0065/2025

I

El proyecto de Real Decreto sometido a informe tiene por objeto completar la transposición al ordenamiento jurídico interno de la Directiva (UE) 2023/2226 del Consejo, de 17 de octubre de 2023 (**DAC 8**), por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad. Esta transposición fue iniciada por la ***Ley XX/2025***, de modificación parcial de la Ley 58/2003, de 17 de diciembre, General Tributaria —LGT—, cuya plena efectividad requiere un desarrollo reglamentario de carácter técnico que concrete las nuevas obligaciones de información, diligencia debida y, en su caso, registro, aplicables a los proveedores de servicios de criptoactivos y a los operadores de criptoactivos.

El incremento de los medios digitales de pago e inversión y la consolidación de nuevos instrumentos –entre ellos el dinero electrónico, los criptoactivos y las monedas digitales de bancos centrales– ha dado lugar a un marco regulatorio europeo orientado a reforzar la transparencia fiscal y garantizar la trazabilidad de los movimientos asociados a tales activos. En este contexto, la DAC 8 introduce nuevas obligaciones de reporte automático y de diligencia que requieren ajustes en diversas normas reglamentarias nacionales, tanto en materia de asistencia mutua como en lo relativo a las obligaciones tributarias internas y procedimientos de recaudación.

Según se señala en la propia MAIN de la norma el Real decreto no consta en el Plan Anual Normativo, sin perjuicio de que la ***Ley XX/2025***, que lo ampara, sí figure en el Plan Anual Normativo correspondiente al año 2025, en los siguientes términos: "LEY POR LA QUE SE MODIFICAN LA LEY 58/2003, DE 17 DE DICIEMBRE, GENERAL TRIBUTARIA, EN MATERIA DE ASISTENCIA MUTUA Y DE RECAUDACIÓN, Y OTRAS NORMAS TRIBUTARIAS."

Sin embargo, el texto de dicho **Proyecto de Ley por la que se modifican la Ley 58/2003, de 17 de diciembre,** en materia de prescripción, recaudación, asistencia mutua y obligaciones de información, y la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas …" ("Proyecto de Ley 121/000060 por la que se modifican la Ley 58/2003: BOCG-15-A-60-1") si bien se encuentra publicado en el Boletín Oficial de las Cortes

Generales (Serie A, Núm. 60-1, expedido el 13 de junio de 2025), **aún no ha sido formalmente aprobado en Cortes, ni publicado en el Boletín Oficial del Estado.**

La aprobación y entrada en vigor de la ***Ley XX/2025*** introducirá diversas modificaciones en la LGT, destacando, en materia de recaudación, *(i)* la incorporación expresa del embargo de criptoactivos y de bienes y derechos situados en entidades de pago y de dinero electrónico, así como la adaptación de los procedimientos de recaudación e ingreso a estos nuevos activos; y, en materia de asistencia mutua e información *(ii)* la reforma de la disposición adicional 22ª para reforzar las obligaciones de información y diligencia debida sobre cuentas financieras; la creación de una nueva disposición adicional 27ª que regula las obligaciones derivadas de la Directiva DAC 8 en relación con criptoactivos, operadores y registros específicos; y la sustitución del término *"moneda virtual"* por *"criptoactivo*" en la normativa interna, incluida la relativa al IRPF, alineando así la legislación con el marco europeo vigente.

El proyecto de Real Decreto se estructura en ocho artículos, una disposición adicional, una disposición transitoria, una disposición derogatoria, siete disposiciones finales y un anexo.

Los artículos 1 a 8 desarrollan las obligaciones de información y las normas de diligencia debida aplicables a los proveedores y operadores de criptoactivos, así como los criterios de sujeción a la obligación de reporte, la información identificativa que debe recabarse de los usuarios y de las personas que ejerzan su control, y el desglose de la información de operaciones con criptoactivos que ha de ser suministrado a la Administración tributaria.

La norma detalla, asimismo, la necesidad de obtener una declaración de residencia fiscal de los usuarios, regula la comunicación de información agregada sobre operaciones distinguiendo su tipología, e incorpora definiciones esenciales en un anexo técnico.

El Real Decreto realiza ajustes y desarrollos en diversos cuerpos reglamentarios con el fin de garantizar la coherencia interna del sistema y su alineación con los estándares internacionales de intercambio de información, así como con los *Comentarios de la OCDE* al Modelo de Acuerdo para la Autoridad Competente y al Marco de intercambio de información sobre criptoactivos oficiales de la DAC 8.

Así, en primer lugar, se modifica el Reglamento General de las actuaciones y procedimientos de gestión e inspección tributaria, aprobado por el Real Decreto 1065/2007, de 27 de julio, incorporando un registro específico de operadores de criptoactivos, regulando su alta, modificación y baja, y

adaptando las obligaciones de información sobre criptoactivos en sustitución del anterior concepto de “moneda virtual”.

En segundo término, se actualizan las obligaciones de identificación y diligencia debida del Real Decreto 1021/2015, de 13 de noviembre, relativo a la identificación de la residencia fiscal de titulares o controladores de cuentas financieras en el marco de la asistencia mutua. Así, se incluye información adicional sobre cuentas sujetas a comunicación y la obligación de reportar datos relativos a dinero electrónico y monedas digitales de bancos centrales, conforme a las modificaciones introducidas por la DAC 8.

Finalmente, en conexión con la reforma legal de la Ley 58/2003, de 17 de diciembre, se desarrolla el procedimiento administrativo de embargo de criptoactivos del Reglamento General de Recaudación —Real Decreto 939/2005, de 29 de julio—.

