

018/2026

I

La Orden que se informa tiene por objeto la modificación de la Orden de 24 de julio de 2013, del Departamento de Sanidad, Bienestar Social y Familia, reguladora de las prestaciones del Sistema para la Autonomía y Atención a la Dependencia en la Comunidad Autónoma de Aragón, introduciendo un conjunto de cambios dirigidos fundamentalmente a adaptar el sistema autonómico a las recientes reformas estatales en materia de dependencia.

La norma proyectada no establece una regulación *ex novo* del sistema, sino que incide sobre preceptos concretos de la Orden vigente, modificando determinados artículos y disposiciones adicionales y transitorias, así como incorporando nuevas previsiones que afectan, principalmente, a la asistencia personal, al régimen económico de las prestaciones y a la introducción de un nuevo grado de dependencia —grado III+— vinculado a situaciones de alta complejidad y curso irreversible.

En este sentido, el artículo único de la Orden proyectada modifica, en primer término, el artículo 19 de la norma de 2013, redefiniendo la asistencia personal como un servicio orientado a la promoción de la vida independiente y la inclusión social de las personas en situación de dependencia, con independencia de su edad o grado, basado en un plan personal que articula los apoyos necesarios para el desarrollo de su proyecto de vida.

Asimismo, se modifica el artículo 20, relativo a los requisitos de las personas que presten servicios de asistencia personal, introduciendo condiciones más detalladas en cuanto a edad, residencia, inexistencia de vínculos familiares próximos con la persona beneficiaria, capacitación profesional y ausencia de antecedentes por delitos de naturaleza sexual. Igualmente, se regulan las modalidades de contratación —directa o a través de entidades— y se exige la inscripción en el correspondiente registro autonómico tanto para empresas como para profesionales autónomos.

Por otra parte, se modifica el artículo 32, que regula la prestación económica vinculada al servicio y la prestación de asistente personal, manteniendo la fórmula general de cálculo basada en el coste del servicio y la capacidad económica del beneficiario, pero introduciendo nuevos supuestos específicos, en particular para determinados servicios y, de forma destacada, para las personas con grado III+ de dependencia extrema. En relación con

estas últimas, se establece un régimen específico de cuantificación de la prestación, basado en el gasto justificado y en la capacidad económica del solicitante, con aplicación de coeficientes progresivos en función del nivel de renta.

La Orden incorpora también modificaciones relevantes en la disposición adicional sexta, en la que se actualizan las cuantías máximas y mínimas de las prestaciones económicas, incluyendo una previsión específica para el nuevo grado III+, así como la introducción de nuevas disposiciones adicionales —décima, undécima y duodécima— destinadas, respectivamente, a definir las enfermedades y procesos que permiten acceder a dicho grado, regular los efectos temporales de las resoluciones y prever la formalización de convenios de colaboración con entidades del tercer sector.

Igualmente, se modifican las disposiciones transitorias primera y segunda, relativas al régimen de acreditación de centros y servicios y a la determinación de los costes de referencia y precios máximos, manteniendo un régimen provisional hasta la aprobación de las correspondientes normas de desarrollo.

Las previsiones contenidas en la Orden que se informa se enmarcan en el desarrollo del Sistema para la Autonomía y Atención a la Dependencia, integrado en el Sistema Público de Servicios Sociales de Aragón, conforme a lo dispuesto en la Ley 5/2009, de 30 de junio, de Servicios Sociales de Aragón, y en la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia, así como en su normativa de desarrollo estatal y autonómica.

En este sentido, la Ley 5/2009, de 30 de junio, define en su artículo 3 el sistema de servicios sociales como el conjunto integrado de recursos y prestaciones públicas y privadas destinadas a la atención social. Dentro de este sistema, los servicios vinculados a la autonomía personal y a la atención a la dependencia figuran como ámbitos de actuación destacados, incluidos en el catálogo de prestaciones del Sistema Público de Servicios Sociales, desarrollado reglamentariamente por el Decreto 143/2011, de 14 de junio, del Gobierno de Aragón.

Asimismo, el artículo 36.3.e) de la citada Ley 5/2009 contempla estos servicios como prestaciones especializadas orientadas a mantener o mejorar la autonomía personal de las personas y apoyar a sus cuidadores, favoreciendo su permanencia en el entorno habitual. Por su parte, la Ley 39/2006, de 14 de diciembre, los incluye en su catálogo de servicios, desarrollados mediante los Acuerdos del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia de 3 de agosto de 2011 y 16 de julio de 2014.

