

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 completar la incorporación al ordenamiento jurídico interno de las modificaciones realizadas en la normativa aplicable a las entidades de crédito en virtud del denominado “paquete bancario”, que recoge los últimos acuerdos adoptados por el Comité de Supervisión Bancaria de Basilea y por el Consejo de Estabilidad Financiera, y que han dado lugar a modificaciones en el marco de resolución y liquidación aplicable a las entidades de crédito, recogidas en el Reglamento (UE) 2019/877 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 modifica el Reglamento (UE) n.º 806/2014 en lo que se refiere a la capacidad de absorción de pérdidas y de recapitalización para las entidades de crédito y las empresas de inversión, y la Directiva (UE) 2019/879 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019 modifica la Directiva 2014/59/UE en relación con la capacidad de absorción de pérdidas y de recapitalización de las entidades de crédito y empresas de servicios de inversión, así como la Directiva 98/26/CE. Por otro lado, también se han introducido modificaciones en el marco normativo prudencial aplicable a las entidades de crédito, recogidas en el Reglamento (UE) 2019/876 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, modifica el Reglamento de Requisitos de Capital, y en la Directiva (UE) 2019/878 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, que modifica la Directiva de Requisitos de Capital.

De este modo, el anteproyecto tiene por objeto la transposición de la Directiva (UE) 2019/878, de 20 de mayo de 2019 por la que se modifica la Directiva 2013/36/UE en lo que respecta a los entes exentos, las sociedades financieras de cartera, las sociedades financieras mixtas de cartera, las

remuneraciones, las medidas y las facultades de supervisión y las medidas de conservación del capital.

Asimismo, procede a la transposición de la Directiva 2019/2034 del Parlamento Europeo y del Consejo, 27 de noviembre de 2019, relativa a la supervisión prudencial de las empresas de servicios de inversión, y por la que se modifican las Directivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE y 2014/65/UE, y que modifica el régimen prudencial de las empresas de servicios de inversión estableciendo un régimen más proporcionado y ajustado a los riesgos específicos de estas empresas, hasta entonces sometidas al mismo régimen prudencial que las entidades de crédito. De esta manera, a la mayoría de las empresas de servicios de inversión pasará a serles aplicable el régimen específico contemplado en la Directiva 2019/2034, 27 de noviembre de 2019, y en el Reglamento 2019/2033, 27 de noviembre de 2019. Sin embargo, un subconjunto de ellas – aquellas consideradas sistémicas– deberá, obligatoriamente, solicitar su autorización como entidades de crédito, de forma que les sea aplicable el régimen prudencial previsto en la Directiva y Reglamento de Requisitos de Capital.

Para dicha transposición, se introducen las modificaciones oportunas en el ordenamiento jurídico español, siendo las principales y de mayor calado las que se realizan en la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, teniendo en cuenta, tal y como señala el texto informado, que las normas europeas presentan un reducido margen de discrecionalidad para los Estados Miembros.

Dentro de dichas modificaciones destaca la ampliación de la definición de entidad de crédito para englobar también a las empresas de servicios de inversión sistémicas que quedan incluidas en el régimen de autorización como entidad de crédito, pasando a tener tal consideración; la atribución de una nueva competencia al Banco de España para aprobar determinadas sociedades financieras de cartera y sociedades financieras mixtas de cartera, regulándose el procedimiento de aprobación de manera similar al de autorización de entidades de crédito; la modificación de los requisitos de colchones de capital y las modificaciones en las potestades de supervisión del Banco de España, en materia de supervisión prudencial y en su colaboración con otros organismos, su cooperación con el resto de las autoridades competentes de la Unión europea y la posibilidad de compartir información con el Fondo Monetario Internacional y el Banco Mundial, el Banco de Pagos Internacionales y del Consejo de Estabilidad Financiera.

Asimismo, se introducen modificaciones en materia de protección del cliente, gobierno corporativo y política de remuneraciones y en el régimen sancionador.

I

Con carácter previo, es de destacar que las Directivas a cuya transposición se procede en el Anteproyecto de Ley objeto de informe son posteriores a la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE, por lo que las mismas ya han tenido en cuenta las previsiones del mismo, tal y como se aprecia en la Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativa a la supervisión prudencial de las empresas de servicios de inversión, y por la que se modifican las Directivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE y 2014/65/UE, cuyo Considerando 17 señala lo siguiente:

A efectos de la presente Directiva, el tratamiento de datos personales debe llevarse a cabo de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (9) y el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo (10). En particular, cuando la presente Directiva permita los intercambios de datos personales con terceros países, deben aplicarse las disposiciones pertinentes del capítulo V del Reglamento (UE) 2016/679 y capítulo V del Reglamento (UE) 2018/1725.

Asimismo, contiene referencias específicas a la protección de los datos personales de las personas físicas en su artículo 20, relativo a la publicación de las sanciones administrativas y de otras medidas administrativas, en el artículo 22, sobre notificación de incumplimientos

II

En lo que a la materia de protección de datos personales respecta, la norma a la que debe ajustarse el Anteproyecto de Ley sometido a consulta es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), plenamente aplicable desde el 25 de mayo de 2018 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El citado Reglamento extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.”

Quedan, en consecuencia, excluidas de su protección las personas jurídicas, pero su ámbito protector se extiende a las personas físicas que las representan, cuyos datos personales deben ser tratados con sujeción a lo previsto en dicho Reglamento.