En este escenario, por parte de los diferentes operadores jurídicos cuya actuación se regula en la norma que se informa, se procederá a la realización de tratamientos de datos personales, en los términos definidos por el Reglamento (UE) 2016/679 (RGPD). Conforme al artículo 4 de dicho RGPD, se entiende por *dato personal* cualquier información relativa a una persona física identificada o identificable, y por *tratamiento* cualquier operación realizada sobre dichos datos, ya sea por medios automatizados o no, como la recogida, registro, conservación, consulta, comunicación o supresión.

II

En primer lugar, en sus artículos 1 al 8, el proyecto de Real Decreto examinado desarrolla las disposiciones introducidas en la Ley 58/2003, de 17 de diciembre, General Tributaria, como consecuencia de la transposición de la Directiva (UE) 2023/2226 (DAC 8), completando el régimen jurídico aplicable a los proveedores y operadores de servicios de criptoactivos en materia de obligaciones de información y diligencia debida. Este desarrollo reglamentario articula la obtención, contrastación, conservación y comunicación de *información identificativa*, fiscal y transaccional relacionada con los usuarios de criptoactivos y con las personas que, en su caso, ejercen el control de usuarios que tienen la condición de entidades.

El proyecto obliga a los proveedores y operadores de criptoactivos a obtener, verificar y comunicar a la Administración tributaria un conjunto exhaustivo *de datos personales* con finalidades estrictamente fiscales. Dichos tratamientos comprenden la obtención de información identificativa de cada usuario, incluyendo nombre, apellidos, domicilio, país o países de residencia fiscal, fecha y lugar de nacimiento y número de identificación fiscal, así como la

identificación de los titulares reales o personas que ejercen el control sobre usuarios que son entidades. Asimismo, se incorpora la obligación de solicitar y conservar documentación justificativa y declaraciones de residencia fiscal, además de verificar la información mediante los procedimientos de diligencia debida que el proveedor tenga implementados en el marco de la normativa de prevención del blanqueo de capitales.

A su vez, se añade el tratamiento de datos económicos y transaccionales, relativos a la totalidad de las operaciones efectuadas por los usuarios con criptoactivos. Ello incluye las adquisiciones, transmisiones, canjes, transferencias y pagos minoristas, así como la determinación del importe bruto pagado o recibido, las unidades transmitidas o adquiridas, el valor de mercado en el momento de la operación y los gastos asociados. El tratamiento no se limita a operaciones individuales, sino que abarca la agregación, clasificación y desglose por tipología, lo que permite reconstruir de manera exhaustiva los movimientos patrimoniales digitales del usuario.

La verificación continua de la información constituye un elemento estructural del Real Decreto que se informa. La norma obliga a aplicar procedimientos que permitan detectar cambios de circunstancias, evaluar la consistencia de los datos aportados, recabar información adicional cuando existan indicios de inexactitud, y contrastar lo declarado con la información disponible en el ámbito de la diligencia debida aplicada al cliente. **Este conjunto de obligaciones configura un tratamiento intensivo, prolongado y sistemático, que afecta tanto a usuarios directos como a terceros relacionados, y que comporta un significativo riesgo de perfilado financiero, patrimonial y fiscal.**

En conclusión, se realizarán un conjunto de tratamientos de datos personales —definidos por el artículo 4.2 del RGPD como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no—, que deben ser analizados a la luz del Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, y del propio marco jurídico fiscal que constituye la base habilitante del tratamiento.

El tratamiento de datos personales realizado por los proveedores y operadores de criptoactivos en virtud del proyecto de Real Decreto encuentra su fundamento jurídico en el **artículo 6.1.c) del RGPD**, en cuanto el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable. La normativa que impone dicha obligación es diversa y converge en la finalidad fiscal: la Directiva 2011/16/UE y sus modificaciones, particularmente la DAC 8; la Ley 58/2003, a través de sus disposiciones

adicionales vigésima segunda y vigésima séptima; el Acuerdo Multilateral Marco de intercambio de información sobre criptoactivos —**CARF**—, y las normas de desarrollo reglamentario. Asimismo, en el caso de los órganos administrativos actuantes, concurre la aplicación del **artículo 6.1.e)** del RGPD, en tanto que el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, en este caso la transparencia fiscal, la prevención del fraude y el intercambio automático internacional de información tributaria.

El tratamiento alcanza *diversas categorías* de datos personales. En primer lugar, se tratan datos identificativos básicos, como nombre, apellidos, fecha y lugar de nacimiento, domicilio y residencias fiscales declaradas. En segundo lugar, se tratan datos fiscalmente sensibles como los números de identificación fiscal en uno o varios países, así como datos relacionados con la titularidad real y las personas que ejercen control sobre entidades usuarias.

De manera destacada, se tratan datos económicos y financieros de gran importancia, al incluir la totalidad de operaciones realizadas con criptoactivos, su valoración económica, los importes brutos pagados y recibidos, los gastos asociados, y las direcciones utilizadas. La combinación de estos elementos configura un tratamiento de información que, aun no siendo formalmente una categoría especial de datos conforme al artículo 9 del RGPD, presenta un *riesgo elevado* por su impacto patrimonial y las potenciales consecuencias para los derechos y libertades de las personas afectadas.