A su vez, este marco normativo constituye desarrollo de las previsiones del Estatuto de Autonomía de Aragón, aprobado por Ley Orgánica 5/2007, de 20 de abril, que atribuye a la Comunidad Autónoma la competencia exclusiva en materia de acción social, comprensiva de la ordenación, organización y desarrollo de un sistema público de servicios sociales destinado a la protección de colectivos que requieren especial atención, en los términos previstos en su artículo 71.34.^a.

De igual modo, la norma proyectada responde a la necesidad de adaptar el ordenamiento autonómico a las recientes modificaciones introducidas en la normativa básica estatal, en particular las derivadas del Real Decreto-ley 11/2025, de 21 de octubre, y del Real Decreto 969/2025, de 28 de octubre, que establecen nuevas categorías de dependencia y criterios para su reconocimiento, lo que exige su desarrollo por parte de las Comunidades Autónomas.

Habida cuenta del objeto de la Orden que se informa, y en la medida en que la misma regula el acceso a prestaciones, la determinación de su cuantía, la acreditación de entidades y la gestión de servicios, resulta evidente que implica la recogida y tratamiento de un amplio conjunto de datos de carácter personal, incluyendo datos identificativos, económicos, sociales y, de forma especialmente relevante, datos relativos a la salud de las personas afectadas, lo que exige su análisis desde la perspectiva de la normativa de protección de datos.

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.”*

En este marco, la aplicación de la Orden proyectada implica necesariamente la realización de múltiples operaciones de tratamiento de datos personales, tanto en el ámbito de la gestión administrativa de las prestaciones como en el seguimiento de las personas beneficiarias, la acreditación de entidades y la evaluación de los servicios prestados, incluyendo en muchos casos categorías especiales de datos, como los relativos a la salud, cuya protección exige un especial rigor conforme al artículo 9 del RGPD.

A este respecto, conforme a lo dispuesto en el artículo 4.7 del RGPD, resulta imprescindible identificar con precisión al responsable del tratamiento, entendido como la persona física o jurídica, autoridad pública u organismo que determina los fines y medios del tratamiento, ya que su correcta determinación constituye un elemento esencial para garantizar los principios de responsabilidad proactiva y transparencia exigidos por la normativa de protección de datos.

Sin embargo, del texto de la Orden proyectada no se desprende con la claridad necesaria qué órgano u órganos ostentan dicha condición. Si bien se contienen diversas referencias al IASS como entidad gestora de las prestaciones, así como al Departamento competente en materia de servicios sociales en relación con la aprobación de normas de desarrollo, la fijación de cuantías o la regulación de determinados aspectos organizativos, no se establece de forma expresa y unívoca cuál de estos órganos, o si ambos, actúan como responsables del tratamiento de los datos personales.

Esta falta de determinación resulta especialmente relevante en una

norma que regula de forma intensiva tratamientos de datos personales, incluidos datos de categorías especiales, y cuya gestión se incardina en el sistema público de servicios sociales. En este sentido, la necesidad de establecer expresamente el órgano responsable del tratamiento no solo deriva de la legislación de protección de datos, sino que se ve reforzada por lo previsto en los artículos 3 y 36.3 de la Ley 5/2009, de 30 de junio, de Servicios Sociales de Aragón, que atribuyen a dicho sistema funciones que implican necesariamente el tratamiento de datos personales en el marco de la atención integral y la promoción de la autonomía personal.

Por todo ello, se considera necesario incorporar un precepto específico en el que se identifique de manera expresa y unívoca al órgano u órganos responsables del tratamiento, a fin de garantizar la seguridad jurídica y la plena conformidad de la Orden con el marco normativo vigente en materia de protección de datos.

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; (La negrita es nuestra)

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.”

La Ley 5/2009, de 30 de junio, de Servicios Sociales de Aragón, en su artículo 36 —Prestaciones de servicio—, comprende la totalidad de los que componen el sistema público de intervenciones realizadas por equipos profesionales, cuya finalidad (apartado 1) es atender situaciones de necesidad social mediante la prevención, la información, el diagnóstico, la valoración, la orientación, la atención doméstica y personal, el acompañamiento social, la mediación, la protección, la promoción, la atención y la inserción de personas, unidades de convivencia, grupos y comunidades. La regulación de dichos servicios se desarrolla en los apartados 2 y 3 del mencionado precepto.