III

Por otro lado, es preciso recordar, como ya se ha indicado en reiteradas ocasiones por esta Agencia que la reforma operada por el Reglamento general de protección de datos respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del “principio de consentimiento” el eje central del derecho a la protección de datos.

En efecto, si bien la Ley Orgánica y el Reglamento no difieren excesivamente en lo que atañe a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación sumamente relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales en relación con el consentimiento, que como regla general debía regir el tratamiento, en el texto del artículo 6.1 del Reglamento general de protección de datos el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento sin ostentar mayor o menor importancia que las restantes que en a norma se enumeran.

A mayor abundamiento, el propio Reglamento general de protección de datos pone de manifiesto que el consentimiento del afectado no debe constituir la base legal del tratamiento en determinados supuestos. Así, el considerando

42 señala en su última frase 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” y el considerando 43 añade que “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”.

De este modo, no procede recabar en ningún caso el consentimiento del afectado en los supuestos en los que el tratamiento se encuentre amparado por cualquiera de las causas incluidas en las letras b) a f) del artículo 6.1 del reglamento general de protección de datos; es decir cuando:

- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Además, en los supuestos en que el tratamiento se fundamente en las letras c) y e), los apartados 2 y 3 del artículo 6 del prevén que las normas que legitimen el mismo puedan establecer disposiciones específicas con el fin de garantizar el cumplimiento 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.

De acuerdo con lo anterior, y teniendo en cuenta que el derecho a la protección de datos personales es un derecho fundamental cuyo contenido, solo por ley, puede regularse (artículo 53 de la Constitución), el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales señala lo siguiente:

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.

Asimismo, y conforme a la doctrina del Tribunal Constitucional, la ley que incida en el derecho fundamental a la protección de datos deberá respetar el principio de proporcionalidad, para lo que es necesario constatar si cumple los tres requisitos o condiciones siguientes:

- a) si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad);
- b) 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);
- c) 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).

IV

El Anteproyecto sometido a informe recoge una serie de previsiones que implicarán la realización de distintos tratamientos de datos de carácter personal y que, en la mayoría de los casos y dado el carácter puntual de las modificaciones, supone aplicar a nuevos supuestos la normativa que ya estaba contenida en la Ley 10/2014. Dentro de dichos tratamientos interesa destacar, en primer lugar, los relativos al nuevo régimen de aprobación de las sociedades financieras de cartera y de las sociedades financieras mixtas de cartera, siendo requisito para su aprobación que “se cumplan los criterios y los requisitos establecidos en el artículo 7 en relación con los accionistas y socios y aquéllos establecidos en el artículo 24 y en el artículo 26, a excepción de lo dispuesto en su apartado 5 en relación con los miembros del consejo de administración u órgano equivalente” procediéndose a las oportunas modificaciones en los artículos 24.1 y 25.3.

En este punto, en relación con los requisitos de idoneidad y honorabilidad previstos en dichos preceptos, el criterio que tradicionalmente había venido manteniendo esta Agencia era la existencia de una habilitación legal, derivada de lo establecido en Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito la normativa de blanqueo de capitales y de ordenación de las entidades de crédito, para el tratamiento por parte de las entidades de crédito de los antecedentes penales de los miembros de su consejo de

administración y de sus directores generales o asimilados, y de los responsables de funciones de control interno y otros puestos clave en la entidad, tratamiento que, limitado a las personas y en los términos señalados en el Real Decreto 84/2015, sería conforme a lo previsto en la Ley Orgánica 15/1999.

No obstante, con posterioridad a la plena aplicación del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, esta Agencia viene insistiendo en la necesidad de que sea la propia norma legal que legitima el tratamiento la que establezca expresamente las garantías necesarias para que el mismo se estime conforme con la normativa de protección de datos de carácter personal, no siendo suficiente, a estos efectos, la mera remisión al desarrollo reglamentario.

En este sentido, si bien referido a las miembros del consejo de administración y de quienes ejerzan la dirección efectiva de las entidades gestoras de los fondos de pensiones, pero cuyos argumentos son plenamente trasladables al presente caso, en el informe 19/2020, reiterando lo que ya se había indicado en el informe 177/2018, se señalaba lo siguiente:

Especial referencia debe realizarse a la regulación de los requisitos de honorabilidad que se lleva a cabo en el nuevo artículo 78 bis del Reglamento de planes y fondos de pensiones, que introduce el proyecto.

En relación con esta cuestión, en el Informe 177/2018 señalábamos lo siguiente:

V

La siguiente cuestión que debe analizarse es la relativa a los requisitos de honorabilidad y aptitud de los miembros del consejo de administración y de quienes ejerzan la dirección efectiva de las entidades gestoras de los fondos de pensiones, aquellas que desempeñen funciones clave previstas en la ley y, en su caso, las personas o entidades a quienes se haya externalizado alguna de las funciones clave, a las que se refiere el artículo 28 de la Ley en la nueva redacción dada por el apartado doce del artículo 1 del Anteproyecto.

Conforme a lo previsto en el Reglamento (UE) 2016/679 tal tratamiento deberá encontrarse legitimado en lo previsto en su artículo 6 y ser respetuoso de los principios recogidos en el artículo 5 del mismo.