En este contexto, deben tenerse en cuenta, muy especialmente los ***Principios relativos al tratamiento*****, aplicables conforme al artículo 5 del RGPD.** Así, el principio de *minimización* exige limitar los datos solicitados a los estrictamente previstos por la normativa DAC 8 / Marco de intercambio de información sobre criptoactivos —CARF—. El proveedor no puede ampliar el alcance de los datos ni requerir información adicional salvo cuando exista una obligación clara de verificación, y siempre documentando la necesidad y proporcionalidad del requerimiento.

El principio de *limitación de la finalidad* impone que los datos solo puedan utilizarse para los fines fiscales legalmente establecidos. Queda prohibida cualquier utilización con fines comerciales, analíticos o de perfilado ajeno a la finalidad tributaria, incluida la elaboración de modelos internos que excedan del cumplimiento de las obligaciones de información.

El principio de *exactitud* adquiere relevancia singular, pues la norma exige una verificación activa, continuada y sistemática. La obligación de detectar cambios de circunstancias y revisar la razonabilidad de la información comporta la implantación de mecanismos estrictos de supervisión interna.

Respecto a la *limitación del plazo de conservación*, debe garantizarse la coherencia entre los plazos previstos en la normativa tributaria, los derivados de las obligaciones internacionales de intercambio de información y los establecidos en la normativa de prevención del blanqueo de capitales. En ausencia de un plazo específico en el proyecto de Real Decreto, deben aplicarse los vigentes en la Ley General Tributaria y en la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo, lo que obliga a definir un cuadro de plazos de conservación preciso y documentado.

Por otra parte, en cuanto a las *Transferencias internacionales de datos*, el intercambio automático de información con otras jurisdicciones es uno de los aspectos más relevantes del régimen DAC 8 / CARF. La información comunicada por los proveedores a la Administración tributaria española será a su vez remitida, conforme a los estándares internacionales, a los Estados miembros de la Unión Europea y a las jurisdicciones que hayan suscrito los acuerdos pertinentes, algunas de las cuales pueden no disponer de un nivel de protección de datos equivalente al de la Unión Europea.

Estas transferencias se amparan jurídicamente en los artículos 6.1.c) y 6.1.e) del RGPD, así como en el artículo 49.1.d, relativo a las transferencias necesarias por razones de interés público. Lo anterior no exime al responsable de adoptar **medidas reforzadas de seguridad y las garantías necesarias para preservar la confidencialidad y la integridad de la información transmitida, conforme a los artículos 5 y 32 del RGPD.**

Finalmente, en cuanto a las **Obligaciones del responsable del tratamiento y las medidas organizativas**, los proveedores y operadores de criptoactivos asumen la condición de responsables del tratamiento en los términos del artículo 4.7 del RGPD.

En segundo término, *la Disposición Final Primera* introduce una reforma de amplio alcance en el Reglamento General de actuaciones y procedimientos de gestión e inspección tributaria, configurando un nuevo subsistema registral y obligacional específicamente orientado a los operadores de criptoactivos y a la información económico-transaccional asociada. Desde la perspectiva de la normativa de protección de datos, dicha modificación despliega efectos significativos, ya que crea nuevas estructuras de tratamiento —*singularmente el Registro de operadores de criptoactivos*—, impone obligaciones de suministro y actualización permanente de datos identificativos y fiscales, y amplía de forma sustancial las facultades de tratamiento de la Administración tributaria, con una base legal que debe interpretarse en consonancia con los principios del RGPD, y el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

La creación del *Registro de operadores de criptoactivos* supone la constitución de un fichero de datos de carácter público cuyo contenido incluye información identificativa, fiscal, societaria, de residencia, y de representación legal, así como elementos que permiten perfilar la actividad internacional de los operadores y sus vínculos con jurisdicciones cualificadas o con usuarios situados en terceros países.

La base jurídica del tratamiento es el cumplimiento de una obligación legal —**art. 6.1.c RGPD**—, pero el principio de minimización obliga a examinar críticamente que la información exigida sea estrictamente necesaria para determinar la sujeción de cada operador a las obligaciones de comunicación e intercambio automático de información. La obligación de declarar datos tan amplios como la jurisdicción de residencia de los usuarios sujetos a comunicación, las circunstancias que determinan la obligación de inscribirse o las direcciones electrónicas, exigen *un análisis de proporcionalidad reforzado*, en la medida en que no solo se identifica al operador, sino que se revelan aspectos de su estructura interna, de su actividad y de su cartera de clientes, configurando un volumen de datos potencialmente muy sensible desde la perspectiva económica y competitiva.

El nuevo artículo 9 quater —declaración de alta— obliga a los operadores a comunicar un conjunto de datos que constituyen información personal que se someterá a tratamientos ulteriores, incluidos los derivados de la comunicación obligatoria a todos los Estados miembros. La exigencia de actualización mediante el artículo 10 quater implica un tratamiento continuo y dinámico que intensifica la carga de exactitud, integridad y trazabilidad, y que en el marco del RGPD debe considerarse como tratamiento sistemático, requiriendo medidas de seguridad reforzadas y políticas de gestión documental adecuadas. Asimismo, el artículo 11 quater —declaración de baja— incrementa el *impacto* sobre la privacidad, ya que, aun cuando el operador deje de estar sujeto a las obligaciones de comunicación, la Administración tributaria continuará conservando los datos durante los periodos legalmente previstos, lo que exige una definición clara de plazos de retención y una justificación proporcionada de la necesidad de conservar información ya no actualizada respecto de la actividad real del proveedor.

