

054/2025**I**

El anteproyecto de ley tiene como finalidad el desarrollo del régimen sancionador aplicable a los productos paneuropeos de pensiones individuales, previstos en el Reglamento (UE) 2019/1238 del Parlamento Europeo y del Consejo, de 20 de junio de 2019. El Reglamento estableció un marco armonizado para la creación de un producto de ahorro para la jubilación de carácter voluntario, transparente y con vocación transfronteriza en el ámbito de la Unión Europea, *dejando en manos de los Estados miembros el desarrollo* de los mecanismos sancionadores y de supervisión. Precisamente en este ámbito se inscribe el texto que se informa, que busca dotar al ordenamiento español de una norma que garantice la eficacia del Reglamento, asegurando la protección de los ahorradores y el correcto funcionamiento del mercado interior de pensiones.

Así, el Reglamento (UE) 2019/1238, de 20 de junio de 2019, indica en su artículo **67.1** que, sin perjuicio de las facultades de supervisión de las autoridades competentes y del derecho de los Estados miembros a establecer e imponer sanciones penales, *los Estados miembros adoptarán las normas sobre las sanciones administrativas y otras medidas adecuadas aplicables a las infracciones contenidas en el propio Reglamento, y adoptarán todas las medidas necesarias para garantizar su aplicación*. Indica asimismo que *las sanciones administrativas y las otras medidas establecidas deberán ser efectivas, proporcionadas y disuasorias*.

Si bien el Reglamento es de directa aplicación, para dar cumplimiento al mandato establecido resulta necesaria la tramitación del anteproyecto de ley que se informa, en orden a la concreción del marco jurídico de este régimen sancionador, desarrollando aspectos tales como los sujetos infractores, la tipicidad de las infracciones y sanciones concretas, sus plazos de prescripción y su sistema de graduación.

El anteproyecto se centra en varios ejes esenciales. En primer lugar, designa a la *Dirección General de Seguros y Fondos de Pensiones* como autoridad nacional competente para la supervisión de los promotores y distribuidores de los *Pan-European Personal Pension Product* —PEPP—. En segundo lugar, tipifica las infracciones que pueden cometerse en la promoción, gestión, vigilancia y distribución de estos productos, clasificándolas en muy graves, graves y leves, y establece el correspondiente catálogo sancionador con criterios de graduación y prescripción. En tercer lugar, regula el procedimiento sancionador, las competencias de resolución y la publicación de las sanciones, incluyendo la obligación de comunicar a la

Autoridad Europea de Seguros y Pensiones de Jubilación las medidas adoptadas en España.

En cuanto a las principales novedades respecto a la normativa actualmente vigente, conviene precisar que hasta ahora no existía en el derecho interno un régimen sancionador específico para los PEPP. En este contexto, el Reglamento (UE), de 20 de junio de 2019, establece —en el artículo 67.1—, un mandato de intervención de los Estados miembros, que en el caso que nos ocupa, y al tratarse de **régimen sancionador**, siguiendo los mandatos del artículo 25 de la Constitución Española y artículo 25 de la Ley 40/2015, de 1 de octubre, requiere que el ejercicio de la potestad sancionadora de las Administraciones Públicas esté reconocido por una norma con rango de ley (principio de legalidad en materia sancionadora). En consecuencia, la aprobación de la propuesta mediante una norma con rango de ley se justifica por su objeto, al proponerse la regulación de un régimen sancionador.

En resumen, el anteproyecto viene a llenar un vacío regulatorio, estableciendo de forma detallada las conductas sancionables, las sanciones posibles y las reglas de procedimiento, lo que aporta mayor seguridad jurídica tanto para los operadores como para los supervisores.