Pues bien, las obligaciones de verificación de los requisitos de honorabilidad e idoneidad a las que nos hemos referido aparecen expresamente recogidas en la Directiva (UE) 2016/2341, siendo fiel trasposición de las mismas, por lo que los tratamientos descritos se pueden considerar amparados por el mencionado artículo 6.1 c), al aparecer la obligación legal de tratamiento recogida en el Derecho de la Unión y pretender el proyecto su incorporación al derecho interno.

El considerando 45 del Reglamento señala que “Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.” En este sentido la Ley Orgánica de protección de datos de carácter personal y garantía de los derechos digitales, dispone en su artículo 8 respecto del tratamiento de datos amparado por la Ley lo siguiente:

“1. El tratamiento de datos de carácter personal sólo 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 de carácter personal sólo 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.”

En cuanto al tratamiento de los datos por parte de la Dirección General de Seguros y Fondos de Pensiones, el mismo encuentra su fundamento además, según lo señalado anteriormente, en lo previsto en el artículo 6.1 letra e): el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Sentado lo anterior, es preciso analizar los concretos datos que puedan ser objeto de tratamiento, que deberán cumplir con los principios establecidos en el artículo 5 del RGPD.

En este punto adquiere especial relevancia lo señalado en al apartado 4 del citado artículo 28, que se remite al desarrollo reglamentario para determinar “los supuestos en los que se entiende que se cumplen los requisitos de aptitud y honorabilidad de quienes llevan la dirección efectiva o desempeñan funciones clave...”.

Por consiguiente, el citado precepto, después de transcribir literalmente lo previsto en el apartado 1 del artículo 22 de la Directiva (UE) 2016/2341, definiendo el requisito de honorabilidad como “deberán ser personas íntegras y de buena reputación”, remite al desarrollo reglamentario la determinación de los supuestos concretos en los que se entiende que se cumplen dichos requisitos.

No obstante, hay que tener en cuenta que la acreditación de dicha honorabilidad puede implicar el tratamiento de datos relativos a condenas penales, posibilidad expresamente contemplada en el artículo 22 de la Directiva, cuyo apartado 3 dispone que “Cuando un Estado miembro de origen exija a las personas mencionadas en el apartado 1 una prueba de honorabilidad, una prueba de que no han sido declaradas anteriormente en quiebra o ambas, ese Estado miembro aceptará como justificación suficiente para los nacionales de otros Estados miembros la presentación de un extracto del registro de antecedentes penales del otro Estado miembro o, si no existe un registro de antecedentes penales en el otro Estado miembro, de un documento equivalente, que acredite que se cumplen esas exigencias, expedido por una autoridad judicial o administrativa competente bien del Estado miembro del que sea nacional la persona en cuestión o por el Estado miembro de origen”.

Asimismo, la acreditación de la misma podría requerir acreditar la ausencia de sanciones en el ámbito administrativo.

De este modo, la delimitación de la honorabilidad podría implicar el tratamiento de datos relacionados con la comisión de infracciones penales y administrativas.

A estos efectos, el artículo 10 del Reglamento General de Protección de Datos establece que “el tratamiento de datos

personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas”.

Esta norma se particulariza por el artículo 10.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que dispone los siguiente:

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

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

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

Por otro lado, respecto de los datos referidos a la comisión de infracciones administrativas, el artículo 27 de la misma ley, en correlación con lo establecido por el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno, establece lo siguiente:

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

De todo lo que se acaba de indicar se desprende que el tratamiento de datos relacionados con las condenas penales o administrativas sólo resulta posible en caso de que se encuentre amparada por una norma con rango de Ley, en que se establezcan, en su caso, las garantías adicionales para la salvaguarda de los derechos de los afectados.

Debe en este punto señalarse que el derecho español no establece la posibilidad de obtención de certificados parciales de antecedentes penales salvo en los supuestos en que así lo establece expresamente, como sucede en el caso de los que obrasen en el registro de delincuentes sexuales y que hubieran de ser apartados por quienes pretendieran desarrollar actividades que impliquen contacto con menores de edad, tal y como dispone la normativa de atención jurídica del menor. Ello supone que para el conocimiento de la existencia o no de los antecedentes relevantes para la determinación de la existencia de honorabilidad a los efectos establecidos en la Ley sería precisa la recogida de datos contenidos en certificados de antecedentes penales que pueden incluir antecedentes de delitos de distinta naturaleza que no afectasen a la mencionada honorabilidad. Lo mismo sucedería en cuanto al tratamiento de las infracciones administrativas, que podrían incluir otras que tampoco hubieran de ser tomadas en consideración para la apreciación de ese requisito.