Las citadas previsiones normativas, establecidas en una norma con rango de ley formal que, a su vez, supone una concreción y desarrollo del Estatuto de Autonomía de Aragón, 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 conclusión, el tratamiento de datos personales derivado de la aplicación de la Orden proyectada encuentra su base de legitimación, fundamentalmente, en lo dispuesto en el **artículo 6.1.c) y e)** del Reglamento (UE) 2016/679, en la medida en que resulta necesario para el cumplimiento de obligaciones legales y para el ejercicio de competencias atribuidas a las

Administraciones Públicas en materia de servicios sociales y atención a la dependencia.

Asimismo, en la medida en que dichos tratamientos implican el uso de categorías especiales de datos, en particular datos relativos a la salud de las personas afectadas, concurre igualmente una habilitación para el tratamiento de los datos conforme al **artículo 9.2** del citado Reglamento, en particular en su **letra h)**, relativa a la gestión de sistemas y servicios de asistencia social, sobre la base del Derecho de la Unión o de los Estados miembros.

Y, a su vez, la regulación contenida en la Ley 5/2009, de 30 de junio, de Servicios Sociales de Aragón, y en la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia, constituye habilitación jurídica suficiente para el tratamiento de los datos personales necesarios para la gestión de las prestaciones del sistema, en los términos previstos en el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre.

En este sentido, el carácter público de las funciones desempeñadas por la Administración autonómica en este ámbito excluye, con carácter general, la necesidad de recabar el consentimiento de las personas interesadas como base de legitimación, sin perjuicio de que deba garantizarse en todo caso el respeto a los derechos de los interesados y el cumplimiento de los principios establecidos en el artículo 5 del RGPD.

IV

Las modificaciones introducidas por la Orden objeto de este informe implican el tratamiento de datos personales en diversos ámbitos específicos.

En relación con el artículo 19, relativo a la asistencia personal, la elaboración de planes personales de apoyo comportará el tratamiento de datos relativos a las circunstancias personales, sociales y, en su caso, de salud de las personas beneficiarias.

El artículo 20, al regular los requisitos de las personas que prestan servicios de asistencia personal, implica el tratamiento de datos identificativos, profesionales y, en particular, datos relativos a antecedentes penales en relación con delitos de naturaleza sexual, lo que exige una especial atención al principio de minimización y a la base jurídica que legitima dicho tratamiento.

Por su parte, el artículo 32, en su nueva redacción, regula el cálculo de prestaciones económicas en función del coste del servicio y de la capacidad económica del beneficiario, lo que implica el tratamiento de datos económicos y patrimoniales, así como la verificación de gastos y servicios efectivamente prestados.

Las nuevas disposiciones adicionales, en particular la décima, implican el tratamiento de datos de salud de especial sensibilidad, al establecer los criterios para el reconocimiento del grado III+ de dependencia extrema, incluyendo la evaluación médica de enfermedades de alta complejidad y curso irreversible.

Asimismo, la gestión de las prestaciones, la acreditación de entidades, la formalización de convenios y la tramitación de procedimientos administrativos asociados a la aplicación de la Orden implicarán tratamientos sistemáticos y continuados de datos personales.

En la recogida y tratamiento de dichos datos deben respetarse los principios de protección de datos recogidos en el **artículo 5** del Reglamento General de Protección de Datos. A los efectos que aquí interesan, el mencionado artículo 5, en su apartado 1, se refiere a los principios de limitación de la finalidad, minimización y exactitud, limitación del plazo de conservación, e integridad y confidencialidad:

“5.1 Los datos personales serán:
(...)

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

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

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

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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

No obstante, se observa que ni el proyecto de Orden que se informa, ni la Orden de 24 de julio de 2013, del Departamento de Sanidad, Bienestar Social y Familia, objeto de modificación, contienen mención expresa alguna al Reglamento (UE) 2016/679, de 27 de abril de 2016, ni a la Ley Orgánica 3/2018, de 5 de diciembre. En este sentido, el texto proyectado no incorpora una referencia expresa a la normativa de protección de datos en relación con la confidencialidad y el tratamiento de la información personal, por lo que se considera conveniente reforzar esta previsión mediante la inclusión de una mención expresa tanto al RGPD como a la LOPDGDD.