La obligación de informar del artículo 37 ter amplía y consolida el alcance del tratamiento al exigir que los proveedores presenten una declaración anual con información de sus usuarios sujetos a comunicación y de las personas que ejercen el control sobre ellos. La incorporación de la diligencia debida prevista en el Real Decreto de transposición implica que los proveedores deberán obtener, verificar y custodiar datos identificativos y transaccionales de usuarios, así como la documentación acreditativa en materia de residencia fiscal y titularidad real.

Las obligaciones de información sobre saldos en criptoactivos (art. 39 bis) y sobre criptoactivos situados en el extranjero (art. 42 quater) constituyen dos de los tratamientos más intrusivos desde el punto de vista de la privacidad. Ambas obligaciones requieren presentar información anual detallada que identifique a los titulares, beneficiarios, autorizados o titulares reales, los saldos exactos y su valoración en euros, así como el historial de tenencia a lo largo del año cuando se pierde o adquiere tal condición. Estos tratamientos permiten reconstruir de manera completa *la posición patrimonial en criptoactivos* de cada persona, tanto en España como en el extranjero.

Las modificaciones del artículo 45 —relativas a intermediarios y al deber de declarar mecanismos transfronterizos— y del artículo 66 —que amplía los datos exigibles en consultas vinculantes con dimensión internacional— también afectan a la protección de datos al incorporar nuevas obligaciones de identificación de terceros afectados, incluidos residentes en otros Estados, así como información relativa a estructuras societarias, transacciones y operaciones que pueden resultar sensibles. Finalmente, la modificación del artículo 147, que vincula la baja cautelar registral con determinadas circunstancias fiscales —incluidas las relacionadas con proveedores de servicios de criptoactivos—, tiene también implicaciones en materia de protección de datos, pues cualquier anotación en un registro administrativo constituye un tratamiento que puede afectar a derechos fundamentales y debe aplicarse con estricta sujeción a los principios de exactitud, necesidad y proporcionalidad.

En conjunto, la Disposición Final Primera despliega un entramado normativo que *crea nuevos tipos de tratamientos de datos*, amplía la tipología de *datos tratados*, incrementa la frecuencia y obligatoriedad de las *comunicaciones, y habilita flujos de información* continuos entre operadores, la Administración tributaria y las autoridades competentes de otros Estados.

La reforma de *la Disposición final segunda*, que modifica el Real Decreto 1021/2015, de 13 de noviembre, sobre la identificación de residencia fiscal y el intercambio automático de información, amplía y actualiza de manera significativa las obligaciones de identificación y reporte financiero según las directivas europeas recientes y los estándares de la OCDE.

El volumen y detalle de la información exigida a las instituciones financieras aumenta notablemente: además de los datos identificativos habituales, deben comunicarse saldos, movimientos, ingresos, naturaleza de los instrumentos y la condición del titular o beneficiario efectivo. Esto supone un tratamiento más intenso de datos personales al combinar información financiera exhaustiva con datos identificativos reforzados.

Se incorpora expresamente la comunicación de datos sobre estructuras societarias y personas con control, basándose en los procedimientos de prevención del blanqueo de capitales. La reutilización de estos datos requiere garantizar la limitación de finalidad y una base jurídica adecuada.

La actualización de definiciones —como institución financiera, cuenta financiera, criptoactivo sujeto a comunicación o dinero electrónico— amplía el número de situaciones sujetas a reporte. Las entidades deben crear nuevos procesos de verificación y agregación que permiten reconstruir la actividad financiera de forma muy detallada y continua. La incorporación de criptoactivos al esquema general extiende la trazabilidad equiparándolos a los activos tradicionales.

Aunque existen excepciones para obtener ciertos datos, estas no reducen de forma sustancial el alcance del tratamiento, dada la obligación de hacer esfuerzos razonables, actualizar información y consultar registros. La posibilidad de usar datos de prevención del blanqueo de capitales consolida un flujo constante de información entre marcos normativos.

En conjunto, la reforma establece un sistema más amplio y granular de información financiera internacionalmente intercambiable, *intensificando el tratamiento de datos personales* y generando desafíos respecto a minimización, limitación de la finalidad y proporcionalidad.

La Disposición final tercera incorpora un nuevo artículo 92 bis al Reglamento General de Recaudación para regular por primera vez un procedimiento específico de embargo de criptoactivos. Basándose en la definición del Reglamento (UE) 2023/1114, se habilita a la Administración tributaria a trabar estos bienes cuando conozca su existencia y titularidad, articulando además un sistema de colaboración con los distintos operadores que intervienen en su emisión, custodia o registro.

Desde la perspectiva de protección de datos, el procedimiento implica un *tratamiento intenso de información personal*, al referirse a datos que identifican al titular o beneficiario y a elementos de su posición patrimonial digital. Así, los proveedores de servicios de criptoactivos, emisores, custodios y entidades vinculadas a plataformas de compraventa deben recibir diligencias, localizar activos, efectuar anotaciones e informar a la Administración, accediendo y comunicando datos relativos a titularidad, saldos y naturaleza de los criptoactivos.

La ampliación del embargo a otros criptoactivos del mismo obligado —aunque inicialmente no constaran ante la Administración— resulta especialmente relevante para los principios de minimización y proporcionalidad.

El artículo permite extender la diligencia a cualquier activo respecto del cual la entidad haya prestado servicios, obligando a consultar y transmitir información adicional sobre activos no identificados previamente y dando lugar a un tratamiento más amplio que el estrictamente necesario para la traba inicial.