Asimismo, debe tenerse en cuenta que, esta Agencia, ha puesto reiteradamente de manifiesto que la mera previsión de un determinado tratamiento o cesión de datos por un proyecto de disposición con rango de Ley no implica por sí sola la licitud de ese tratamiento o cesión desde el punto de vista de la normativa de protección de datos por cuanto deberá respetar el contenido esencial del derecho fundamental a la protección de datos de carácter personal, tal y como impone el artículo 53.1 de la Constitución. Así lo ha puesto de relieve el Tribunal Constitucional en la Sentencia 17/2013, de 31 de enero, en cuyo fundamento jurídico 4 se señala lo siguiente:

“En conclusión, tal como establece nuestra doctrina, es claro que la LOPD no permite la comunicación indiscriminada de datos personales entre Administraciones Públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento. Por tanto, la cesión de datos entre Administraciones Públicas sin consentimiento del afectado, cuando se cedan para el ejercicio de competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible, fuera de los supuestos expresamente previstos por la propia LOPD, si existe previsión legal expresa para ello [art. 11.2.a) en relación con el 6.1 LOPD] ya que, a tenor de lo dispuesto en el art. 53.1 CE, los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de ley. Reserva legal que, como es obvio, habrá de cumplir con los restantes requisitos derivados de nuestra doctrina- esencialmente, basarse en bienes de dimensión constitucional y respetar las exigencias del principio de proporcionalidad- para poder considerar conforme con la Constitución la circunstancia de que la norma legal en cuestión no contemple, por tanto, la necesidad de contar con el consentimiento del afectado para autorizar la cesión de datos.”

En particular, será preciso que el tratamiento y comunicación de los datos resulten conformes con el principio de limitación de la finalidad (“Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines”) y de minimización (“serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”) recogidos en el artículo 5 del RGPD.

En el presente caso, en cuanto a la información sobre antecedentes penales existe una norma de derecho de la Unión

que habilita el tratamiento de “un extracto del registro de antecedentes penales”.

De este modo, el derecho de la Unión establece una habilitación para el tratamiento de los datos relacionados con los antecedentes penales cuando los Estados Miembros exijan prueba de la honorabilidad, pero sin concretar los delitos que pueden tener incidencia en dicha honorabilidad.

A diferencia de lo referido a las infracciones penales, y lo previsto para el caso de quiebras (en el caso español, referido a la declaración de concurso e inhabilitación conforme a la Ley Concursal) la Directiva no incorpora referencia alguna a la comisión de infracciones administrativas para valorar la concurrencia de honorabilidad empresarial.

Esta Agencia Española de Protección de Datos ha tenido la oportunidad de analizar la cuestión a la que ahora se está haciendo referencia, incluso dentro del ámbito del sector asegurador que también resulta afectado por la norma objeto de informe, al informar diversos proyectos de disposiciones en las que se establecía la información necesaria para delimitar la concurrencia de honorabilidad. Así, cabe hacer referencia a los informes emitidos al Anteproyecto de Ley de distribución de seguros y reaseguros privados de 5 de diciembre de 2017, al Anteproyecto de Ley de Ordenación, Supervisión y Solvencia de las entidades aseguradoras y reaseguradoras, de fecha 13 de febrero de 2015, a su Reglamento de desarrollo, emitido en fecha 19 de noviembre de 2015 y al Proyecto de Orden por la que se aprueba la lista de información a remitir en supuestos de adquisición o incremento de participaciones significativas en entidades aseguradoras y reaseguradoras y por quienes pretendan desempeñar cargos de dirección efectiva o funciones que integran el sistema de gobierno en entidades aseguradoras, reaseguradoras y en los grupos de entidades aseguradoras y reaseguradoras, de fecha 16 de febrero de 2016.

En el informe de 13 de febrero de 2015 se valoraba la procedencia y conformidad con los principios de finalidad y proporcionalidad del tratamiento de estos datos, señalando lo siguiente:

“Obviamente, la concurrencia de los requisitos adecuados de idoneidad y honorabilidad en los directivos y consejeros de las entidades aseguradoras resulta esencial para garantizar su adecuado funcionamiento y evitar los posibles riesgos que de su

actividad, en caso de no reunirse los requisitos, pudieran derivarse en la actividad económica. Sin embargo, la legitimidad de este fin no puede fundamentar por sí sola la recolección de información “disponible” que exceda de la que resulte adecuada, pertinente y no excesiva en relación con el objetivo perseguido, teniendo en cuenta no sólo la normativa sectorial, sino el conjunto del ordenamiento jurídico.

De este modo, como se ha comprobado, la “información disponible” referida a condenas penales debería quedar limitada a la derivada de los antecedentes penales en vigor y, particularmente, de la situación de inhabilitación del candidato al puesto directivo o de administración. Del mismo modo, en cuanto a las infracciones administrativas, sería preciso el establecimiento de límites similares, tanto en lo referente a la normativa a la que debe referirse la infracción, no acumulándose datos irrelevantes o que no guarden en ninguna medida relación con el puesto que se pretende desempeñar ni aquéllos respecto de los que el tiempo transcurrido determine su irrelevancia para la toma de decisiones.”

De lo que acaba de transcribirse, trasladado al supuesto ahora estudiado, se desprende que, efectivamente, el conocimiento del requisito de honorabilidad por parte de quienes intervienen en la actividad de gestión de los fondos de pensiones constituye una finalidad legítima que garantiza el adecuado funcionamiento y transparencia en el mercado de planes de pensiones.

No obstante, con el fin de habilitar el tratamiento de los datos relativos a las condenas penales y a las infracciones administrativas, se considera necesario que así se establezca expresamente en el Anteproyecto de ley, delimitándose, conforme al principio de minimización, los supuestos concretos de infracciones penales y administrativas que se consideran relevantes a efectos de valorar la honorabilidad.

En todo caso, el tratamiento de los datos, tanto relativos a la comisión de infracciones penales como de ilícitos administrativos únicamente debería llevarse a cabo con la finalidad de evaluar la honorabilidad exigida por los preceptos del Anteproyecto a los que se ha hecho exhaustiva referencia en un lugar anterior de este informe y para su comunicación a la Dirección General de Seguros y Fondos de Pensiones.