Asimismo, se echa en falta una regulación específica relativa a las medidas de seguridad aplicables al tratamiento de datos personales y a la limitación de acceso a los mismos, conforme a lo dispuesto en los artículos 29 y 32 del citado Reglamento.

A este respecto, y en atención a la necesaria garantía de confidencialidad, debería establecerse de forma expresa que el acceso a los datos personales de las personas afectadas se encuentre limitado exclusivamente a quienes estén debidamente autorizados por el órgano responsable del tratamiento, en atención a sus funciones, en los términos previstos en el artículo 29 del Reglamento (UE) 2016/679.

En la misma línea, se considera conveniente prever expresamente la obligación de suscribir compromisos de confidencialidad por parte de todas aquellas personas que accedan a la información personal de los usuarios de los servicios. Así, cualquier persona que actúe bajo la autoridad del responsable del tratamiento y tenga acceso a datos personales no podrá tratarlos salvo que haya sido previamente autorizada y haya recibido las instrucciones correspondientes. Asimismo, el artículo 32 del Reglamento impone la necesidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento, exigencia que se ve reforzada por lo dispuesto en el artículo 28 de la Ley Orgánica 3/2018, que impone la adopción de medidas que aseguren el cumplimiento de los principios del tratamiento y el deber de confidencialidad del personal con acceso a los datos.

En conclusión, se considera necesario introducir un precepto específico sobre sometimiento a la normativa de protección de datos, garantizando el cumplimiento de sus mandatos, con el fin de garantizar la seguridad jurídica y la plena adecuación al marco normativo en materia de protección de datos, mediante una referencia expresa al RGPD y a la LOPDGDD.

Asimismo, se recomienda reforzar las previsiones relativas a la confidencialidad exigible a las personas con acceso a datos personales, limitando dicho acceso al personal debidamente autorizado, y se sugiere la inclusión de un precepto relativo a la adopción de medidas de seguridad técnicas y organizativas adecuadas al riesgo, así como a la limitación del acceso a los datos personales, en línea con lo dispuesto en la normativa vigente en materia de protección de datos.

De acuerdo con todo lo anterior, se propone la introducción de un nuevo artículo, o bien de una nueva disposición adicional, con un contenido de igual o similar tenor al siguiente:

“Las actuaciones reguladas en esta Orden se llevarán a cabo con el debido cumplimiento de 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, y de 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.

Los tratamientos de datos personales que, en su caso, pudieran derivarse de la aplicación de esta Orden se ajustarán a los principios relativos al tratamiento establecidos en el artículo 5 del citado Reglamento, 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. Del mismo modo, el responsable del tratamiento adoptará las medidas técnicas y organizativas apropiadas previstas en el artículo 32 del Reglamento 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.

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 y en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre.

Dichas medidas de seguridad, de carácter técnico y organizativo, deberán garantizar un nivel de seguridad 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.”

V

El proyecto de Orden ha sido objeto de tramitación administrativa en el seno de la Comunidad Autónoma de Aragón, habiéndose recabado diversos informes y dictámenes en el curso de su elaboración. En este contexto, resulta relevante señalar que el órgano consultivo autonómico ha considerado oportuno someter el proyecto a informe de esta Agencia Española de Protección de Datos, en la medida en que la norma proyectada incide de manera directa en el tratamiento de datos personales.

En efecto, tal y como se ha puesto de manifiesto a lo largo del presente informe, la modificación normativa proyectada comporta la realización de tratamientos de datos personales de carácter amplio y sistemático, incluyendo categorías especiales de datos, en particular los relativos a la salud de las personas en situación de dependencia, así como datos económicos y sociales necesarios para la determinación de las prestaciones.

No obstante lo anterior, y pese a la relevancia de los tratamientos previstos, no consta que en el proceso de elaboración de la Orden se haya llevado a cabo un análisis de riesgos ni una evaluación de impacto relativa a la protección de datos personales (EIPD), ni que tal circunstancia haya sido reflejada en la memoria justificativa del proyecto ni en la propia norma proyectada.

Debe recordarse, a este respecto, que el artículo 35 del Reglamento (UE) 2016/679, de 27 de abril de 2016, establece la obligación de realizar una evaluación de impacto relativa a la protección de datos cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías y teniendo en cuenta su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, supuesto que concurre claramente en el caso que nos ocupa.