El procedimiento también impone obligaciones de comunicación inmediata, como aportar una relación de activos cuando los identificados sean insuficientes e informar de incidencias que afecten al embargo. Esto genera una transmisión recurrente y actualizada de información patrimonial digital, exigida además con una valoración conforme al mercado, lo que convierte el tratamiento en un proceso dinámico y continuado.

Finalmente, la norma contempla escenarios complejos como la autocustodia, permitiendo el aseguramiento de dispositivos que contienen claves privadas o frases de recuperación. Estas actuaciones pueden comprometer información sensible, tanto patrimonial como tecnológica, por lo que requieren una interpretación especialmente cuidadosa para garantizar la necesidad, la limitación de finalidad y la protección de datos cuya exposición podría afectar a la integridad de la información digital del afectado.

En resumen, el Real Decreto sometido a informe implica la **realización de tratamientos de datos personales cuya necesidad y adecuación deben analizarse conforme a las exigencias de la normativa de protección de datos.**

Sin embargo, el proyecto apenas incorpora referencias a este marco normativo. Únicamente incluye una mención en el Capítulo III de la parte expositiva, cuando indica que *“la información suministrada a la Administración tributaria […] será comunicada al resto de Estados miembros de la Unión Europea e intercambiada con terceros países, de acuerdo con la normativa de protección de datos personales”.*

A la vista de ello, se considera necesario introducir una referencia expresa al pleno sometimiento de los tratamientos previstos al Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos, y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo, resultaría conveniente que el Real Decreto incluyera una mención explícita al cumplimiento de los principios y obligaciones establecidos en los artículos 5 y 32 del RGPD. Ello garantizaría la integridad, disponibilidad y confidencialidad de la información tratada, así como la aplicación efectiva del principio de minimización, de forma que los datos recabados sean adecuados, pertinentes y limitados a lo estrictamente necesario para la finalidad perseguida.

En conclusión, se **propone incorporar** un nuevo artículo o una Disposición adicional con un contenido similar al siguiente:

> **"La totalidad de las actuaciones reguladas en este Real Decreto y en sus normas de desarrollo se llevarán a cabo con el debido respeto a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y a lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como en el resto de normativa aplicable en la materia."**
>
> **Asimismo, los tratamientos de datos personales efectuados por los responsables al amparo de este Real Decreto se ajustarán a los principios relativos al tratamiento establecidos en el artículo 5 del RGPD, en particular a los de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad y confidencialidad. De igual modo, los responsables de los tratamientos de datos adoptarán las medidas técnicas y organizativas apropiadas previstas en el artículo 32 del RGPD para garantizar un nivel de seguridad adecuado al riesgo, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental."**

De tal modo, con la incorporación del precepto propuesto, no solo se garantizaría el sometimiento de los tratamientos de datos a la normativa

aplicable sobre protección de datos, sino que, **además, se determinaría la responsabilidad** en relación con la realización de dichos tratamientos, en consonancia con la definición del artículo 4.7 RGPD, que se refiere a *"7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros."*

III

De acuerdo con lo anterior, en cuanto a las obligaciones de los operadores jurídicos responsables de los tratamientos y las medidas organizativas del proyecto de Real Decreto, los proveedores y operadores de criptoactivos asumen la condición de responsables del tratamiento en los términos del artículo 4.7 del RGPD. Estos responsables deben implantar políticas de seguridad reforzadas que incluyan mecanismos de cifrado, segmentación de bases de datos, control estricto de accesos, trazabilidad completa de consultas e integridad de los canales de transmisión. Asimismo, deben garantizar la adecuada formación del personal y establecer controles internos que aseguren la detección inmediata de desviaciones o anomalías en la información aportada por los usuarios.

En tal condición, les corresponde llevar un registro actualizado de actividades de tratamiento, *elaborar e implementar* ***una evaluación de impacto relativa a la protección de datos***, debido al carácter sistemático y masivo del tratamiento, y a la existencia de transferencias internacionales periódicas. **Dicha evaluación —EIPD— es obligatoria a tenor del artículo 35 del RGPD.**

> "Artículo 35. Evaluación de impacto relativa a la protección de datos
>
> 1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
>
> 2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
>
> 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o (la negrita es nuestra)

c) observación sistemática a gran escala de una zona de acceso público.
(…)

10.Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, **y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento."** (la negrita es nuestra)

En este sentido, de acuerdo con el análisis de los Puntos anteriores de este informe, la regulación contenida en el proyecto de Real Decreto implica un tratamiento de datos personales particularmente intenso y complejo, derivado de la necesidad de cumplir con los estándares europeos e internacionales de intercambio automático de información fiscal en el ámbito de los criptoactivos. Dicho tratamiento se ampara en una obligación legal y en una misión de interés público, con limitaciones claras en el ejercicio de derechos, y requiere la adopción de medidas reforzadas de diligencia, seguridad, transparencia e impacto. **La naturaleza y volumen de los datos tratados, su sensibilidad financiera y la existencia de transferencias internacionales sistemáticas exigen una aplicación estricta de los principios del RGPD —*ex* artículo 5 RGPD—, y la elaboración obligatoria de una evaluación de impacto —*ex* artículo 35 RGPD— exhaustiva por parte de los operadores afectados.**

Por otra parte, como se indicó *ut supra*, *la Disposición Final Primera* —que modifica el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria aprobado por el Real Decreto 1065/2007, de 27 de julio— incorpora un nuevo artículo 37 ter que establece una obligación informativa de alcance significativamente ampliado. Este precepto exige a los

proveedores remitir anualmente información detallada tanto sobre los usuarios sujetos a comunicación obligatoria como sobre las personas que ejercen su control. A ello se suma la diligencia debida prevista en el Real Decreto de transposición, que obliga a dichas entidades a obtener, verificar y conservar datos identificativos y operativos de los usuarios, así como la documentación que acredite su residencia fiscal y su condición de titulares reales, lo que intensifica y prolonga de forma notable el tratamiento de datos requerido.