A título de ejemplo, entre las normas más recientemente informadas por esta Agencia, puede citarse el Anteproyecto de

Ley de distribución de seguros y reaseguros privados, cuyo artículo 2.19 definía la «Honorabilidad comercial y profesional» como la “cualidad aplicable a aquellas personas que hayan venido observando una trayectoria personal de respeto a las leyes mercantiles u otras que regulen la actividad económica y la vida de los negocios, así como a las buenas prácticas comerciales, financieras y de seguros. Dicha condición será aplicable a aquellas personas que no tengan antecedentes penales por haber cometido infracciones penales relativas al ejercicio de actividades financieras, y que no hayan sido sancionadas en el ámbito administrativo en materia aseguradora, bancaria, de mercado de valores, Hacienda Pública, Seguridad Social, defensa de la competencia, movimiento de capitales, transacciones económicas con el exterior, blanqueo de capitales y financiación del terrorismo y protección de consumidores y usuarios por la comisión de infracciones tipificadas como muy graves o graves. La inhabilitación para el ejercicio de cargos públicos o de administración y dirección de entidades financieras, así como la declarada conforme a la Ley 22/2003, de 9 de julio, Concursal, mientras no haya concluido el periodo de inhabilitación fijado, o el estado de quebrado o concursado no rehabilitado en el caso de procedimientos concursales anteriores a la entrada en vigor de la referida ley, se considerarán circunstancias que no permiten cumplir el requisito de honorabilidad”.

VI

A los efectos anteriores, y para recalcar la insuficiencia de la remisión a la normativa reglamentaria para determinar los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, procede traer a colación la doctrina sentada por el Tribunal Constitucional en su reciente sentencia de 22 de mayo de 2019, en la que se comienza realizando una síntesis de la doctrina recogida en otras sentencias anteriores:

“6. A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental. En este fundamento jurídico precisaremos la naturaleza y el alcance de este específico requisito constitucional.

a) La necesidad de establecer las garantías adecuadas para procurar el respeto del contenido esencial del derecho fundamental a la protección de datos personales fue señalada específicamente en el FJ 10 de la STC 292/2000, que ha sido correctamente invocado por el Defensor del Pueblo. Del mencionado fundamento jurídico se extraen las siguientes conclusiones:

- La previsión legal y la legitimidad del fin perseguido son requisitos necesarios pero no suficientes para fundamentar la validez constitucional de una regulación del tratamiento de datos personales, pues para ello se requieren también “garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático”.

- Esas garantías son necesarias “para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos” y “para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos”.

- La mera inexistencia de “garantías adecuadas” o de las “mínimas exigibles a la Ley” constituye de por sí una injerencia en el derecho fundamental, de gravedad similar a la que causarían intromisiones directas en su contenido nuclear.

- La exigencia de “garantías adecuadas” se fundamenta, por tanto, en el respeto del contenido esencial del derecho fundamental.

Asimismo, del examen conjunto de los FFJJ 7 y 10 de la STC 292/2000 se deduce que las “garantías adecuadas” o “garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula” deben diferenciarse también del “haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal”, que, como se indicó antes, son aquellas que otorgan al titular del derecho fundamental “un poder de disposición y de control sobre los datos personales”.

b) Esta doctrina sobre las garantías adecuadas es también la que sigue la jurisprudencia del Tribunal de Justicia de la Unión Europea. En la Sentencia de la Gran Sala de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd, apartado 54, el Tribunal de Justicia señaló lo siguiente: “la normativa de la Unión de que se trate debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto

de tales datos (véanse, por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias TEDH, Liberty y otros c. Reino Unido de 1 de julio de 2008, nº 58243/00, §§ 62 y 63; Rotaru c. Rumanía, antes citada, §§ 57 a 59, y S y Marper c. Reino Unido, antes citada, §§ 99).”

En la citada sentencia, la constatación de la carencia de, por un lado, reglas claras y precisas que regulasen el alcance de la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la Carta de Derechos Fundamentales y de, por otro lado, garantías suficientes que permitieran una protección eficaz de los datos conservados fundamentó la declaración de invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

c) La necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad.”

Para añadir, resolviendo la cuestión objeto de debate, que:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. 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. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales”.

Por consiguiente, correspondiendo a los Estados Miembros definir los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, en la medida en que afectan al derecho fundamental a la protección de datos y conforme a la doctrina constitucional citada, dicha definición deberá contenerse en el propio Anteproyecto al menos en sus elementos esenciales”.

Dicha observación fue recogida en la modificación realizada por el Real Decreto Ley 3/2020, en la que ya se identificaron, al regular la información a facilitar en el caso de personas no residentes en España, concretos tipos delictivos, procediendo el nuevo artículo 78 bis a regular más detalladamente los supuestos en los que se entiende que se cumplen los requisitos de honorabilidad, identificando las conductas y tipos delictivos que deben ser objeto de valoración, dando cumplimiento, de este modo, al principio de minimización de datos. Asimismo, y de acuerdo con el principio de limitación de la finalidad, se señala expresamente que “El tratamiento de los datos que las entidades lleven a cabo en el marco de lo dispuesto en este precepto deberá limitarse a la exclusiva finalidad de suministro de la información a la Dirección General de Seguros y Fondos de Pensiones, quedando expresamente limitado el número de personas de la entidad que dentro de su organización pueda tener acceso a dichos datos”.