Asimismo, el artículo 25 del RGPD consagra el principio de protección de datos desde el diseño y por defecto, que exige integrar las garantías necesarias en el tratamiento desde el momento mismo de la concepción de las medidas normativas que lo habilitan, teniendo en cuenta los riesgos asociados a los tratamientos previstos.

En esta línea, el artículo 35.10 del RGPD prevé expresamente la posibilidad de que, cuando el tratamiento tenga su base en una norma con rango legal o reglamentario, sea el propio órgano proponente quien lleve a cabo la evaluación de impacto en el contexto del procedimiento de elaboración normativa, integrándola en el análisis general de impacto de la disposición.

Del mismo modo, el Real Decreto 311/2022, de 3 de mayo, por el que

se regula el Esquema Nacional de Seguridad, establece que cuando un sistema de información trate datos personales, el responsable o el encargado del tratamiento deberán realizar un análisis de riesgos conforme al artículo 24 del RGPD y, en su caso, una evaluación de impacto conforme a su artículo 35, debiendo prevalecer las medidas derivadas de dichos análisis cuando resulten más exigentes.

En el presente caso, no resulta dudoso que la norma proyectada da lugar a tratamientos de datos personales que, por su naturaleza —incluyendo datos de salud—, su alcance y su carácter sistemático, pueden entrañar altos riesgos para los derechos y libertades de las personas afectadas, lo que refuerza la necesidad de haber realizado una evaluación de impacto en materia de protección de datos.

La ausencia de dicha evaluación impide identificar de forma precisa los riesgos asociados a los tratamientos previstos, así como determinar las medidas técnicas y organizativas necesarias para mitigarlos, lo que limita la posibilidad de integrar dichas garantías en el propio texto normativo, conforme exige el principio de responsabilidad proactiva recogido en el artículo 24 del RGPD.

Por ello, esta Agencia considera de especial relevancia que el órgano proponente lleve a cabo un análisis de riesgos y, en su caso, una evaluación de impacto relativa a la protección de datos, incorporándolos a la memoria justificativa del proyecto, de conformidad con lo previsto en el Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.

A su vez, se recomienda que, una vez identificados y evaluados los riesgos, las medidas y garantías necesarias para su mitigación se integren, en la medida de lo posible, en el propio texto de la norma proyectada, asegurando así el cumplimiento efectivo de los principios de protección de datos desde el diseño y por defecto.

En definitiva, la inexistencia de una evaluación de impacto en materia de protección de datos en el proceso de elaboración de la Orden constituye una carencia relevante, cuya subsanación resulta necesaria a fin de garantizar la adecuación de la norma al Reglamento (UE) 2016/679 y a la Ley Orgánica 3/2018, de 5 de diciembre, así como la efectiva protección de los derechos de las personas afectadas.

VI

Finalmente, debe señalarse que **tampoco** la Orden de 24 de julio de 2013, objeto de modificación por la norma proyectada, contiene referencia

alguna a la normativa vigente en materia de protección de datos personales ni incorpora previsiones específicas relativas a los principios, garantías o medidas de seguridad exigibles en este ámbito.

Esta ausencia resulta especialmente relevante si se tiene en cuenta que dicha norma regula de forma intensiva el acceso a prestaciones del Sistema para la Autonomía y Atención a la Dependencia, lo que comporta el tratamiento sistemático de datos personales, incluidas categorías especiales, en particular los datos relativos a la salud de las personas beneficiarias.

En este contexto, la modificación normativa objeto del presente informe constituye una oportunidad idónea para integrar de forma expresa en el texto regulador las exigencias derivadas del Reglamento (UE) 2016/679, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, incorporando los preceptos o apartados específicos a los que se ha hecho referencia en los puntos anteriores del informe.

En consecuencia, la inexistencia de una regulación previa en materia de protección de datos en la Orden que ahora se modifica refuerza la necesidad y conveniencia de introducir en la nueva redacción previsiones expresas relativas a (i) **la identificación del responsable del tratamiento**, (ii) **al debido cumplimiento de la normativa de protección de datos**, (iii) **a la limitación de acceso a los datos personales**, (iv) **a la adopción de medidas de seguridad adecuadas y la garantía de confidencialidad**, y (v) **a la realización del correspondiente análisis de riesgo y de una evaluación de impacto de protección de datos**, a fin de asegurar la plena conformidad del régimen jurídico aplicable con el marco normativo vigente en materia de protección de datos personales.