aprobación por el borrador sometido a informe, cuyo apartado 1 dispone que “Con carácter general, la información se actualizará en el Portal de la Transparencia, al menos, trimestralmente, salvo que la normativa específica establezca otros plazos atendiendo a las peculiaridades propias de la información de que se trate y sin perjuicio de la posibilidad de publicar en plazos más breves toda la información que se estime conveniente por el órgano competente”, añadiendo el apartado 2 que “Se habilitará la posibilidad de acceder a la información que, habiendo sido objeto de publicidad, hubiera sido sustituida”.*

*De este modo, se establecería un régimen de permanencia indefinida de los datos en el portal de la transparencia, con independencia de su antigüedad y relevancia.*

*En este sentido, es preciso recordar que el artículo 5.1 e) del reglamento general de Protección de Datos consagra el denominado principio de conservación, al disponer que los datos de carácter personal 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”.*

*Ciertamente, el principio se completa con un segundo inciso, a cuyo tenor, “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”. No obstante, la finalidad de archivo de interés público no aparecería vinculada a un principio general de publicidad activa, sino al derecho de acceso a la información pública, de modo que el hecho de que los datos se conservasen para tal finalidad no implicaría que los mismos se encontrasen a disposición de cualquier persona en un portal libremente abierto al público.*

*Por este motivo, entiende esta Agencia que sería necesario completar la previsión del apartado 2 del artículo 10 del Reglamento que sería aprobado por el Proyecto sometido a informe, incorporando una regla que determinase la posible desaparición de los datos del portal de la transparencia transcurridos determinados períodos de tiempo que supusiesen una pérdida de relevancia de la información a efectos de publicidad activa, sin perjuicio de que, en su caso, continuase la conservación de los datos, en los términos establecidos en la legislación reguladora de los archivos de interés público y, particularmente en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.*

*De este modo, el texto debería incorporar una regla que estableciese el período de obsolescencia de los datos para su conservación en el Portal de la Transparencia, bien de forma general, bien sometida a un desarrollo posterior, que en todo caso debería ser sometido al parecer de esta Agencia Española de Protección de Datos.*

**Siguiendo el mismo criterio, se considera necesario que se establezca un plazo máximo de permanencia de los datos personales correspondientes a inscripciones caducadas en el Registro, al menos en cuanto a su accesibilidad pública y sin perjuicio de la aplicación de la correspondiente normativa archivística pública.**

Por último, en cuanto a **los principios de integridad y confidencialidad**, ya se ha indicado la necesidad de atender a lo señalado en el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, prevaleciendo las medidas de seguridad que deriven de la aplicación de la normativa sobre protección de datos personales.

## **V**

Para concluir, y con el objeto de sistematizar la normativa contenida en el anteproyecto que afecta al tratamiento de los datos de carácter personal a la que nos venimos refiriendo en el presente informe y facilitar su aplicación, se sugiere la posibilidad de incluirla en una disposición adicional específica, tal y como se ha realizado en otras normas a propuesta de esta Agencia, como la Ley 20/2022, de 19 de octubre, de Memoria Democrática (disposición adicional décima) o la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte (disposición adicional cuarta).

Para ello, se propone la siguiente redacción:

### **Disposición adicional primera. Protección de datos de carácter personal.**

**1. Los tratamientos de datos personales regulados en la presente ley se llevarán a cabo conforme a lo dispuesto en 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 y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**

**Los derechos de acceso, rectificación y supresión se ejercitarán conforme a la normativa referida en el párrafo anterior.**

**2. El tratamiento de los datos personales relativos al Registro de grupos de interés a que se refiere el artículo 5 tendrá por finalidad garantizar la transparencia y la integridad de las actividades que desarrollan dichos grupos en sus relaciones con las personas miembros del Gobierno, el personal que ostenta la condición de alto cargo, el personal directivo y demás personal público.**

**El responsable del tratamiento es la OCI.**

**La base jurídica principal del tratamiento de acuerdo con el objetivo y finalidad de la presente ley es el cumplimiento de una obligación legal**



**aplicable al responsable del tratamiento de acuerdo con lo dispuesto en el artículo 6.1.c) del Reglamento (UE) 2016/679.**

**Podrán ser objeto de tratamiento las siguientes categorías de datos personales: datos identificativos y de contacto, datos referidos a la actividad profesional y datos financieros, en los términos previsto en la presente ley. Los datos personales deberán ser adecuados, pertinentes y limitados a lo necesario para la finalidad perseguida, de acuerdo con el principio de minimización de datos, sin que, en ningún caso, puedan ser objeto de tratamiento las categorías especiales de datos previstas en el artículo 9.1. del Reglamento (UE) 2016/679.**

**Los datos personales serán recabados de las personas que actúen en nombre y representación de los grupos de interés y deberán ser actualizados por los mismos conforme a las previsiones de la presente ley.**

**El responsable del tratamiento garantizará que se facilite a dichos representantes la información referida al tratamiento de los datos personales, en los términos previstos en el artículo 13 del Reglamento (UE) 2016/679. Asimismo, dicha información estará accesible a través del portal de transparencia de la Administración General del Estado y del sitio web de la OCI.**

**El representante del grupo de interés deberá, por su parte, informar a las personas físicas que van a ejercer la actividad de influencia respecto del tratamiento de sus datos personales en el Registro conforme a lo previsto en la normativa sobre protección de datos personales, incluido que sus datos identificativos van a hacerse públicos.**

**El acceso a los datos de carácter personal que no tengan carácter público por aplicación de la normativa sobre protección de datos personales solo procederá en los términos previstos en dicha normativa.**

**De acuerdo con la finalidad del tratamiento, se conservarán los datos recogidos en virtud de las disposiciones legales durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos y en su caso por el tiempo necesario para atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Los datos personales correspondientes a las inscripciones caducadas dejarán de ser públicos una vez transcurridos cinco años desde que se produzca dicha caducidad.**

**El responsable del tratamiento deberá garantizar la aplicación de las medidas técnicas y organizativas que resulten del análisis de riesgos y, en su caso, de la correspondiente evaluación de impacto en la protección de datos, en los términos previstos en el artículo 3 del Real Decreto**

**311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.**

**En el supuesto de que intervenga una entidad como encargada del tratamiento, deberá suscribirse o adoptarse el correspondiente instrumento jurídico en los términos previstos en el artículo 28.3 del Reglamento (UE) 2016/679.**