Por consiguiente, aun cuando no es propiamente objeto de modificación en virtud de la transposición directa de la Directiva, teniendo en cuenta que la apreciación del cumplimiento de los requisitos de idoneidad y honorabilidad puede implicar el tratamiento de datos relativos a condenas penales y sanciones administrativas, y al objeto de adecuar la regulación contenida en la Ley 10/2014 a los requisitos normativos y jurisprudenciales señalados, esta Agencia considera necesario que se modifique el artículo 24 de la Ley 10/2014, de manera que se 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, incorporando en el texto legal las previsiones contenidas en el artículo 30.2.b) del Real Decreto Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. De este modo, dichos tratamientos se encontrarían amparados por lo previsto 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), de acuerdo con lo previsto en el artículo 10 del RGPD y en los artículos 10 y 27 de la LOPDGDD.

V

En segundo lugar, dentro de las novedades introducidas por el Anteproyecto y por lo que se refiere a las competencias de esta Agencia, interesa destacar las que afectan a la actuación del Banco de España como autoridad supervisora de las entidades de crédito, reforzándose sus facultades de supervisión y la coordinación con las autoridades supervisoras competentes de otros Estados miembros así como de otros órganos competentes en otras áreas como la prevención de blanqueo de capitales y financiación del terrorismo.

A este respecto, se modifica el artículo 4.2 de la Ley 10/2014, introduciendo una letra a) bis que incluye entre sus competencias la de aprobar las sociedades financieras de cartera y las sociedades financieras mixtas de cartera, regulando su régimen de aprobación en el nuevo Capítulo II bis, que incluye el deber de información regulado en el artículo 15 quinquies, debiendo suministrarse la información que se determine reglamentariamente, información que el Banco de España compartirá con la autoridad competente del Estado miembro en que esté establecida la sociedad, así como el ejercicio de las medidas de supervisión del artículo 15 sexies.

Asimismo, se modifica la regulación del Registro de altos cargos contemplado en el artículo 27 de la Ley 10/2014, creando un nuevo registro, añadiendo un apartado 3 conforme al cual “Adicionalmente, el Banco de España se encargará de la inscripción y gestión del Registro de miembros del consejo de administración u órgano equivalente de las sociedades financieras de cartera y de las sociedades financieras mixtas de cartera aprobadas de conformidad con lo dispuesto en el artículo 15 bis y sujetas a supervisión en base consolidada por parte del Banco de España”.

En el artículo 29, se incluye la obligación de las entidades y los grupos consolidables de entidades de crédito documentar de manera adecuada y poner a disposición y, en su caso, remitir al Banco de España la información relativa a los préstamos otorgados a miembros del consejo de administración y a sus partes vinculadas en la forma en que éste lo determine mediante circular, incluyendo en el concepto de parte vinculada al cónyuge, pareja de hecho y descendientes o ascendiente en primer grado por consanguinidad o adopción.

Se introduce el artículo 60 bis, relativo a la Colaboración del Banco de España con otras autoridades, entre las que se incluyen el coordinador determinado de conformidad con el artículo 5 de la Ley 5/2005, de 22 de abril, de supervisión de los conglomerados financieros y por la que se modifican otras leyes del sector financiero, la unidad de inteligencia financiera, y las autoridades en las que recaiga la función pública de supervisión de la normativa de prevención del blanqueo de capitales y financiación del terrorismo cooperarán estrechamente entre sí y con las autoridades que desempeñen las

funciones equivalentes en otros Estados Miembros, en el marco de sus respectivas competencias; el nuevo apartado 1 bis, del artículo 61 se refiere expresamente a la colaboración estrecha con todas aquellas autoridades competentes de la Unión Europea que sean responsables de la supervisión de las entidades de crédito, las empresas de servicios de inversión, o las sucursales establecidas en la Unión Europea por entidades de crédito o empresas de servicios de inversión con sede en un tercer país, que formen parte de un mismo grupo de un tercer país; el artículo 62.1.e) la autoridad competente del Estado miembro en que esté establecida una sociedad financiera de cartera o una sociedad financiera mixta de cartera, o cuando estando establecida la sociedad financiera de cartera o sociedad financiera mixta de cartera en España no le corresponda al Banco de España la supervisión en base consolidada del grupo.

Y, consecuentemente, se modifican las excepciones previstas a la obligación de secreto al objeto de facilitar el intercambio de información del Banco de España con las unidades de inteligencia financiera y con las autoridades competentes u organismos responsables de la aplicación de las normas relativas a la separación estructural dentro de los grupos bancarios.

El artículo 6.1 e) del reglamento general de protección de datos considera lícito el tratamiento “necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”.

Por ello, los tratamientos de datos vinculados al ejercicio de las potestades atribuidos al Banco de España por el Anteproyecto, en su condición de autoridad de supervisión se encontrarían amparados en lo dispuesto en el citado artículo 6.1 e). Del mismo modo, encontrarían amparo en dicho precepto las comunicaciones derivadas del deber de colaboración previsto en el artículo 60 bis y el Registro de miembros del consejo de administración u órgano equivalente de las sociedades financieras de cartera y de las sociedades financieras mixtas de cartera aprobadas de conformidad con lo dispuesto en el artículo 15 bis y sujetas a supervisión en base consolidada por parte del Banco de España al que se refiere el artículo 27.3.

A este respecto, hay que tener en cuenta que el artículo 50 de la Ley 10/2014, al regular la función supervisora del Banco de España, continúa refiriéndose a la derogada Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, por lo que sería conveniente aprovechar la presente modificación para adecuar la misma a la normativa vigente, al objeto de indicar que el acceso a las informaciones y datos requeridos por el Banco de España se encuentra amparado por el artículo 6.1.c) del RGPD, y que los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de

abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en el resto de la normativa sobre protección de datos personales.

VI

Por otro lado, el artículo 82 bis se refiere a la transmisión de información a organismos internacionales:

«Artículo 82 bis. Transmisión de información a organismos internacionales.

1. No obstante lo dispuesto en el artículo anterior, el Banco de España podrá transmitir o compartir determinada información, siempre que se cumplan los requisitos previstos en este artículo, con los siguientes organismos internacionales:

a) El Fondo Monetario Internacional y el Banco Mundial a efectos del Programa de Evaluación del Sector Financiero.

b) El Banco de Pagos Internacionales, a los efectos de los estudios de impacto cuantitativo.

c) El Consejo de Estabilidad Financiera, a efectos de su función de supervisión.

2. La información de carácter confidencial solo podrá compartirse a solicitud expresa del organismo pertinente y siempre que se reúnan las siguientes condiciones:

a) Que la solicitud esté debidamente justificada por razón de las funciones concretas que desempeña el organismo solicitante de conformidad con su mandato estatutario;

b) Que la solicitud describa con la precisión suficiente la naturaleza, el alcance y el formato de la información solicitada, así como la forma de facilitarla o transmitirla;

c) Que la información solicitada sea estrictamente necesaria para el desempeño de funciones concretas del organismo solicitante y que no exceda de las competencias estatutarias otorgadas a dicho organismo;

d) Que la información se transmita o facilite exclusivamente a las personas que participan directamente en el desempeño de la función de que se trate; y,

e) Que las personas que tengan acceso a la información estén sujetas a requisitos de secreto profesional al menos equivalentes a los previstos en el artículo 82.

Cuando la solicitud proceda de alguno de los organismos internacionales mencionados en el apartado 1, el Banco de España sólo podrá transmitir información agregada o anonimizada y únicamente podrá compartir otra información en sus dependencias.

Asimismo, cuando facilitar la información implique el tratamiento de datos personales, todo tratamiento de datos personales por parte del organismo solicitante cumplirá los requisitos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.»

En relación con la transmisión de información prevista en el citado precepto, en la medida en la que la misma pudiera suponer transferencias de datos personales a terceros países, será de aplicación lo dispuesto en el Título V del Reglamento general de protección de datos que, como regla general, establece en su artículo 44 que “Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado”.

Pues bien, el régimen regulador de las transferencias internacionales de datos en el Reglamento establece una serie de reglas que deberán ser adecuadamente cumplidas para que proceda la transmisión a la que se refiere el Anteproyecto.

En primer lugar, será posible la colaboración en caso de que sea aplicable el artículo 45.1 del Reglamento, a cuyo tenor “Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica”.

Si el Estado de destino no tuviese el citado nivel adecuado, seguiría siendo posible la transferencia si se diera cumplimiento a lo dispuesto en el artículo 46.1, cuyo apartado 1 dispone que “A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas”.

En particular, en lo que afecta a la colaboración entre organismos con potestades de derecho público, el artículo 46.2 a) del Reglamento establece que “Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control,

por (...) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.

De no existir dicho instrumento, el artículo 46.3 b) aún permite la transferencia, si bien en ese caso sometida a autorización de la autoridad de control. Así se indica que “Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante (...) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados”.

En este mismo sentido, el artículo 42.1 b) de la LOPDGDD dispone que “Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse (...) cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento”.

Por último, deberán tenerse en consideración los criterios establecidos por el Tribunal de Justicia de la Unión Europea en su sentencia de 16 julio 2020, asunto C-311/18, Caso Data Protection Commissioner contra Facebook Ireland Ltd y Otros (más conocida como SCHREMS II), que ha declarado inválida la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU.

Estas disposiciones deberán ser respetadas en los supuestos establecidos en el artículo 82.bis, circunstancia que, como se ha señalado, ha sido expresamente prevista en el Considerando 17 de la Directiva (UE) 2019/2034:

A efectos de la presente Directiva, el tratamiento de datos personales debe llevarse a cabo de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (9) y el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo (10). En particular, cuando la presente Directiva permita los intercambios de datos personales con terceros países,

deben aplicarse las disposiciones pertinentes del capítulo V del Reglamento (UE) 2016/679 y capítulo V del Reglamento (UE) 2018/1725.

Asimismo, el artículo 58 bis de la Directiva 2013/36/UE, introducido por la Directiva (UE) 2019/878 y a cuya transposición se procede en este artículo 82 bis, ha previsto expresamente, como cautela, que

“3. Cuando la solicitud proceda de alguno de los organismos enumerados en el apartado 1, las autoridades competentes únicamente podrán transmitir información agregada o anonimizada y únicamente podrán divulgar otra información en las dependencias de la autoridad competente.

4. Cuando la divulgación de información implique el tratamiento de datos personales, todo tratamiento de datos personales por parte del organismo solicitante cumplirá los requisitos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo”

Ambos apartados, que han sido trasladados literalmente al artículo 82 bis, implican dos cautelas respecto al tratamiento de datos personales:

En primer lugar, que la regla general es que la transmisión de la información solo procederá respecto de la información agregada o anonimizada.

En este punto, debe tenerse en cuenta que, tratándose de datos anónimos, no será de aplicación el RGPD, tal y como señala en su Considerando 26:

Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

En segundo lugar, que la comunicación de datos personales, que solo procederá “en las dependencias de la autoridad competente”, según el apartado anterior, requerirá que “todo tratamiento de datos personales por parte del organismo solicitante cumplirá los requisitos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo”. En este punto, debe tenerse en cuenta que previamente se han establecido otra serie de cautelas para el acceso a la información que inciden igualmente en la protección de datos personales conforme al RGPD, como son las relativas a que la información solicitada sea estrictamente necesaria para el desempeño de funciones concretas del organismo solicitante y que no exceda de las competencias estatutarias otorgadas a dicho organismo (principios de minimización y limitación de la finalidad) o la necesidad de que las personas que tengan acceso a la información estén sujetas a requisitos de secreto profesional.

Partiendo de lo anterior, en una interpretación amplia del último apartado, una vez comunicados los datos al organismo solicitante, el mismo queda sujeto a las previsiones del RGPD, lo que implicaría la posibilidad de realizar transferencias internacionales de datos si se ajusta a su Capítulo V. Sin embargo, a juicio de esta Agencia, una interpretación conjunta de los dos últimos apartados del artículo 82.bis, implicaría que no pudieran transferirse datos personales a un tercer país sin que previamente se haya procedido a su anonimización.

Por otro lado, en el supuesto de colaboración con las autoridades de países que no sean Estados miembros de la Unión Europea, como es el caso al que se refiere el artículo 82.3.h) de la Ley 10/2014, que exceptúa de la obligación de secreto “Las informaciones que el Banco de España tenga que facilitar, para el cumplimiento de sus funciones, a los organismos o autoridades de otros países en los que recaiga la función pública de supervisión de las entidades de crédito, de las empresas de servicios de inversión, de las empresas de seguros, de otras instituciones financieras y de los mercados financieros, o la gestión de los sistemas de garantía de depósitos o indemnización de los inversores de las entidades de crédito, de mantener la estabilidad del sistema financiero en los Estados miembros mediante la utilización de normas macroprudenciales, de actividades de reorganización encaminadas a mantener la estabilidad del sistema financiero, o de supervisión de los sistemas contractuales o institucionales de protección, siempre que exista reciprocidad, y que los organismos y autoridades estén sometidos a secreto profesional en condiciones que, como mínimo, sean equiparables a las establecidas por las leyes españolas”, en el supuesto de que dichas informaciones contengan datos de carácter personal deberá cumplirse, además, con lo previsto en el Capítulo V del RGPD.

Por ello, esta Agencia considera necesario que se modifique el citado artículo 82 incluyendo un nuevo apartado en el que se indique que para facilitar información que contenga datos personales a terceros países, será en todo caso de aplicación el régimen de transferencias internacionales de datos previsto en el Capítulo V del Reglamento (UE) 2016/679.

VII

Por último, hay que hacer referencia a las modificaciones que se realizan el artículo 5, relativo a la protección del cliente de entidades de crédito, al objeto de introducir la obligación de las entidades de crédito de actuar “de manera honesta, imparcial, transparente y profesional, con respeto a los derechos y los intereses de la clientela”. Como señala la Exposición de Motivos, “en el ámbito bancario, existen diversas disposiciones de rango reglamentario que exigen un deber de diligencia en la ejecución de órdenes y en la corrección de errores, así como, en materia de préstamo responsable, la obligación de actuar honesta, imparcial y profesionalmente, atendiendo a la situación personal y financiera y a las preferencias y objetivos de los clientes. Sin embargo, dicho deber general no se recogía por la ley de forma similar a lo que sucede en el ámbito de los productos y servicios de inversión”.

A este respecto, hay que tener en cuenta que para el cumplimiento de dicho deber, así como para otras funciones que se desarrollan por las entidades de crédito, debe conocerse la situación financiera y los intereses de la clientela, lo que implica tratamientos de datos, incluido el perfilado de los clientes, que han de realizarse con estricta sujeción a lo previsto en la normativa de protección de datos personales, asegurándose dichas entidades de contar con una base jurídica adecuada que legitime el tratamiento, informar debidamente a los afectados y cumplir con el resto de dicha normativa.

Aunque la aplicación de la normativa de protección de datos deriva directamente del RGPD, siendo la autoridad competente para velar por su cumplimiento esta Agencia, no formando parte de la normativa de ordenación y disciplina cuya supervisión corresponde al Banco de España, de acuerdo con el artículo 5.5. de la Ley 10/2014, dada la trascendencia que su cumplimiento tiene para garantizar el derecho fundamental a la protección de datos personales, se sugiere la introducción de una disposición adicional en la que se recuerde que los tratamientos de datos de carácter personal de las personas físicas por parte de las entidades de crédito se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en el resto de la normativa sobre protección de datos personales.