Otra novedad relevante es la *homogeneización* de la materia sancionadora. El texto prevé sanciones económicas de considerable cuantía, alineadas con los estándares europeos, y añade medidas adicionales como la cancelación de la inscripción de un producto, la prohibición de su comercialización o la inhabilitación de directivos responsables. Se amplía, además, **la responsabilidad a las personas físicas** que ejerzan funciones de dirección o administración efectiva en las entidades implicadas, lo que refuerza la diligencia exigible a los órganos de gobierno de las gestoras y distribuidores.

Asimismo, con el fin de conseguir un efecto disuasorio en los potenciales infractores, el anteproyecto refuerza la transparencia al obligar a **la publicación de las sanciones** en el portal de la Dirección General (dando cobertura a dicha publicación), salvo excepciones justificadas por motivos de estabilidad financiera o protección de datos.

En suma, esta norma pretende consolidar el marco de supervisión nacional en coherencia con el Reglamento (UE) 2019/1238, de 20 de junio de 2019, garantizando una adecuada protección de los consumidores e impulsando la confianza en los productos paneuropeos de pensiones. Con ello se busca no solo dar cumplimiento a un mandato europeo, sino también favorecer el desarrollo de un mercado más transparente, competitivo y robusto de productos de previsión complementaria.

II

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos —RGPD—), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales —LOPDGDD— conforman el marco jurídico de referencia en España que afecta a la protección de datos de carácter personal. En estas normas se regulan los principios y fundamentos a los que deben ajustarse la recogida y tratamiento de los datos personales por cualquier persona pública o privada que lleve a cabo tratamiento de datos de carácter personal en el ejercicio de su actividad.

Entre otras definiciones, el artículo 4 del RGPD se refiere a «datos personales» 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. Y «tratamiento» como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Por su parte, el apartado 1 del artículo 2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que: *“Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.”*

Pues bien, del texto normativo informado se desprende que, conforme a lo previsto en su articulado, **se procederá al tratamiento de datos de carácter personal.**

En particular, respecto de *i)* la tramitación de expedientes sancionadores que afecten a personas físicas y el eventual uso de datos identificativos de los infractores, *ii)* la publicación de las sanciones impuestas, y *iii)* la comunicación de información con datos personales a autoridades

europas, se realizarán operaciones de tratamiento que exigen un análisis de necesidad conforme a los principios y obligaciones establecidos por la normativa de protección de datos.

En este contexto, sin perjuicio de lo dispuesto en el artículo 11 del anteproyecto relativo a la publicación de sanciones, así como de las excepciones que, en su caso, justifiquen la no divulgación de determinados datos personales, se aprecia en la norma la **ausencia de referencias expresas al marco jurídico** aplicable en materia de protección de datos personales. Tal omisión resulta relevante, pues tanto el ámbito material objeto de regulación como el contenido específico del mencionado artículo 11 justificarían plenamente la inclusión de una mención directa a dicha normativa.

En consecuencia, se considera conveniente introducir una referencia explícita al régimen de protección de datos, que deje constancia del sometimiento de los tratamientos previstos tanto al Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos, como a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. A tal efecto, se propone incorporar un nuevo artículo o una disposición adicional con un contenido análogo al siguiente:

“La totalidad de las actuaciones reguladas en esta ley y en sus normas de desarrollo se llevarán a cabo con el debido respeto a lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; 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 (Reglamento General de Protección de Datos); así como en el resto de normativa aplicable en la materia.”

III

La normativa de protección de datos contempla diferentes supuestos que pueden dar lugar al tratamiento de datos de carácter personal. En concreto, de acuerdo con el **artículo 6** –“Licitud del tratamiento”-, del **RGPD**, entre otros, dicho tratamiento es lícito y legítimo cuando:

“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

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; (La negrita es nuestra)

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.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.”

Conforme al articulado de la norma que se informa las competencias se ejercerán por el órgano que las tenga conferidas en virtud de lo dispuesto en la ley. En el presente supuesto, dichas competencias corresponderán a la **Dirección General de Seguros y Fondos de pensiones** (artículo 2.1), sin perjuicio de que el Banco de España, la Comisión Nacional del Mercado de Valores y los demás entes u órganos encargados de la supervisión de la solvencia y la comercialización de las entidades financieras, colaboren con dicha Dirección general en la supervisión de los productos paneuropeos de pensiones individuales *cuando les sea requerido*.

