

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.

La emisión del presente informe se solicita con carácter urgente, conforme al artículo 47 del Real Decreto-Ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, al enmarcarse dentro del componente 11 de dicho Plan.

El anteproyecto tiene por objeto, conforme al artículo 1.1., *“crear la Autoridad Administrativa Independiente de Defensa del Cliente Financiero, establecer un sistema público de resolución extrajudicial de controversias surgidas entre las entidades financieras y los clientes financieros e impulsar la educación financiera”*. De este modo, la finalidad perseguida, como especifica el artículo 1.2. es *“aumentar la protección de los clientes de las entidades financieras, aumentar la seguridad jurídica en el ámbito de las normas de conducta que deben observar las entidades financieras, y contribuir a la extensión de las buenas prácticas y usos financieros en las relaciones de las entidades financieras con sus clientes, con unos estándares adecuados y comunes de protección en el que se fortalezca la transparencia, la inclusión financiera de los colectivos vulnerables y la competencia en cuanto a calidad del servicio, en beneficio del conjunto de la sociedad”*.

Tal y como se señala en su Exposición de Motivos, después de un análisis de la normativa aplicable, en el sistema actual de protección de los clientes que operan en los mercados financieros coexisten diversas instancias específicas de resolución de conflictos: En primer lugar, los servicios de atención a la clientela de las entidades financieras; en un segundo estadio, los servicios de reclamaciones de los organismos supervisores; y, por último, los órganos judiciales. A ellos se suma la posibilidad de acudir a otros mecanismos extrajudiciales de resolución de conflictos desarrollados en nuestro país, en particular para determinado tipo de controversias de alcance general que desborden de la capacidad de los órganos jurisdiccionales.

Partiendo de lo anterior, el Anteproyecto de ley tiene como objetivo complementar este sistema institucional de resolución de reclamaciones mediante la creación de una única autoridad que goce de autonomía e independencia y cuyas resoluciones se dicten con celeridad, atendiendo a criterios uniformes y de carácter vinculante para las entidades financieras en reclamaciones de cuantía inferior a 20.000 euros. Esta nueva autoridad integrará los actuales servicios de reclamaciones de los organismos supervisores, que dejarán de realizar estas funciones de acuerdo con las disposiciones transitorias de esta ley.

De este modo, el sistema de resolución extrajudicial de conflictos resultante, tal y como se señala en su artículo 5.1. estará integrado por los servicios de atención a la clientela y defensores de la clientela de las entidades financieras y la Autoridad Administrativa Independiente de Defensa del Cliente Financiero, en los términos previstos, respecto de la Autoridad, en esta ley, en la ley 44/2002, y sus normas de desarrollo.

I

En el ámbito de competencias de esta Agencia, dos son los aspectos fundamentales del Anteproyecto de ley que inciden en materia de protección de datos de carácter personal: la exclusión por un lado, del ámbito de competencias de la Autoridad que se crea de las reclamaciones que versen sobre protección de datos personales y el régimen jurídico aplicable a los tratamientos de datos personales que se realicen en el ámbito del Anteproyecto de ley.

En relación con la primera de estas cuestiones, la exclusión del ámbito de aplicación de la ley de los conflictos que puedan plantearse en materia de protección de datos personales, prevista en el artículo 3.2.d) del Anteproyecto deriva de la propia normativa aplicable a los mismos, en cuanto que de las previsiones contenidas 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, la competencia en esta materia está atribuida a esta Agencia Española de Protección de Datos.

II

En cuanto a la normativa aplicable a los tratamientos de datos personales, la norma proyectada contiene una previsión genérica al regular el

sistema de resolución extrajudicial de conflictos en su artículo 7, en el que se limita a indicar la normativa aplicable:

Artículo 7. Tratamiento de datos personales.

El tratamiento de datos personales realizado en el ámbito de esta ley se hará atendiendo a lo establecido 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; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo y en la Convención sobre los Derechos de las Personas con Discapacidad en su artículo 31.1.a).

A este respecto, deben realizarse algunas precisiones.

En primer término, siendo el elemento fundamental del anteproyecto la regulación de la actuación de la Autoridad administrativa independiente de defensa del cliente financiero, configurada como Autoridad Administrativa independiente de las previstas en el Capítulo IV del Título II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (Título II del Anteproyecto) y de la cooperación con el Ministerio de Asuntos Económicos y Transformación Digital, el Ministerio de Consumo, Banco de España y Comisión Nacional de los Mercados y de la Competencia (Título III del Anteproyecto) debe comenzarse identificando la base jurídica que determina la licitud de los respectivos tratamientos de datos personales.