Desde la óptica del RGPD, esto comporta un *tratamiento intensivo de datos financieros y patrimoniales, de alto impacto,* que exige aplicar plenamente los principios de privacidad desde el diseño y por defecto, así como la obligación de realizar **una evaluación de impacto previa a la puesta en marcha del sistema, dada la escala y naturaleza del tratamiento.** En este contexto, deviene necesario establecer límites y cautelas que garanticen que el volumen de datos comunicados no excede de lo estrictamente necesario ni deriva en usos amplificados o finalidades implícitas no explicitadas en la habilitación legal.

Como también se señaló anteriormente, las obligaciones informativas relativas a los saldos mantenidos en criptoactivos (art. 39 bis) y a los criptoactivos ubicados fuera del territorio nacional (art. 42 quater) configuran algunos de los tratamientos de datos personales de mayor intensidad desde la óptica de la privacidad. Ambas previsiones requieren la remisión anual de datos pormenorizados que permiten identificar plenamente a titulares, beneficiarios, personas autorizadas o titulares reales, incluyendo el importe exacto de los saldos, su correspondiente valoración en euros y, en su caso, la evolución de la titularidad durante el ejercicio cuando esta se adquiere o se pierde. El conjunto de esta información posibilita una reconstrucción exhaustiva de la situación patrimonial de cada individuo en materia de criptoactivos, tanto respecto de los mantenidos en España como en el exterior.

La creación de este nuevo sistema declarativo, unido al carácter masivo, continuo y de alto riesgo del tratamiento, **obliga a realizar una EIPD previa a su implantación,** en tanto concurren varios de los supuestos de obligatoriedad: tratamiento de datos financieros sensibles, volumen elevado de interesados, elaboración de perfiles patrimoniales detallados, posibilidad de decisiones automatizadas indirectas y existencia de transferencias internacionales sistemáticas. La inclusión de supuestos de exención por razón de contabilidad o de límites cuantitativos no reduce el impacto del sistema ni la obligación de examinar los riesgos derivados del conjunto del tratamiento.

Por su parte, la introducción de obligaciones de información detallada y la ampliación de competencias de la Administración tributaria sobre criptoactivos y cuentas financieras, como se establece en las *Disposiciones*

Finales Segunda y Tercera, generan un tratamiento intensivo de datos personales especialmente intrusivo. Estos tratamientos incluyen información identificativa reforzada, datos financieros completos, movimientos de cuentas, saldos y claves, y registros de custodia. La magnitud, diversidad y persistencia de los datos implicados **hace recomendable realizar una Evaluación de Impacto sobre la Protección de Datos para identificar riesgos potenciales para los derechos y libertades de los interesados y adoptar medidas de mitigación adecuadas.**

En particular, la *Disposición Final Segunda* amplía la obligación de las instituciones financieras de reportar datos de residentes fiscales y beneficiarios efectivos, incluyendo información sobre múltiples jurisdicciones, funciones de control y características de cada cuenta. La *Disposición Final Tercera*, por su parte, establece la posibilidad de embargar criptoactivos, incluyendo activos en auto-custodia, lo que implica el tratamiento de información altamente técnica y potencialmente identificativa de las personas físicas involucradas. Ambos supuestos combinan información personal con datos financieros y de control que podrían permitir la reconstrucción exhaustiva del patrimonio y actividades de los interesados, **reforzando la necesidad de una EIPD para garantizar la proporcionalidad y seguridad del tratamiento.**

Una EIPD permitiría, además, identificar los posibles riesgos derivados de la agregación de datos de distintas fuentes, la transferencia de información entre jurisdicciones y la interacción con sistemas tecnológicos complejos, como los registros distribuidos de criptoactivos. Esta evaluación sería clave para definir medidas técnicas y organizativas que limiten el acceso, preserven la confidencialidad y aseguren la trazabilidad del tratamiento, contribuyendo a cumplir con los principios de protección de datos y a proteger los derechos fundamentales de los afectados.

Sin embargo, de acuerdo con su Memoria de Análisis de Impacto Normativo, el proyecto se limita a completar la transposición reglamentaria de la DAC 8 sin introducir particularidades específicas en materia de protección de datos personales. A dichos efectos, según se indica en la MAIN, la propia DAC 8 fue objeto de evaluación por el Supervisor Europeo de Protección de Datos, declarando expresamente, en su Considerando 46, el pleno respeto al derecho fundamental a la protección de datos (artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea), recordando la aplicación directa de los Reglamentos (UE) 2016/679 y 2018/1725 a los tratamientos de datos derivados de la Directiva 2011/16/UE.