Se tratarán así los datos por parte del responsable del tratamiento, dentro del ámbito de su **gestión pública**, siendo esta la realizada por la Dirección General de Seguros y Fondos de pensiones. Esto es, el tratamiento de los datos personales será realizado por el **responsable** en el marco de sus funciones, que en este caso corresponden a la citada Dirección General.

Así, sin perjuicio de la aplicación de la base jurídica prevista en la **letra c) del artículo 6.1** del Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), resultará igualmente de aplicación la establecida en la **letra e)** del mismo precepto, en tanto que el tratamiento se fundamenta en el **interés público** reconocido —y expresamente señalado en la Memoria del Análisis de

Impacto Normativo— **relativo a** la protección de los ahorradores y a la seguridad jurídica de los distribuidores y promotores. Dicho interés se manifiesta, además, en la necesidad de favorecer la creación de un mercado europeo de pensiones individuales caracterizado por su simplicidad, eficiencia y competitividad.

En todos estos casos, las citadas previsiones competenciales, establecidas en una norma con rango de ley formal, responden a las exigencias derivadas del artículo 8 de la LOPDGDD, cuando dispone que:

“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. (La negrita es nuestra)

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**.” (La negrita es nuestra)

En consecuencia, **la base de legitimación de los tratamientos derivados del anteproyecto de ley que se analiza se encuentra claramente incardinada en las previsiones de las letras c) y e) del artículo 6.1 del RGPD.**

IV

Aunque el objeto del anteproyecto no se centra en el tratamiento de datos personales, sus disposiciones inciden de forma directa en esta materia. Tal y como se ha adelantado, dicha incidencia resulta particularmente importante en lo relativo a la publicación de sanciones, a la transmisión de información a autoridades europeas y al eventual tratamiento de datos identificativos de infractores y responsables. Estos aspectos deben analizarse a la luz del Reglamento General de Protección de Datos y de la Ley Orgánica

3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

El artículo 11 del anteproyecto establece que las sanciones impuestas **serán publicadas** en el portal de la Dirección General de Seguros y Fondos de Pensiones, incluyendo la calificación de la infracción, su naturaleza y la identidad de los sujetos infractores. Ello implica necesariamente el tratamiento de datos de carácter personal cuando los infractores sean personas físicas, o bien la difusión de datos que permitan su identificación.

Aquí resultan esenciales los principios relativos al tratamiento del artículo 5 del RGPD. En concreto, solo se podrán publicar aquellos datos necesarios para garantizar la finalidad de transparencia y disuasión, evitando excesos o publicaciones desproporcionadas. De hecho, el propio anteproyecto prevé la posibilidad de anonimizar la información cuando la publicación de la identidad del infractor pueda resultar desproporcionada o poner en riesgo una investigación en curso, lo que se alinea con el principio de minimización de datos.

Sin embargo, a la vista de la regulación que se analiza, no se vislumbran cuáles serán los elementos valorativos que deberá tener en cuenta el responsable del tratamiento al realizar su juicio de proporcionalidad.

La protección de datos no es un derecho absoluto y puede limitarse siempre dentro de un justo equilibrio. Un tratamiento desarrollado en una norma debe respetar el principio de proporcionalidad lo que restringe a las autoridades en el ejercicio de sus facultades al exigir un equilibrio entre los medios utilizados y el objetivo previsto (o el resultado alcanzado).

En este sentido, la STJUE de 16 de julio de 2020, Schrems 2 (apartado 176), señala que:

“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.”