A estos efectos, tal y como se señalaba en nuestro Informe 175/2018, *“con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según os casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD)”. Por otro lado, respecto de la obligación legal, el Informe 74/2019 matizaba que la base jurídica del artículo 6.1.c) “únicamente en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal, y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público”.*

De este modo, los tratamientos de datos de carácter personal que se puedan realizar por la Autoridad Administrativa Independiente de Defensa del Cliente Financiero quedarían legitimados, con carácter general, conforme a lo previsto en la letra e) del artículo 6.1 del RGPD: “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”. En cuanto a los que se puedan realizar en cumplimiento del deber de cooperación regulado en el Título III del Anteproyecto, la base jurídica sería la determinada por la letra c) del citado artículo 6.1 del RGPD: “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”. En ambos casos se cumpliría, además con el principio constitucional de reserva de ley que recuerda el artículo 8 de la LOPDGDD:

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

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

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

Por otro lado, en los supuestos en que sea necesario proceder al tratamiento de categorías especiales de datos, sería necesario que, con carácter previo, concurra alguna de las causas que permiten levantar la prohibición de su tratamiento, conforme a lo previsto en el artículo 9 del RGPD. Al no contener la Memoria de análisis de impacto normativo referencias específicas a los tratamientos de datos de carácter personal que puedan realizarse (algo sobre lo que se incidirá más adelante), no puede determinarse a priori si, para la correcta aplicación del anteproyecto, será necesario el tratamiento de las categorías especiales de datos, como pudieran ser, por ejemplo, datos de salud, si la reclamación versara sobre algún producto financiero en que se traten este tipo de datos personales.

Por tanto, esta Agencia considera que, con carácter general, el tratamiento de las categorías especiales de datos a las que se refiere el artículo 9.1. del RGPD no resultará necesario para la gestión de las reclamaciones recibidas y la tramitación de los correspondientes procedimientos, por lo que debería recogerse expresamente en el anteproyecto que si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

No obstante, si previo el análisis de riesgos o la EIPD a los que nos referiremos posteriormente, se considerara necesario que en determinados supuestos se trataran categorías especiales de datos personales, debe identificarse el supuesto concreto del artículo 9.2. del RGPD que levanta la prohibición.

En el caso de que así fuera, debe entenderse excluida la causa del artículo 9.2.a) del RGPD, partiendo de que el consentimiento del afectado requiere que el mismo sea libre, lo que en principio se presume que no es así en las relaciones con la Administración (Considerando 43 del RGPD) y que implicaría que el mismo pudiera denegarlo sin sufrir perjuicio alguno y, por tanto, sin que se viera perjudicada su reclamación y, en su caso, la cooperación con otros órganos administrativos, lo que supondría, al mismo tiempo, que dicho tratamiento no sería necesario para la correcta aplicación de la ley. Por tanto, debería concurrir alguna de las demás causas de levantamiento de la prohibición que contempla el citado artículo 9.2., entendiendo esta Agencia que podría aplicarse, en su caso y siempre que se acredite la concurrencia de los requisitos que las mismas establecen, las prevista en sus letras f) o g):

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

No obstante, debe traerse a colación la doctrina de nuestro Tribunal Constitucional contenida en la Sentencia 76/2019, de 22 de mayo respecto de la necesidad de que las normas que habiliten al tratamiento de categorías especiales de datos establezcan las garantías oportunas para la protección del derecho fundamental y la norma en la que deben recogerse dichas garantías (F.J.8):

(...) La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (...). Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares. (...)

Por consiguiente, debería analizarse si procede el tratamiento de estas categorías de datos personales y, en su 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.** Algunas de estas garantías pueden ser comunes al tratamiento de otros datos personales, como son las derivadas del deber de secreto ya contemplado en la norma, o las derivadas del principio de limitación de la finalidad, de modo que no puedan tratarse para finalidades distintas de las contempladas en el anteproyecto, o las del principio de minimización de datos personales, de modo que se traten los que sean estrictamente necesarios para dicha finalidad, a las que nos referiremos posteriormente. **No obstante, pueden incluirse garantías específicas para el tratamiento de estas categorías especiales de datos, como su posible anonimización o pseudonimización.**

III

Por otro lado, además del principio de licitud, deberán respetarse todos los principios recogidos 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 el fin de facilitar el cumplimiento de los citados principios en los supuestos, como el presente, en que el tratamiento viene legitimado conforme a las letras c) y e) del artículo 6.1. del RGPD, tanto el artículo 6.3. del RGPD como el artículo 8 de la LOPDGDD prevén la posibilidad de que las normas que legitiman el tratamiento puedan contener disposiciones específicas para adaptar la aplicación de la normativa sobre protección de datos personales.