En la misma línea, la MAIN del Proyecto de Ley de modificación de la Ley 58/2003, de 17 de diciembre, señala igualmente que no se incorporan particularidades adicionales en materia de protección de datos ni resulta

precisa una nueva evaluación de impacto, puesto que la propia DAC 8 ya fue analizada por el Supervisor Europeo de Protección de Datos y en su Considerando 46 afirma expresamente el pleno respeto al derecho fundamental a la protección de datos, en los siguientes términos:

> "Considerando (46):
>
> La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»). En particular, la presente Directiva garantiza plenamente el derecho a la protección de los datos de carácter personal establecido en el artículo 8 de la Carta. A ese respecto, es importante recordar que los Reglamentos (UE) 2016/679 y (UE) 2018/1725 se aplican al tratamiento de datos personales en virtud de la Directiva 2011/16/UE. Además, la presente Directiva está dirigida a garantizar el pleno respeto del derecho a la libertad de empresa."

En su Opinión 9/2023, el Supervisor Europeo de Protección de Datos (EDPS) analiza la propuesta de Directiva que dio lugar a la DAC 8, centrándose en la mejora de la cooperación administrativa en materia tributaria y en las nuevas obligaciones de intercambio de información, especialmente respecto de criptoactivos. Aunque el EDPS formula observaciones relevantes sobre el tratamiento de datos personales, la Opinión **no incluye ninguna referencia específica a la necesidad de realizar una Evaluación de Impacto en materia de Protección de Datos (EIPD)**.

El EDPS insiste en que cualquier uso de datos personales debe apoyarse en una base legal clara y en finalidades estrictamente definidas, recomendando concretar los propósitos de reutilización de la información, clarificar los roles de responsables y corresponsables entre Estados miembros y Comisión, y establecer límites precisos a la conservación de datos. Asimismo, subraya que la creación de un registro central de información sobre criptoactivos exige garantizar que el acceso y tratamiento por parte de la Comisión se ajusten al principio de minimización.

En términos generales, el EDPS valora positivamente los objetivos de la propuesta, pero recuerda que deben incorporarse medidas de protección de datos "desde el diseño y por defecto". Sin embargo, pese a estas recomendaciones —que ponen de relieve la complejidad y el impacto del tratamiento—, la Opinión **no aborda en ningún momento la obligación de realizar una EIPD**, omisión significativa dado el alcance masivo y sistemático de los tratamientos previstos.

En conclusión, tanto las MAIN como los proyectos de Ley y de Real Decreto (este último, objeto del presente Informe) no incorporan una evaluación

de impacto en materia de protección de datos específicamente vinculada a los tratamientos que habilitan. La mera transposición de la Directiva (UE) 2023/2226 (DAC 8) no exime del cumplimiento de los artículos 24, 25 y 35 del RGPD, ni los considerandos de la Directiva, ni tampoco la Opinión del Supervisor Europeo de Protección de Datos resultan suficientes para liberar a las autoridades nacionales de analizar el impacto real y efectivo de los tratamientos introducidos y los riesgos derivados para los derechos y libertades de los interesados.

De acuerdo con las *"Orientaciones para la realización de una evaluación de impacto en el desarrollo normativo de la AEPD (abril 2023)"*, el rango de la norma es un factor determinante para apreciar la necesidad de realizar una EIPD. En este caso, nos encontramos ante una normativa legal y reglamentaria que establece tratamientos nuevos, masivos, sistemáticos y permanentes, basados en datos económicos y transaccionales altamente sensibles; impone obligaciones reforzadas de diligencia; y prevé intercambios automatizados e internacionales de información. Conforme a dichas *Orientaciones*, cuando una norma habilita tratamientos de alta intensidad o afecta a sectores tecnológicos o financieros especialmente sensibles, la autoridad pública está obligada a realizar un análisis anticipado y documentado del impacto, incluso si la medida deriva de obligaciones europeas.

Por ello, y dado que concurren todos los factores de riesgo identificados —novedad del tratamiento, volumen masivo de datos, sistematicidad, elaboración de perfiles fiscales, verificaciones continuas, decisiones automatizadas y transferencias internacionales de datos recurrentes— **no basta con el Considerando 46 de la DAC 8 ni con la Opinión del EDPS, que además no tiene efecto directo ni sustituye las exigencias del RGPD.**

En consecuencia, para la aprobación definitiva de las normas de transposición resulta imprescindible realizar el correspondiente análisis de riesgos y la evaluación de impacto en materia de protección de datos, con el fin de asegurar que la regulación incorpora las salvaguardas técnicas, jurídicas y organizativas necesarias para cumplir con los principios del RGPD y proteger adecuadamente los derechos fundamentales de las personas.

La EIPD aplicable a normas que habilitan tratamientos de datos personales debe evaluar el impacto sobre los derechos y libertades de los individuos, e intereses de la sociedad, no limitarse a un análisis meramente jurídico o declarativo. Su finalidad es identificar riesgos, proponer medidas de mitigación y orientar la configuración del tratamiento conforme a los principios de necesidad, proporcionalidad y minimización. Tanto la jurisprudencia del TJUE como del TEDH exigen que la *proporcionalidad* de una norma que

habilita tratamientos intensivos de datos se evalúe atendiendo a los hechos concretos, finalidades específicas y circunstancias reales del tratamiento.