En consecuencia, concurren dos elementos esenciales que refuerzan la necesidad de realizar una **Evaluación de Impacto relativa a la protección de datos personales** —EIPD— por parte del responsable del tratamiento, y de que dicha exigencia se incorpore expresamente en la versión definitiva de la norma objeto de informe. *De un lado*, debe tenerse en cuenta que, por regla general, la **ley formal** constituye el instrumento habilitante suficiente para autorizar la publicación o difusión de determinados datos personales —especialmente aquellos de naturaleza infractora o sancionadora—. *De otro*, resulta imprescindible atender al **principio de proporcionalidad**, tal como ha sido interpretado por la jurisprudencia, que exige contemplar **excepciones** justificadas en la publicación de tales datos cuando puedan derivarse efectos desproporcionados para los derechos fundamentales de las personas afectadas.

La evaluación de la proporcionalidad requiere una valoración previa y positiva de la necesidad del tratamiento, de la cual se nutre directamente. En este sentido, partiendo del resultado de analizar la estricta necesidad del tratamiento y el grado de injerencia que comporta, debe realizarse una ponderación equilibrada entre las ventajas y los riesgos —o, en términos más amplios, entre los beneficios sociales y los costes individuales— que se derivan de la medida. Ello implica que la proporcionalidad ha de evaluarse de manera concreta y caso por caso, considerando las salvaguardias que acompañen la medida adoptada y que resulten adecuadas para mitigar los riesgos sobre los derechos y libertades fundamentales de las personas afectadas (de conformidad con las *Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo* de esta Agencia Española de Protección de Datos).

En este punto, conviene destacar que el propio **artículo 11 del anteproyecto** ya alude a la necesidad de una **evaluación previa**, al prever que la autoridad competente pueda valorar la proporcionalidad de la publicación de datos personales en supuestos sancionadores. Dicha referencia puede entenderse —en el contexto de la norma y de su finalidad— como una **evaluación previa en materia de protección de datos personales**, orientada a ponderar los riesgos para los derechos de los interesados.

No obstante, con el fin de dotar de mayor claridad y coherencia al texto normativo, se sugiere que tanto la MAIN como el propio artículo 11 incorporen una **mención expresa** a la obligación de realizar una **Evaluación de Impacto relativa a la protección de datos personales**, conforme a lo previsto en el artículo 35 del Reglamento (UE) 2016/679, de 27 de abril de 2016, y en los artículos 28 y concordantes de la Ley Orgánica 3/2018, de 5 de diciembre.

De forma alternativa, a efectos de reforzar la seguridad jurídica y la transparencia del proceso, podría añadirse un precepto específico con un contenido análogo al siguiente:

Evaluación de Impacto en materia de protección de datos personales

- 1. Cuando los tratamientos de datos personales derivados de la aplicación de esta norma puedan implicar un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá realizar, con carácter previo a su puesta en práctica, una Evaluación de Impacto relativa a la protección de datos personales, en los términos previstos en el artículo 35 del Reglamento (UE) 2016/679 y en los artículos 28 y concordantes de la Ley Orgánica 3/2018, de 5 de diciembre.**
- 2. La evaluación deberá valorar, entre otros aspectos, la proporcionalidad y necesidad del tratamiento, el riesgo potencial para los derechos fundamentales de los interesados y las medidas de seguridad o salvaguardias que se adopten para mitigarlo.**

V

El anteproyecto de ley que se analiza contempla, entre otros aspectos, la posibilidad de que los **datos personales de administradores y directivos** figuren en los procedimientos sancionadores y en las resoluciones públicas que de ellos deriven, al establecer su **responsabilidad directa** en las infracciones detectadas. Esta previsión implica que la publicación de resoluciones sancionadoras podrá incluir información personal identificativa, lo que exige aplicar criterios estrictos de licitud, necesidad y proporcionalidad, asegurando que el tratamiento de dichos datos se fundamente en una base jurídica clara y suficiente conforme a lo dispuesto en el artículo 6 del Reglamento (UE) 2016/679, de 27 de abril de 2016, —esto es, en el cumplimiento de una obligación legal y en la existencia de un interés público prevalente— y que, además, se respeten los derechos y libertades fundamentales de las personas afectadas.

El **artículo 86 del RGPD** dispone que *“los datos personales contenidos en documentos oficiales en poder de una autoridad pública o de un organismo público pueden comunicarse por dicha autoridad u organismo de conformidad con el Derecho de la Unión o de los Estados miembros al objeto de conciliar el acceso del público a los documentos oficiales con el derecho a la protección de los datos personales con arreglo al presente Reglamento”*. Esta previsión pone de manifiesto la necesidad de que el legislador y las autoridades nacionales establezcan mecanismos que permitan armonizar el principio de transparencia y publicidad de las actuaciones administrativas con el derecho fundamental a la protección de datos personales, especialmente

cuando se trata de la difusión de información vinculada a infracciones o sanciones.

En desarrollo de este mandato, el **artículo 27 de la LOPDGDD** regula de manera específica el tratamiento de datos personales vinculados a infracciones y sanciones administrativas en los siguientes términos:

Artículo 27. Tratamiento de datos relativos a infracciones y sanciones administrativas.

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 la literalidad del precepto se desprende que el tratamiento de datos personales relacionados con infracciones y sanciones administrativas está **estrictamente condicionado** por tres elementos esenciales:

i) que el tratamiento sea efectuado **únicamente por los órganos competentes** en materia sancionadora;

ii) que se limite a los **datos imprescindibles** para la finalidad perseguida, evitando cualquier exceso o difusión innecesaria; y

iii) que, en los casos en que no concurren estas condiciones, el tratamiento

solo pueda realizarse con consentimiento expreso del interesado o **autorización mediante norma con rango de ley, que además establezca las garantías adicionales necesarias** para proteger los derechos y libertades de las personas afectadas.

Este marco normativo evidencia que la publicación de sanciones administrativas con datos personales requiere un tratamiento especialmente prudente y proporcionado. Aunque el principio de transparencia justifica la difusión de determinadas resoluciones, dicha publicación debe limitarse a los datos **estrictamente necesarios** para garantizar la finalidad informativa o disuasoria de la medida. Además, la publicación no puede tener carácter indefinido, debiendo **circunscribirse temporalmente** al periodo necesario para cumplir dicha finalidad (artículo 11.4 del anteproyecto de ley). En este sentido, la LOPDGDD insiste en la necesidad de establecer mecanismos de anonimización o seudonimización adecuados que reduzcan el impacto en la esfera personal de los interesados, así como plazos de eliminación o desindexación de la información publicada.

En definitiva, la publicación de infracciones y sanciones administrativas constituye una manifestación legítima de la transparencia y del control público de la actuación administrativa; sin embargo, dicha transparencia debe ejercerse de manera equilibrada y respetuosa con el derecho fundamental a la protección de datos personales, conforme a los principios de legalidad, proporcionalidad y minimización del tratamiento, y en el marco de las garantías establecidas tanto en el RGPD como en la LOPDGDD. **En este sentido, sin perjuicio de las observaciones realizadas en relación con la Evaluación del Impacto en materia de datos personales, las previsiones del artículo 11 resultan conformes con lo dispuesto en los artículos 86 RGPD y 27 LOPDGDD.**

Finalmente, en el artículo 12 del anteproyecto de ley, se regula la comunicación de sanciones a la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ). Dicha cesión supone también un tratamiento de datos personales. En este caso, el flujo transfronterizo de información se produce dentro del Espacio Económico Europeo y bajo el paraguas de la normativa comunitaria, lo que asegura un nivel equivalente de protección (Capítulo V, artículos 44 a 50 RGPD). No obstante, **debe garantizarse que los datos transmitidos se limiten a los estrictamente necesarios (artículo 5 RGPD).**

VI

Finalmente, de la lectura del articulado del anteproyecto de ley tampoco se obtiene mención alguna a la obligación de adoptar las medidas **técnicas y organizativas adecuadas, en cumplimiento de los artículos 25 y 32 del RGPD. A su vez, debe asegurarse** la confidencialidad de la información que contenga datos de carácter personal objeto de tratamiento.

A este respecto, conviene recordar que el artículo 5.1 del RGPD, en su apartado f), dispone expresamente lo siguiente:

“5.1 Los datos personales serán:

(...)

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»).

En consecuencia, **se sugiere** que el anteproyecto de ley incorpore una referencia explícita al cumplimiento de los principios de seguridad e integridad, de manera que los responsables de los tratamientos garanticen plenamente ambos mandatos, en los términos exigidos por la normativa vigente en materia de protección de datos.

En este sentido, el redactor de la norma podría optar entre incluir, por vía de remisión, una referencia expresa al artículo 32 del RGPD y al artículo 28 de la LOPDGDD, o bien introducir un precepto específico que regule de manera directa las condiciones de seguridad y confidencialidad aplicables a los tratamientos de datos derivados de la aplicación de la ley. Asimismo, se echa en falta el establecimiento de medidas de seguridad concretas vinculadas a dichos tratamientos, lo que aconseja modificar el texto actualmente sometido a informe para introducir las correspondientes previsiones de sometimiento y cumplimiento de las obligaciones establecidas en el RGPD.

Por ello, la referencia expresa a dichos preceptos se considera igualmente oportuna.

En conclusión, se propone la adición de un nuevo artículo, o bien de una Disposición adicional con una redacción que podría adoptar la siguiente fórmula —o similar—:

“El responsable del tratamiento de datos personales adoptará, en todo caso, las medidas de seguridad que correspondan, de conformidad con lo dispuesto en el artículo 32 del Reglamento (UE) 2016/679, de 27 de abril de 2016, y en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Las medidas de seguridad a adoptar serán de carácter técnico y

organizativo, y deberán garantizar un nivel de protección adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, así como la naturaleza, el alcance, el contexto y los fines del tratamiento.”

En conclusión, la aplicación práctica del anteproyecto de ley que se informa exige una lectura coordinada con el RGPD y la LOPDGDD. Es imprescindible que la Dirección General de Seguros y Fondos de Pensiones, en su condición de autoridad supervisora, adopte protocolos internos que aseguren el cumplimiento de los principios de minimización, limitación de la finalidad y proporcionalidad en la publicación y transmisión de datos personales, garantizando —además— la seguridad y la confidencialidad de los tratamientos de datos. Solo de este modo se logrará un equilibrio entre la transparencia y la rendición de cuentas que persigue la norma y el respeto debido a los derechos fundamentales de las personas sancionadas.

VII

En conclusión, el anteproyecto de ley que se informa carece de referencias expresas a la garantía y cumplimiento de la normativa de protección de datos.

A juicio de esta Agencia, el redactor de la norma debería aprovechar el anteproyecto de ley para introducir las previsiones legales a las que se ha hecho mención en el cuerpo de este informe, garantizando así el cumplimiento riguroso del RGPD y de la LOPDGDD por parte de la Dirección General de Seguros y Fondos de Pensiones y demás agentes implicados.

Así, en primer lugar, se sugiere la introducción de una mención específica a la normativa sobre protección de datos, que explicita de forma clara el sometimiento de los tratamientos de datos que se realicen tanto a lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos, como a la Ley Orgánica 3/2018, de 5 de diciembre, en los términos en los que ha quedado expuesto en el **Punto II** de este Informe.

Por otra parte, según se expone en el **Punto IV**, se sugiere la adición de un nuevo artículo o de una Disposición adicional, con una redacción que incorpore una mención concreta a la Evaluación de Impacto en materia de protección de datos. Finalmente, según se analiza en el **Punto VI**, por parte del responsable del tratamiento deberá procederse a la adopción de las medidas de seguridad técnicas y organizativas necesarias, y a la debida garantía de confidencialidad.