Además, siendo el derecho a la protección de datos personales 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» (STC 76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre) resulta imperativo cumplir con los requisitos señalados por el Tribunal Constitucional en las citadas sentencias, que reconociendo su carácter de derecho limitado, 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).

De acuerdo con la citada doctrina jurisprudencial, los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

Para el adecuado establecimiento de dichos límites y la correcta identificación de las garantías que deban trasladarse al texto legal, 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, realice un análisis de riesgos y, en su caso, 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 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 -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- 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 (MAIN). 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, o cuando menos, no se ha aportado a esta AEPD. Su realización permitiría que los responsables o encargados del tratamiento, una vez promulgada la norma, 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 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 se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y, en su caso, 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 (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.

En relación con dichas garantías, el texto remitido incluye como garantía específica un concreto deber de secreto en su artículo 28, que refuerza al deber de confidencialidad establecido en el artículo 5 de la LOPDGDD:

Artículo 28. Confidencialidad.

1. La Autoridad Administrativa Independiente de Defensa del Cliente Financiero y su personal deberán guardar secreto de cuantos datos e informaciones reciban en el desempeño de sus funciones, y no podrán utilizarlos en beneficio propio, ni facilitarlos a terceros ni a otros órganos administrativos, sin perjuicio de las obligaciones de transparencia e información que imponga la legislación vigente.

2. Las autoridades y personas que, conforme a lo previsto legalmente, puedan recibir información de la Autoridad Administrativa Independiente de Defensa del Cliente Financiero quedarán también obligadas a guardar secreto y a no utilizar la información recibida con finalidades distintas de aquélla para la que les fue suministrada.

3. Los intercambios mutuos de información en los que se materialice la cooperación y colaboración en cumplimiento de lo previsto en los artículos 29, 30 y 50 deberán realizarse atendiendo en todo caso a las normas sobre protección de datos personales y sobre secreto profesional y comercial.

La inclusión de dicho deber de secreto se valora positivamente por esta Agencia, si bien considera necesario la inclusión de otras garantías tendentes a hacer efectivos el resto de los principios contenidos en el artículo 5 del RGPD.

No obstante, al no haberse realizado el análisis de riesgos ni la EIPD no se conocen cuáles son esos riesgos que derivan del tratamiento de datos personales que la norma prevé, lo que adquiere singular relevancia respecto del deber de cooperación regulado en el Título III y, particularmente, respecto de la previsión contemplada en el artículo 50 al final de su apartado 1:

Las autoridades supervisoras y la Autoridad Administrativa Independiente de Defensa del Cliente Financiero tendrán, respectivamente, en los términos que se establezcan reglamentariamente, acceso a la información de las bases de datos de

reclamaciones recibidas y resueltas para llevar a cabo las funciones que tengan legalmente encomendadas.

Como hemos indicado, se carece de información respecto de la necesidad de dicho acceso a las bases de datos, así como la forma en la que se procederá a la misma, sin que las garantías que afecten al derecho fundamental a la protección de datos personales se puedan dejar al desarrollo reglamentario, tal y como se viene indicando. Además, al no contener la MAIN previsión alguna respecto del tratamiento generalizado y mecanizado, masivo, de datos personales que establece la norma, a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia las posibles medidas y garantías que paliarían esos riesgos.

En relación con esta cuestión, debe recordarse que La ley 40/2015 establece, con carácter general, un deber de colaboración entre las distintas Administraciones, pero dicho deber de colaboración está sujeto a que se respeten los derechos fundamentales de los individuos, y más concretamente al derecho a la protección de datos de las personas físicas. El art. 13 h) de la ley 39/2015 así lo establece expresamente, por lo que el deber de colaboración interadministrativa previsto en el art. 3 k) de la ley 40/2015 ha de entenderse modulado por dicho precepto, tal y como expresamente resulta, por otra parte, del artículo 155 de la propia ley 40/2015, en cuanto que sujeta el acceso de los datos que cada Administración debe facilitar a las restantes Administraciones Públicas a lo previsto en la normativa de protección de datos de carácter personal.

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional contraria al tratamiento masivo de datos personales, recogida con claridad en su Sentencia 17/2013 de 31 de enero de 2013, en sus Fundamentos Jurídicos 7 y 8.

Señala el FJ7, referido al acceso por parte de los órganos competentes en materia de extranjería a los datos obrantes en poder de otros órganos administrativos:

En cuanto al segundo párrafo de la disposición adicional impugnada, el mismo autoriza a los órganos de la Administración estatal, competentes en el ámbito de los procedimientos administrativos que se tramiten en el ámbito que regula la Ley Orgánica de derechos y libertades de los extranjeros y solamente en el ejercicio de las competencias que tienen atribuidas, para acceder a los ficheros en los que obren datos necesarios para su actuación de la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al padrón municipal de

habitantes, lo cual ha de realizarse de acuerdo con la legislación sobre protección de datos sin que sea preciso el consentimiento del interesado. Al respecto, conviene hacer notar que la mención del precepto a los procedimientos administrativos tramitados en el ámbito de la Ley Orgánica de derechos y libertades de los extranjeros no puede entenderse sino haciendo referencia a la tramitación de un determinado expediente en el que resulta necesaria la constancia de determinado dato que ya obra en poder de otro órgano de la Administración General del Estado, tratándose así de un acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado. La finalidad de esa cesión no es otra que comunicar el contenido de ficheros con datos tributarios, de Seguridad Social o de residencia, datos que, en cualquier caso, son ya previamente conocidos por la Administración General del Estado, atendiendo a la necesidad de que la misma disponga de la información oportuna para la gestión de procedimientos en materia de extranjería que son también de su competencia. Por ello, en la medida en que han de tratarse de datos relacionados con un concreto procedimiento y que ya obran en poder de la Administración pública, no puede considerarse vulnerado el art. 18.4 CE. En todo caso, como ya hemos señalado, tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación. Así, rectamente interpretada en los términos antes expuestos, resulta que esa cesión de datos que el acceso previsto supone ha de realizarse de acuerdo con lo que al respecto disponga la Ley Orgánica de protección de datos lo que determina, no solamente la aplicación de lo que la misma dispone en materia de información al interesado respecto de la cesión de datos (art. 5.4 LOPD), sino también que la cesión, establecida en una norma legal [art.11.2 a) LOPD], se produce para el cumplimiento de finalidades legítimas del órgano cedente y del cesionario (art. 4.1 LOPD), finalidades que, desde el punto de vista material, no resultan ser incompatibles entre sí (art. 4.2 LOPD), sino que, por el contrario, los datos son comunicados para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario que contribuyen a garantizar un bien de relevancia constitucional: dar cumplimiento a lo dispuesto en la ley, en este caso la de extranjería (arts. 10.1 y 13.1 CE).

Asimismo, en su FJ 8, interpreta el artículo 16.3 de la Ley de Bases de Régimen Local para determinar la constitucionalidad del mismo. Tal y como ha sido interpretado por el TC en dicha sentencia (FJ 8), este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten

solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes. En suma, esta petición, que no se refiere específicamente a la cesión de datos del padrón en lo concerniente a los datos de los extranjeros, tiene por finalidad poder disponer de los datos relativos a la residencia o el domicilio que constan en el padrón municipal, (...). De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el principio de reserva de ley para establecer dicho cambio, (...) la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.

(...) los datos cedidos han de ser los estrictamente necesarios para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá motivarse la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal. El precepto ha contemplado ambos extremos de manera que cualquier cesión de los datos del padrón debe fundamentarse en la necesidad por parte de la Administración cesionaria actuando en el ejercicio de sus competencias, de conocer, en cada caso concreto, el dato relativo al domicilio de la persona afectada, extremos que han de ser adecuadamente valorados por la cedente a fin de apreciar si los datos que se solicita son realmente necesarios, pertinentes y proporcionados, atendiendo a la competencia que pretende ejercer la Administración cesionaria (art. 4 in fine de la Ley 30/1992). Se trata así de una regla de por sí restringida a los datos relativos a la residencia y al domicilio en cada caso concreto, y a la que le resultarán de aplicación, de más está decirlo, el resto de principios y previsiones que conforman el contenido del derecho reconocidos en la legislación sobre protección de datos.

De lo anteriormente transcrito, y del resto de la fundamentación jurídica contenida en dicha sentencia resulta que el TC ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley.

Por consiguiente, no cabe un acceso masivo e indiscriminado a datos personales, y por lo tanto, en cambio, cuando exista la posibilidad de cesión establecida en una ley, como ocurre en el presente caso, dicho acceso deberá ser siempre ***“específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado”***; ***“tal acceso sólo podría producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación.”*** (STC 19/2013, FJ 7º), debiendo recogerse en el texto legal las garantías oportunas que garanticen el cumplimiento de dichos requisitos.

IV

Conforme a lo señalado en los apartados precedentes y con la finalidad de colaborar a identificar las garantías oportunas, sin perjuicio de las que puedan resultar del correspondiente análisis de riesgos o, en su caso, de la EIPD, esta Agencia propone que se complete el artículo 7, recogiendo, al menos los siguientes aspectos:

- El tratamiento de datos personales que resulte necesario para el cumplimiento de los fines de la Autoridad Administrativa Independiente de Defensa del Cliente Financiero se encuentra amparado por lo dispuesto en el artículo 6.1.e) del Reglamento (UE) 2016/679, al realizarse para el cumplimiento de una misión de interés público y en el ejercicio de potestades públicas conferidas a la misma.

Los datos personales obtenidos por la Autoridad Administrativa Independiente de Defensa del Cliente Financiero solo podrán utilizarse para el cumplimiento de los fines del artículo 9.

- El tratamiento de los datos personales que resulten necesarios para el cumplimiento de los deberes de colaboración y de cooperación previstos en el artículo 30 y en el Título III se encuentra amparado por lo dispuesto en el artículo 6.1.c) del Reglamento (UE) 2016/679, al ser necesarios para el cumplimiento una obligación legal.

El acceso a los datos personales sólo podrá producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente sin que sea posible un acceso masivo e indiscriminado a los datos de carácter personal.

- Los sistemas de información que traten datos personales deberán garantizar la aplicación de las medidas técnicas y organizativas que resulten del análisis de riesgos o 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 con los respectivos responsables del tratamiento el correspondiente instrumento jurídico en los términos previstos en el artículo 28.3 del Reglamento (UE) 2016/679.

Además, si previo los análisis oportunos se concluyera que resulta necesario el tratamiento de categorías especiales de datos personales deberá 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 su posible anonimización o pseudonimización, según proceda.

Todo ello sin perjuicio de otras garantías específicas que pudieran resultar del correspondiente análisis de riesgos o, en su caso, de la EIPD.

V

Para concluir, debe hacerse especial referencia a los tratamientos de datos personales necesarios para acreditar el requisito de honorabilidad comercial y profesional previsto en el artículo 14 respecto de las personas titulares de la Presidencia y Vicepresidencia:

Artículo 14. Requisitos de las personas titulares de la Presidencia y Vicepresidencia.

1. Las personas titulares de la Presidencia y de la Vicepresidencia de la Autoridad Administrativa Independiente de Defensa del Cliente Financiero deberán poseer reconocida honorabilidad comercial y profesional y acreditar para su designación que poseen conocimientos y experiencia profesional adecuados de, al menos, diez años y un reconocido prestigio en el ámbito jurídico, económico o financiero, así como en materia de protección de los clientes financieros, así como no incurrir en potenciales conflictos de interés como consecuencia de sus actividades anteriores.

2. Concorre honorabilidad en quienes hayan venido mostrando una conducta personal, comercial y profesional que no arroje dudas sobre su capacidad para desempeñar una gestión sana y prudente de la Autoridad Administrativa Independiente de Defensa del Cliente Financiero.

En relación con la acreditación del citado requisito se plante la hipotética cuestión de que el legislador pueda prever, al igual que ocurre en otras normas jurídicas aplicables en los sectores financieros, asegurador o del mercado de valores, la necesidad de tratar datos relativos a condenas penales o infracciones administrativas.

A este respecto, debe recordarse que el tratamiento de dichos datos, conforme a las previsiones de los artículos 10 y 27 de la LOPDGDD en relación con el artículo 6.1.c) del RGPD, requiere que esté expresamente previsto en una norma con rango de ley, siendo criterio reiterado de esta Agencia que la correspondiente norma legal recoja, de manera expresa, el tratamiento de dichos datos, precisando, asimismo, las conductas y tipos delictivos que deben ser objeto de valoración y el uso de los mismos, de acuerdo con los principios de minimización y limitación de la finalidad.

Por lo tanto, si así se prevé, deberá recogerse esta circunstancia, en los términos señalados, en el propio artículo 14, sin que pueda dejarse a un hipotético desarrollo reglamentario al amparo de la disposición final undécima.