Por tanto, **la EIPD** no puede entenderse como un trámite formal, sino como una metodología estructurada paso a paso que permite identificar riesgos, valorar su impacto y diseñar medidas jurídicas, técnicas y organizativas para mitigarlos. **Su ausencia en el procedimiento de elaboración del presente Real Decreto evidencia un déficit que debería ser corregido antes de su aprobación definitiva a través de la realización de una adecuada valoración ex ante de todos los riesgos que los tratamientos de datos personales derivados de su aplicación pudieran conllevar, lo que a su vez permitiría la adopción de las medidas de protección técnicas y organizativas necesarias dirigidas a la mitigación de tales riesgos.**

En este sentido, según se señalaba en nuestro **Informe 015/2024**, de 29 de abril de 2024, y ahora se reitera:

> "Dicho análisis, evaluación de impacto y establecimiento en la norma de las circunstancias que permiten y las medidas adecuadas y específicas que legitiman la incidencia en el derecho fundamental a la protección de datos personales debería llevarse a cabo con la ayuda del Delegado de Protección de datos correspondiente. Y dicho análisis de riesgos y EIPD habrían de llevarse a cabo incluso en el caso de que la norma que regulase los tratamientos de datos personales tuviera rango de ley.
>
> Esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos puedan tener como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, **haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, quien realice en el curso del procedimiento de creación de la norma una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto *"Otros impactos",* el análisis del "impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma".** (la negrita es nuestra):
>
> *g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el*

desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.

En similares términos, en el Punto VI de nuestro **Informe 0100/2022**, se señala que:

"Por último, cabe hacer una reflexión general relativo al establecimiento en el proyecto de diversos registros, a los que ya se ha hecho referencia.

El proyecto expone que es desarrollo de determinadas modificaciones de la LGT, en la redacción añadida por la Ley 11/2021, de 9 de julio, que, en definitiva, entre otras circunstancias, responden al establecimiento de las características que han de tener determinados registros. Como tal, dichos registros tratan datos personales cuando se refieren a datos de personas físicas (véanse por ejemplo art. 4.1 RGAT). Dichos tratamientos de datos están incluidos en el ámbito de aplicación del RGPD, y de la LOPDGDD, y por lo tanto habrán de regirse igualmente por dicha normativa.

A este respecto, es preciso mencionar que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece expresamente (art. 3.1) que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto. Añade expresamente (art. 3.2) que, en estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

En el proyecto presentado a informe no se contiene, en cambio, ninguna referencia a la necesidad de que el responsable, o encargado del tratamiento, realice, como establece el art. 3.2 citado del Real Decreto sobre el ENS, un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. Y es de señalar igualmente que la Memoria de Análisis de Impacto Normativo (MAIN) tampoco contiene referencia al impacto en la protección de los datos personales de los interesados, ni establece medida específica de seguridad o garantías para que esos tratamientos no interfieran más allá de lo estrictamente necesario en el derecho fundamental a la protección de datos de que disfrutan las personas físicas.
(…)

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

> Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta "los riesgos que se derivan del tratamiento de los datos personales" (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), **en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado Real Decreto (art. 3.3).** (la negrita es nuestra)
>
> En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece (ver art. 35.7.d) RGPD). Al no haber una EIPD no se conocen cuáles son esos riesgos que derivan de los tratamientos de datos personales que establece la norma, por lo que a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia las posibles medidas y garantías que paliarían esos riesgos.
>
> Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo "desde el diseño" del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma."

En conclusión, esta Agencia recuerda que en el citado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), se establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta *"los riesgos que se derivan del tratamiento de los datos personales"* (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales, en todo caso prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado Real Decreto (art. 3.3).

Por todo lo expuesto, la Agencia recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 y 25 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece —art. 35.7.d) RGPD—. *Al no existir una EIPD en el presente caso, no se conocen cuáles son esos*

riesgos que derivan de los tratamientos de datos personales que establece la norma, por lo que tampoco se recogen las posibles medidas y garantías que paliarían esos riesgos.

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

Como consecuencia de lo indicado, se considera necesario que —de acuerdo con el artículo 35 RGPD y art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre— se realice, con intervención del delegado de protección de datos del Ministerio de Hacienda, un análisis de riesgos y una Evaluación de impacto en la protección de datos, que permita identificar las garantías necesarias que habría que trasladar al Real Decreto que se informa.

V

En conclusión, en primer lugar, se considera conveniente que la norma proyectada prevea la realización de un análisis de riesgos y de una **Evaluación de Impacto en la Protección de Datos**, de acuerdo con el artículo 35 del RGPD y con el artículo 2.1.g) del Real Decreto 931/2017, de 27 de octubre. Dichos instrumentos, que deberán elaborarse con la intervención del delegado de protección de datos del Ministerio de Igualdad, permitirán identificar las garantías que deban incorporarse al Real Decreto para asegurar la plena adecuación de los tratamientos previstos a la normativa de protección de datos.

Asimismo, en segundo lugar, y conforme a lo expuesto en el cuerpo del presente informe, se sugiere la *modificación o incorporación de los preceptos* indicados en los términos ya detallados. Concretamente, tal y como se ha explicado más arriba, se propone añadir un nuevo artículo o disposición adicional con un contenido equivalente al siguiente:

"La totalidad de las actuaciones reguladas en este Real Decreto y en sus normas de desarrollo se llevarán a cabo con el debido respeto a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y

del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y a lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como en el resto de normativa aplicable en la materia."

Asimismo, los tratamientos de datos personales efectuados por los responsables al amparo de este Real Decreto se ajustarán a los principios relativos al tratamiento establecidos en el artículo 5 del RGPD, en particular a los de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad y confidencialidad. De igual modo, los responsables de los tratamientos de datos adoptarán las medidas técnicas y organizativas apropiadas previstas en el artículo 32 del RGPD para garantizar un nivel de seguridad adecuado al riesgo, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental."