

047/2025

## I

En primer lugar, debe partirse de la naturaleza reglamentaria del proyecto informado y de la vigencia, en relación con las limitaciones al derecho fundamental de protección de datos personales, del principio de reserva de ley exigido por el artículo 53.1 de la Constitución y el artículo 8 de la LOPDGDD, que, conforme a reiterada jurisprudencia del Tribunal Constitucional, requiere, por un lado, la necesaria intervención de la *ley* para habilitar la injerencia; y, por otro lado, esa norma legal *“ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica”*, esto es, *“ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención”* (STC 49/1999, FJ 4). En otras palabras, *“no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites”* (STC 292/2000, FJ 15). Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

## II

Desde la perspectiva de la normativa de protección de datos personales, que es lo que compete a esta Agencia, y de acuerdo con la Memoria Justificativa, el texto plantea, en este aspecto, esencialmente las siguientes cuestiones.

En primer lugar, su Título I regula *“la recomendación proactiva de servicios, que se basará -continúa la Memoria- en el denominado “mapa de derechos”, cuya función será vincular rasgos, momentos vitales o estados conocidos de cada ciudadano con los derechos y prestaciones para los que es elegible”*.

En segundo lugar, el título IV se dedica a la actuación administrativa automatizada.

La Memoria añade además, con carácter general, que *“en aplicación del principio de control de los datos por la ciudadanía se establece la obligación de obtener el consentimiento expreso del interesado, también en las personas*

*jurídicas, cuando el tratamiento no esté legitimado por una autorización legal asociada al ejercicio de una competencia”.*

Esto es, y para centrar la cuestión, la norma considera que la base de licitud de los tratamientos de datos personales para las recomendaciones proactivas de servicios es el consentimiento.

### III

El Proyecto referenciado tiene por objeto, según su art. 1, *regular las medidas necesarias para la mejor prestación por medios digitales de servicios a la ciudadanía, mediante el desarrollo de los objetivos y principios de transformación digital en la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos vinculados o dependientes, especialmente a través de la sede electrónica de la Administración de la Comunidad Autónoma de Aragón, desarrollando lo dispuesto en la legislación básica estatal, en la Ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón y en la Ley 1/2021, de 11 de febrero, de simplificación administrativa.*

El proyecto ha sido objeto de una extensa tramitación administrativa, de suerte que la versión sometida a informe de esta AEPD es la versión 8, habiendo sido ya, en el seno de la Administración de la Comunidad Autónoma, informado por el Consejo Consultivo de Aragón una versión anterior (Dictamen 182/2024, de 16 de diciembre de 2024). El texto del Dictamen, entre otras circunstancias, requiere de la Administración aragonesa que someta a informe de esta AEPD el proyecto por considerar que este proyecto se refiere a tratamientos personales de datos o inciden en esta materia.

Y efectivamente, esta AEPD concuerda en que el proyecto sometido a informe incide en la materia de protección de datos personales, y se hace necesario realizar no sólo puntualizaciones a los concretos preceptos singulares, sino comentarios más generales sobre los conceptos o principios generales en que se base el proyecto de Decreto.

También se ha tenido en cuenta la información publicada por la Administración autonómica, tal y como ha requerido en su Dictamen el Consejo Consultivo de Aragón citado (apartado 60), en virtud del art. 15.1 de la Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón, que exige que los proyectos de reglamento, así como las memorias, informes, dictámenes y, en general, todos los documentos o trámites que conformen los expedientes de elaboración de los textos normativos, se pongan a disposición del público en el portal de transparencia del Gobierno de Aragón, <https://transparencia.aragon.es>. Esta

AEPD ha podido comprobar que en la dirección <https://sena.aragon.es/iniciativa/4404> consta documentación de la tramitación administrativa del proyecto.

Entre esa documentación figura el Informe de la Secretaría General Técnica del Departamento de Ciencia, Universidad y Sociedad del Conocimiento, que con acierto señala que:

*(...) como se ha ido poniendo de manifiesto en varios pasajes de este informe, hay diversas actuaciones que van a suponer la realización de operaciones que suponen tratamiento de datos personales, por ello parece conveniente la **participación de la Unidad de Protección de Datos del Gobierno de Aragón**, prevista en el artículo 12.2 del Decreto 7/2020, de 10 de febrero, del Gobierno de Aragón, sea mediante la emisión de un informe en el ámbito de las funciones que desarrolla, sea haciendo constar en la Memoria Justificativa, si así ha sido, que ha existido participación de la citada Unidad en la elaboración del proyecto.*

El apartado 56 del Dictamen del Consejo Consultivo de Aragón recoge que se dio traslado del proyecto, en cumplimiento del art. 48.3 del Texto refundido de la Ley del Presidente o Presidenta y del Gobierno de Aragón (TRLGPA), aprobado por Decreto Legislativo 1/2022, de 6 de abril, del Gobierno de Aragón, a la Unidad de Protección de Datos, pero no consta que dicha Unidad haya emitido ningún tipo de informe o realizado sugerencias o modificaciones al mismo.

Del mismo modo, en la Memoria Justificativa del proyecto consta que se han recabado informes de evaluación de impacto de género y de impacto por razón, de orientación sexual, expresión e identidad de género y de impacto por razón de discapacidad del proyecto de decreto de servicios a la ciudadanía, y se ha realizado por la Dirección General de Administración Electrónica y Sociedad de la Información un Informe contestación a los anteriores. Sin embargo, no se ha realizado ningún informe, análisis de riesgos o evaluación de impacto en materia de protección de datos (EIPD) respecto de los riesgos asociados a los tratamientos de datos, amplios, variados y que afectan de manera importante al derecho fundamental a la protección de datos, que la norma proyectada conlleva.

Es de recordar que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, de aplicación a todo el sector público (art. 2), establece que:

**1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto 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 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.*

**2. 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.**

**3. En todo caso**, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

No resulta dudoso, sino evidente del propio texto del proyecto informado, que los sistemas de información a los que se refiere el proyecto de Decreto tratan (o pueden tratar) datos personales.

Cabe recordar que el art. 25 RGPD establece la necesidad de la protección de datos “desde el diseño” de los tratamientos, y la necesidad de tener en cuenta los riesgos que se derivan de estos.

#### *Artículo 25. Protección de datos desde el diseño y por defecto*

**1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas**, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

Dicho análisis de riesgos y evaluación de impacto deberían de llevarse a cabo con la ayuda del Delegado de Protección de datos correspondiente.

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, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, -en vez de a posteriori los responsables de los tratamientos- 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 <sup>1</sup>. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en las Memorias justificativas de los proyectos normativos, (en el caso del Estado, la Memoria de Análisis de Impacto Normativo, MAIN), dentro del concepto “Otros impactos”, el análisis del *“impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”*.

*g) Otros impactos: **La memoria del análisis de impacto normativo incluirá** cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al **impacto que tendrá para la***

<sup>1</sup> Véase su mención en Memorias justificativas de proyectos normativos en Aragón por ejemplo en: <https://gd.aragon.es/cgi-bin/ITCN/BRSCGI?CMD=VEROBJ&MLKOB=1178921404242>

***ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma***

Dicho análisis de riesgos o la EIPD no parece haberse llevado a cabo por el órgano proponente del proyecto. Y esta Agencia considera de la mayor importancia en una norma como la proyectada la realización de un análisis de riesgos y la evaluación de los impactos en materia de protección de datos que resulten en una norma como la proyectada, pues precisamente el objeto central de la norma, no meramente indirecta o derivada, es establecer esos medios y servicios por la Administración digital, que conlleva tratamientos automatizados, predictivos y perfilados de los ciudadanos.

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), análisis de riesgos y evaluación de impactos en protección de datos que, al no haberse realizado, o no constar haberlos realizados, no puede saberse si las medidas a implantar serían o no las correctas.

En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la Memoria justificativa del proyecto el análisis de riesgos (art. 24 y 25 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), que con carácter obligatorio, como resulta del art. 35.3 RGPD, habrá de realizarse por los responsables de los tratamientos, al prever la norma proyectada tratamientos automatizados de datos personales, lo que incluye, pero no agota la materia, *“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”*, como resulta del art. 35.3.a) RGPD, y sin descartarse tampoco, pues resulta del texto proyectado que podrían tratarse datos de categorías especiales, que concurriera un *“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”*, como establece el art. 35.3.b) RGPD. Ello permitirá 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 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 en la norma se recogen 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 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, 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.

Desde un punto de vista práctico, esta Agencia ha publicado su **Guía** denominada **“Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”**<sup>2</sup>, que tienen como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas normativas de las Administraciones Públicas implican el tratamiento de datos personales. Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el RGPD, así como 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 (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

En esta “Guía” se contienen, con profundidad y rigor, los pasos o el método a seguir para determinar la necesidad y el contenido de la Evaluación de Impacto, y entre ellos esta AEPD desea resaltar en este momento el

<sup>2</sup> <https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>

apartado D del epígrafe II del mismo, relativo a las características de la norma que ampara el tratamiento:

***Toda medida legislativa que habilite un tratamiento debe cumplir con la premisa de “previsto en la ley”. Esto implica que debe ser clara y precisa, y su aplicación accesible y previsible para sus destinatarios, de conformidad con el TEDH, el TJUE y el Tribunal Constitucional (TC). Por lo tanto, en la norma han de estar claramente definidos, con precisión y apropiadamente:***

1.- La finalidad o finalidades del tratamiento.

2.- La legitimidad del tratamiento.

3.- La descripción de la implementación del tratamiento en sus aspectos relevantes, como pueden las operaciones y los procedimientos determinantes del tratamiento (por ejemplo, recogida, almacenamiento, acceso, transmisión, difusión,...), las tecnologías planteadas para implementar las operaciones (inteligencia artificial, almacenamiento en Nube, biometría, IoT, móviles, videovigilancia,...), la existencia de decisiones automatizadas, así como la participación o posible participación de encargados y/o subencargados en distintas operaciones del tratamiento, entre otros.

4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las categorías de interesados afectados, las circunstancias en las que se utiliza la información personal (por ejemplo: de forma sistemática, solo en determinados casos, durante un periodo de tiempo limitado, etc.), los plazos de conservación de los datos, la frecuencia de recogida de datos, la granularidad de los datos y otros factores que definan el alcance del tratamiento.

5.- Los responsables/corresponsables o categorías de responsables y, en su caso, los encargados o categorías de encargos y/o de subencargados.

6.- Las entidades que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación, en particular, las condiciones de la **comunicación de datos entre autoridades públicas en virtud de una obligación legal** para el ejercicio de una misión oficial según las condiciones del RGPD (Cons. 31):

- En el marco de una investigación concreta.
- De interés general.



- *De conformidad con el Derecho de la Unión o de los Estados miembros.*
- *Por escrito y de forma motivada.*
- *Con carácter ocasional.*
- *No deben referirse a la totalidad de un fichero.*
- *No deben dar lugar a la interconexión de varios ficheros.*

*7.- La justificación de la solución adoptada para el acceso a datos personales, teniendo en cuenta que supone la utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.*

*8.- Las **medidas para garantizar un tratamiento lícito y equitativo, habida cuenta de la naturaleza, alcance (especialmente con relación a las categorías especiales de datos), contexto y finalidades del tratamiento** o de las categorías de tratamientos, los mecanismos de información y transparencia, así como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX del RGPD, en particular, aquellas orientadas a evitar los accesos o las transferencias de datos ilícitos o abusivos.*

*9.- En el caso de limitación por ley de derechos u obligaciones al amparo de los arts. 23 del RGPD o 24 de la L.O. 7/2021, debe estar muy clara su determinación, las condiciones específicas de limitación de las obligaciones y derechos (Cons. 19 del RGPD), y los perjuicios concretos a la consecución de los fines que justifican la falta de información a los interesados sobre la limitación. La lista anterior no es exhaustiva, sino que cualquier otra disposición pertinente, para cada caso concreto, debería incluirse en la descripción del tratamiento.*

#### IV

El art. 5 del proyecto, desde la perspectiva de la normativa de protección de datos personales, establece un sistema de información (sistema de relación con la ciudadanía compartido), gestionado por un órgano administrativo (el departamento competente en materia de administración electrónica) cuyo personal (las personas dedicadas a la atención de la ciudadanía) llevarán a cabo tratamientos de datos (accederán) sobre los datos de tramitación de expedientes que obren en la Plataforma de Gobernanza de Datos (que son todos, de toda la Administración y de todos los servicios, apartado 5). Ello, con la finalidad, según parece resultar de la norma, para informar a los interesados del estado de tramitación de sus procedimientos.

Pero no sólo, sino que conforme al art. 6 y concordantes del proyecto, ello parece comportar que los órganos responsables de los diferentes servicios, cuando consideren que una determinada persona puede beneficiarse de un servicio -se supone porque conoce las necesidades de esa persona por haber conocido datos personales de ella al “tratarse de forma unificada la información de cada persona” ex art. 6.2 del proyecto- se lo comunicará y, si desea acceder al mismo, le facilitará dicho acceso (...). En definitiva, la Administración tiene conocimiento completo, íntegro, de las circunstancias de una persona -sin excluir datos de salud, por ejemplo – y en base a dicho conocimiento exhaustivo (“ciudadanos de cristal”) le ofrece otros servicios que es posible que no conozca, pero por otro lado que puede que ni siquiera desee, o que ni desee que sus datos sean conocidos por quienes no son destinatarios de la finalidad para la que fueron recogidos inicialmente.

La norma proyectada, al establecer la base de licitud de los tratamientos de datos personales que conlleva, apela en primer lugar al “consentimiento informado” del interesado, y en segundo lugar a que todo ello se habrá realizado “de acuerdo con lo establecido en la normativa reguladora de la protección de datos personales”; y además en el consentimiento, se añade, se incluirá la autorización para realizar operaciones de perfilado con la finalidad descrita (art. 6.2, in fine, en relación con el apartado 6.3 del proyecto).

A este respecto cabe exponer, en primer lugar, que se utiliza reiteradamente en la norma las expresiones “*en todo caso, de acuerdo con la normativa vigente en materia de protección de datos de carácter personal*” o similares, como una suerte de fórmula curativa de los posibles defectos que la regulación pudiera tener. Lo que la normativa de protección de datos de carácter personal en realidad requiere es que la norma que establezca los tratamientos contenga los requisitos necesarios para que estos, los tratamientos de datos personales, sean acordes a dicha normativa y salvaguarden el derecho fundamental a la protección de datos de los interesados. En consecuencia, dicha apelación genérica a la normativa de protección de datos personales cabe considerarla, en general, vacía de contenido, porque ya esté presente o no en la norma dicha admonición (*de acuerdo con lo establecido en la normativa reguladora de la protección de datos personales*), los tratamientos que resulten de la norma habrán de cumplir, por supuesto, la normativa sobre protección de datos personales.

Ya más en concreto, el art. 6.2 de la norma proyectada requiere el *consentimiento informado* del interesado. Sin perjuicio de que pueda ser necesario dicho consentimiento para poner en marcha un determinado procedimiento administrativo, la base jurídica del tratamiento de datos personales por la Administración no es, en general, el consentimiento del interesado. El Considerando (43) RGPD dice así:

*Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.*

Como punto de partida, por lo tanto, para el RGPD, el consentimiento no opera como base general del tratamiento de datos personales por las autoridades públicas, al existir normalmente una relación de poder entre la autoridad pública y el interesado/ciudadano que determina que ese consentimiento no pueda ser considerado “libre” en los términos del art. 4.11 RGPD y del Considerando 43 citado; esto es, que se trate de un consentimiento “libre, específico, informado e inequívoco”, y, además, cuando se traten datos personales mediante decisiones individuales automatizadas, incluida la elaboración de perfiles, ese consentimiento sea “explícito” (art. 22.2.c) RGPD). En estos casos, será necesario otra base de licitud de los tratamientos, que el RGPD contempla en el art. 6.1.c) o 6.1.e), esto es, será necesaria en general una habilitación legal basada en el interés público o en el ejercicio de potestades públicas.

Ahora bien, aunque no sea “probable”, en términos del considerando antes transcrito, no hay que excluir que cuando el ciudadano dispone de una libertad real y efectiva de optar, sin consecuencia negativa alguna, pueda considerarse que la base jurídica del tratamiento de datos personales pueda ser el consentimiento del art. 6.1.a) RGPD.

Así lo reconoce, por otra parte, el Comité Europeo de Protección de Datos (CEPD) en sus Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión 1.1, adoptadas el 4 de mayo de 2020. En concreto, en sus apartados 16 y 17:

*16. El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El CEPD considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.*

*17. Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por*

*parte de las autoridades públicas **no queda totalmente excluido en virtud del marco jurídico del RGPD.** (...)*

Y cita a continuación ejemplos que muestran que el uso del consentimiento puede ser adecuado en determinadas circunstancias.

Así las cosas, podría partirse de la hipótesis de que el consentimiento tenga lugar para *servicios adicionales* como los de personalización, que no son estrictamente necesarios para el ejercicio de la función administrativa. Ahora bien, cuando para prestar estos servicios se requiere un tratamiento masivo e intensivo de datos, e incluso suponen un tratamiento automatizado, procede exigir una base de rango legal. Cuando esos servicios de personalización impliquen un tratamiento de datos personales que pasa a ser estructural, necesario y ofertado como parte del funcionamiento ordinario del servicio público, la cobertura debe venir de una norma con rango de ley. En estos casos un reglamento -como es el caso- no es suficiente, porque se están definiendo finalidades de tratamiento y modulando la base del artículo 6.1 e) RGPD, lo que exige habilitación legal conforme al artículo 6.3 RGPD y al artículo 8.2 LOPDGGD

Asimismo, debe entenderse que cuando un servicio administrativo de personalización se integra de forma estructural y generalizada en el funcionamiento ordinario de una Administración, dejaría de ser adecuada la utilización del consentimiento del ciudadano como base de legitimación. En ese contexto se debilita, cuando no desaparece, la libertad real de elección, en la medida en que la negativa a consentir puede comportar consecuencias relevantes, directas o indirectas, en el acceso, la calidad o la eficacia del servicio. En tales condiciones, resulta difícil sostener que se trate de un servicio meramente añadido o prescindible, que sí que permitiría la legitimación por el consentimiento, sino que también procede reconducir su cobertura al marco del interés público con base legal suficiente.

Para que el consentimiento pueda ser considerado libre, por lo tanto, el interesado debería poder *optar* por recibir la información sobre los servicios de forma no personalizada, fácil, accesible y comprensible, lo que conlleva que la Administración habría de publicar esa misma información, en canales igualmente accesibles, y en su integridad, de manera no “personalizada” pero informativa, del mismo modo que podría acceder a ella cualquier persona que accediese a ser objeto de un tratamiento “predictivo” o “personalizado”. Es decir, si existiese disimetría o menor facilidad de acceso, o coste o esfuerzo, entre acceder a la información personalizada por quien ha accedido a ser “perfilado” que por quien ha decidido libremente no serlo, entonces ese consentimiento no sería libre, por no gozar el interesado de verdadera o libre elección o porque no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (Considerando 42 RGPD).

## V

En cualquier caso, el art. 6.1 RGPD tan sólo requiere para que exista un tratamiento lícito de datos personales que se cumpla “al menos una” de las condiciones de este. Esto significa, en primer lugar, que basta la existencia de una de ellas para que el tratamiento de datos sea lícito. Por supuesto, si cumple además todos los principios del tratamiento del art. 5; (véase, por todas, STJUE de 13 de marzo de 2025, C-247/23, Deldits, apartado 28:

*todo tratamiento de datos personales debe, en particular, cumplir los principios relativos al tratamiento de dichos datos establecidos en el artículo 5 del RGPD, (...) y satisfacer las condiciones de licitud enumeradas en el artículo 6 de dicho Reglamento (véase, en este sentido, la sentencia de 9 de enero de 2025, Association Mousse, C-394/23, EU:C:2025:2, apartado 22 y jurisprudencia citada).*

Pero, además, en segundo lugar, que no cabe descartar que existan dos bases jurídicas que den cobertura a un mismo tratamiento (norma legal y consentimiento), si se dieran todas las condiciones para ello.

De todas maneras, y conforme al principio de responsabilidad proactiva que rige en el RGPD (art. 5.2, 24, 32), corresponde al responsable del tratamiento (en este caso, la Administración autonómica) cumplir con lo dispuesto en el Reglamento, y ser capaz de demostrarlo. Y particularmente si el responsable descansa en la base de licitud del consentimiento, corresponde la responsable demostrar a la autoridad de control que el interesado consintió el tratamiento de sus datos personales, y que dicho consentimiento cumple los requisitos del art. 4.11 RGPD.

En cuanto a la base de licitud de los artículos 6.1.c) o e) RGPD, sólo puede venir establecida en una *ley*, y que reúna los requisitos que la jurisprudencia del Tribunal Constitucional y del TJUE establece. El art. LOPDGDD dice:

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

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

*de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.*

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

Se requiere, en definitiva, de una competencia atribuida por una norma con rango de ley, y, en consecuencia, la norma proyectada ahora informada carecería de rango normativo suficiente. No se considera, por otra parte, que los arts. 44.3 o 50.3 de la ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón cumplan íntegramente esta función, y mucho menos cuando se podrían tratar, de acuerdo con ellas, incluso datos de categorías especiales para el perfilado o los tratamientos automatizados. Véanse las STC 292/2000 o STC 76/2019, entre otras.

Estos preceptos citados de la ley de Aragón 5/2021 dicen:

*Artículo 44. Dato único y compartido.*

*1. Los titulares de los órganos administrativos son los responsables de la gestión de la información que sirve de base a la toma de decisiones o a la actuación administrativa sea automatizada o individualizada.*

*2. Los datos incluidos en las bases de datos de la Administración pública de la Comunidad Autónoma de Aragón serán considerados como válidos a efectos de la actuación administrativa automatizada y de la provisión de información pública. A estos efectos, los órganos responsables de los procedimientos administrativos serán responsables de la integridad, veracidad y exactitud de los datos que obren en sus bases de datos.*

*3. **El departamento con competencias en administración electrónica establecerá los criterios** necesarios para la consecución del objetivo de **dato único y compartido en la Administración pública de la Comunidad Autónoma de Aragón** que conlleva que la información se introduzca una sola vez en origen, se mantenga depurada y actualizada por los órganos responsables, **y se pueda gestionar o consultar desde cualquier punto o sistema que así lo requiera en las condiciones que se establezcan reglamentariamente***



***y, en todo caso, de acuerdo con la normativa vigente en materia de seguridad y protección de datos de carácter personal.***

*4. En todo caso, los órganos de la Administración pública de la Comunidad Autónoma de Aragón deberán poner a disposición sus datos para su verificación y consulta a través del mismo Servicio de Consulta y Verificación de Datos o herramienta corporativa equivalente gestionada por el departamento con competencias en materia de administración electrónica que garantiza la integración con la plataforma de intermediación estatal.*

*Artículo 50. Racionalización de los procedimientos.*

*1. Los Departamentos de la Administración de la Comunidad Autónoma y sus organismos públicos serán responsables de la racionalización y agilización de los procedimientos administrativos y de las actividades materiales de gestión. El departamento competente en materia de administración electrónica propondrá criterios para la racionalización de los procedimientos administrativos electrónicos que faciliten la prestación de servicios a la ciudadanía.*

*2. El departamento competente en materia de administración electrónica instará la revisión de los procedimientos administrativos con objeto de homogeneizar trámites dentro de los mismos y de modificar las peticiones de identificación a las y los ciudadanos así como las peticiones de documentación que no se consideren necesarias para la prestación de los servicios.*

***3. El departamento con competencias en materia de administración electrónica definirá las condiciones necesarias para que se puedan incorporar a la prestación de servicios tratamientos automatizados de datos que tengan por finalidad ofrecer de forma proactiva servicios adaptados a las necesidades de las personas, empresas o entidades interesadas de acuerdo con las condiciones establecidas en la normativa de protección de datos personales.***

## VI

La apelación al consentimiento en el proyecto informado a los efectos de la oferta de servicios predictivos se realiza en términos amplios, sin referencia

al **principio de limitación de la finalidad** (art. 5.1.b) RGPD) -véase al respecto el art. 14.6 del proyecto- de manera que los interesados no conocerían con claridad y precisión su aplicación previsible (Considerando 4.1 RGPD) a otras finalidades distintas de las iniciales para las que se requirieron los datos personales, lo que sobrepasaría el principio de limitación de la finalidad.

Estas expectativas que puede tener el afectado respecto al tratamiento de su información personal para finalidades diferentes, podrían incluir, en principio, la recepción de información relacionada con el trámite o servicio realizado, pero no necesariamente la recepción de información referida a cualquier otro trámite o servicio, diferente o alejado, que le pueda ofrecer cualquier Administración pública a partir de un análisis predictivo de la información que habrá facilitado a una determinada Administración.

Además, el consentimiento ha de ser **específico**. Es decir, el ciudadano debe conocer con un nivel de concreción suficiente a lo que está consintiendo, de forma que pueda prever las consecuencias de dicho consentimiento. En el proyecto no queda suficientemente claro ni el origen de la información que se utilizará para tratar sus datos y ofrecerle nuevos servicios personalizados (parecería que el origen puede ser la información tratada en cualquier área privada y por parte de cualquier administración), ni cuáles serán los aspectos que se analizarán en partir de su información personal, ya que el proyecto permite una enorme amplitud.

El art. 6 del proyecto dice así:

*Artículo 6. Recomendación proactiva de servicios a la ciudadanía.*

*1. Cuando el órgano responsable de **un servicio** de la Administración de la Comunidad Autónoma y sus organismos públicos considere que una determinada persona puede beneficiarse del mismo de forma que suponga para ella una ventaja o prestación directa, se lo comunicará y, si desea acceder al mismo, le facilitará dicho acceso ofreciéndole los trámites ya cumplimentados en la medida de lo posible. Estas recomendaciones se recordarán periódicamente **y se practicarán en todos los canales de acceso a los servicios y, especialmente, a través del espacio personal de relación con la ciudadanía.***

*2. Para la identificación de los supuestos previstos en el apartado anterior **se tratará de forma unificada la información de cada persona interesada, previo el consentimiento informado de la misma y de acuerdo con lo establecido en la normativa reguladora de la protección de datos personales, en el cual se incluirá la autorización para realizar operaciones de perfilado con la finalidad descrita.***

*3. El departamento competente en materia de administración electrónica gestionará los **perfiles únicos y compartidos de los interesados y, con la colaboración del conjunto de los diferentes órganos y unidades gestoras de los servicios, elaborará un mapa de derechos que servirá de base para los protocolos y prácticas de descubrimiento y recomendación de servicios.***

Tal y como está formulado el texto, resultará muy difícil para el ciudadano poder prever el alcance de su consentimiento, especialmente si en la elaboración de posibles perfiles, se emplean técnicas de inteligencia artificial (véase art. 52 del proyecto). Si la persona afectada no puede conocer qué aspectos de su vida van a ser evaluados en cada caso, para qué ámbito material o por parte de qué Administración pública, difícilmente el consentimiento será una base jurídica viable para el tratamiento. **Por el contrario, si todos estos aspectos son claros, y el afectado tiene la información adecuada y previa al tratamiento, y puede comprender el alcance de la prestación de su consentimiento, éste sí podría ser viable,** como ya se ha expuesto. No lo sería si se pretende utilizar esta habilitación para recoger cualquier tipo de información sobre esta persona que se encuentre en poder de cualquier otra administración.

Por exigencia del principio de limitación de la finalidad (art.5.1.b) RGPD), el proyecto debería concretar que las finalidades para las que se utilizará la información están relacionadas con aquella finalidad para la que se ha recogido la información inicial sometida a evaluación y que, además, serán compatibles con la finalidad para la que se recogió.

No parece compatible con este principio una redacción según la cual los datos en poder de una Administración puedan acabar siendo utilizadas por cualquier otra Administración para elaborar perfiles de todos los ciudadanos que se relacionan con estas Administraciones, con el fin de ofrecer servicios personalizados desvinculados del servicio inicialmente prestado.

Habría que tener en cuenta pues, caso por caso, los criterios establecidos en el artículo 6.4 RGPD para determinar la viabilidad del tratamiento. Recordemos asimismo que el artículo 6.3 RGPD también prevé que esta norma pueda contener otras previsiones tales como las condiciones generales que rigen la licitud, los tipos de datos objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos y la finalidad de la comunicación, la limitación de la finalidad, así como, entre otros, las medidas para garantizar un tratamiento lícito y equitativo.

Por otro lado, no cabe olvidar que los interesados tienen derechos a ser **informados** de la finalidad para las que va a ser tratados los datos personales que se les requieren en los distintos procedimientos, así como de quiénes van a ser los distintos destinatarios de estos (arts. 13 y 14 RGPD, en especial

apartado 1, letra e)). Ello incluye también los tratamientos por las autoridades públicas (véase STJUE 1 octubre 2015, C-201/14, Smaranda Bara)

En definitiva, y en lo que respecta a estos apartados, no es lo mismo que el interesado tenga un control sobre sus datos personales de manera que la Administración ponga a su disposición un sistema de acceso centralizado para que el interesado pueda acceder a dichos datos desde un único lugar (“espacio personal de relación electrónica con la ciudadanía” según art. 5.3 del proyecto de Decreto), que el que cualquier órgano de la Administración, por el hecho de que existe un sistema que permite agrupar dicha información para el interesado, pueda tener acceso a cualesquiera datos personales de dicho interesado (esto es, incluso a datos personales en procedimientos que están fuera de sus competencias o potestades establecidas en una norma con rango de ley), tal y como parece resultar del apartado 5 del art. 5 del proyecto, según el cual: *[t]odos los órganos instructores o gestores de expedientes administrativos deberán compartir en la Plataforma de Gobernanza de Datos el estado de tramitación de los servicios y sus datos de contacto, por medio de los cuales facilitarán, con las limitaciones que imponga el ordenamiento jurídico, información funcional de los servicios de los que sean responsables.* Precepto éste que parece estar redactado para permitir, no al interesado exclusivamente el control sobre sus datos y procedimientos en los que sea parte, sino para que cualesquiera órganos de la Administración puedan tener acceso y conocimiento de dichos datos, lo que incurriría en los defectos respecto de la normativa de protección de datos personales que hemos expuesto. Lo mismo cabe reseñar respecto del art. 63 del proyecto, Intercambio de datos, según el cual a través de la plataforma de Gobernanza de Datos los responsables de los tratamientos (gestores de los procedimientos administrativos) deberán compartir los datos de las personas, a la mayor brevedad y conforme al modelo de datos único (...).

Se trata, en definitiva, de un nuevo modelo de gestión de los datos personales, novedoso, pero no por ello habrán de incumplirse los preceptos de la normativa de protección de datos

Cabe mencionar en este punto, a título de mero ejemplo comparado, la muy reciente modificación por la Ley 9/2025, de 13 de noviembre (DOGC de 14.11.2025), de la Ley 26/2010, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, para adicionar un art. 40 bis, para dar cabida en una norma legal (superando la regulación meramente reglamentaria del Decreto 76/2020, de 4 de agosto, de Administración Digital) tanto para dar cabida a los servicios personalizados en la ley como para, que es el objetivo de este comentario, establecer límites a, y la necesidad de, que dichos servicios cuenten, una vez establecidos en la ley, con el consentimiento del interesado y este consentimiento reúna los requisitos previstos en la normativa de protección de datos.

Se recogen aquí los apartados 3, 4 y 5 de dicho art. 40 bis:

3. *La prestación de servicios proactivos y personalizados requiere el consentimiento expreso y específico, informado e inequívoco de la persona interesada. Este **consentimiento** debe otorgarse de forma **libre y específica para cada servicio, indicando clara y detalladamente los datos a tratar y la finalidad concreta del tratamiento**. Para cumplir el carácter específico e informado del consentimiento, **la descripción del servicio de que se trate debe ser lo suficientemente detallada** para permitir a la persona decidir las condiciones de perfilado de su persona para el ofrecimiento de este. No se permiten descripciones genéricas o globales, ni consentimientos generales o indefinidos.*

4. ***Antes** de obtener el consentimiento para la prestación de servicios proactivos y personalizados, debe **informarse a las personas afectadas de todos los aspectos** que requiere la normativa de protección de datos, especialmente sobre la **elaboración de perfiles, la lógica aplicada y las consecuencias que pueden derivarse**.*

5. *Las personas afectadas por la prestación de servicios proactivos y personalizados **deben poder revocar en cualquier momento** los consentimientos mediante un sistema fácilmente accesible y, si procede, rectificar los datos que sean inexactos o estén desactualizados.*

## VII

Del mismo modo, y como continuación de la regulación que acabamos de mencionar en el art. 5 del proyecto, el art. 6 del proyecto, así como el posterior art. 63, inciden en la posibilidad de que se someta a los interesados a un perfilado a los efectos de ofrecerles servicios de manera predictiva. Esto es, la norma prevé que todos los ciudadanos de la Comunidad Autónoma -pues todos los ciudadanos tienen relaciones de uno u otro tipo con la Administración autonómica- estén sujetos a un tratamiento de perfilado.

El art. 22 del RGPD regula este aspecto:

*Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles*

1. *Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.*

*2. El apartado 1 no se aplicará si la decisión:*

*a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;*

*b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o*

*c) se basa en el consentimiento explícito del interesado.*

*3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.*

*4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*

A lo que cabe añadir el derecho de oposición genérico a que se refiere el art. 21.1 RGPD, que incluye tratamientos de datos por la Administración conforme al art. 6.1.f) RGPD:

*1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.*

La norma proyectada, en su Capítulo III, regula la actuación administrativa automatizada.

En el art. 52.2, letras b) y c), la redacción del ámbito de aplicación del capítulo es en exceso ambigua, pues se utilizan términos como “*su posible complejidad o posible impacto en derechos fundamentales [...] así lo justifique*”,



el “alto grado de automatización y la decisión o decisiones adoptadas puedan verse condicionadas por la información aportada por los sistemas utilizados con una intensidad que así lo justifique”, que pueden dar lugar a una inseguridad jurídica para los ciudadanos que no pueden determinar con certeza la normativa que regirá los tratamientos de sus datos personales en estos casos, o su alcance. En cualquier caso, el RGPD no distingue en el art. 22 en cuanto a los tratamientos de especial, o no especial, complejidad, sino que su regulación se aplica a todos los tratamientos de datos personales.

El art. 54 del proyecto regula las “*garantías de los derechos de las personas en las decisiones individuales automatizadas*”. El apartado 2, que trata de recoger las excepciones previstas en el art. 22.2 RGPD, no se comparte, por cuanto ni el apartado a) ni el c) serían aplicables a la actividad administrativa, ya que la base jurídica de sus tratamientos de datos personales (incluso cuando se trate de la ejecución de un contrato, ya administrativo o privado -véase la Ley 9/2017, de 8 de noviembre, de contratos del sector público, o Informe de esta AEPD 175/2018) requiere una norma legal, ni el consentimiento es aplicable como base jurídica, con carácter general, si hay una situación de desequilibrio entre las partes, como ya hemos expuesto anteriormente, para el tratamiento de datos por la autoridades públicas.

El apartado 3 del art. 54 se refiere a la posibilidad de utilizar categorías especiales de datos para llevar a cabo decisiones individuales automatizadas, pero ya hemos reiterado que el consentimiento no es base jurídica lícita en los tratamientos de datos personales por la Administración cuando existe ese desequilibrio entre las partes. Para evitar reiteraciones innecesarias, esta afirmación ha de entenderse extensible a todos los supuestos en que la norma proyectada prevé dicho consentimiento como base de licitud de los tratamientos de datos, como pueda ser, por ejemplo, el art. 14.6 o el art. 20.2.b), o específicamente el art. 61.2 o 61.3 del proyecto.

Por otra parte, y en cualquier caso, el art. 9.1 LOPDGDD impide que el *solo* consentimiento del afectado baste para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, también a estos efectos.

Y en cuanto a la mención al “interés público esencial”, se considera que debería de redactarse reflejando de manera más fiel el texto del RGPD, por ejemplo, “*(...) en los casos en que conforme al art. 9.2.g) RGPD el tratamiento sea necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de una ley nacional, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado*”.

No puede olvidarse, además, lo que debería de tener reflejo en la norma, que los interesados tienen un específico derecho a ser informados también en estos casos. Cuando en el tratamiento existen decisiones individuales automatizadas el RGPD refuerza el derecho de información de los interesados y establece la obligación de que el responsable del tratamiento informe específicamente sobre estas, sobre la información significativa de la lógica aplicada, así como la importancia y las consecuencias prevista de dicho tratamiento para el interesado (arts. 13, 14 y 15 RGPD). Asimismo, el art. 11.1, último inciso, de la LOPDGDD, regula la información a suministrar al interesado cuando sus datos fueran a ser tratados para la elaboración de perfiles. Si el interesado no dispone de la información que por derecho propio le corresponde, no podrá oponerse a dicho tratamiento (art. 21 de la LOPDGDD) cercenando en última instancia su poder de disposición y control en relación con los datos personales que le conciernen.

El considerando 71 del RGPD establece sobre las decisiones individuales automatizadas, incluyendo que,

*“71. (...) En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor”.*

En este sentido, las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 adoptadas el 29 de noviembre de 2017, revisadas por última vez y adoptadas el 11 de abril de 2018, del Grupo de Trabajo del artículo 29, establecen que,

*“41. La información sobre la existencia de decisiones automatizadas, **incluida la elaboración de perfiles**, tal como se menciona en el artículo 22, apartados 1 y 4, junto con información significativa sobre la lógica subyacente y las consecuencias notables y previstas del tratamiento para el interesado, forma parte de la información obligatoria que debe facilitarse a un interesado en virtud del artículo 13, apartado 2, letra f), y del artículo 14, apartado 2, letra g). El GT29 ha elaborado directrices sobre las decisiones automatizadas individuales y la elaboración de perfiles que deben consultarse para obtener orientación adicional sobre cómo poner en práctica la transparencia en las circunstancias concretas de la elaboración de perfiles. Cabe señalar que, además de los requisitos de transparencia específicos aplicables a las decisiones automatizadas en virtud del artículo 13, apartado 2, letra f), y el artículo 14, apartado 2, letra g), las observaciones en dichas directrices relativas a la importancia de informar a los interesados de las consecuencias del tratamiento de sus datos personales, y el principio general de que los interesados no deben verse sorprendidos por el tratamiento de sus*

*datos personales, se aplican igualmente a la elaboración de perfiles en términos generales (no solo a la elaboración de perfiles mencionada en el artículo 22), como un tipo de tratamiento". (el subrayado es nuestro)*

Así, las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018, del Grupo de Trabajo del Artículo 29 disponen, como expresión del principio de lealtad, transparencia y responsabilidad proactiva, que,

*“Teniendo en cuenta el principio básico de transparencia que sustenta el RGPD, los responsables del tratamiento deben garantizar que explican a las personas de forma clara y sencilla el funcionamiento de la elaboración de perfiles o las decisiones automatizadas...”*

La sentencia del TJUE de 27 de febrero de 2025, en el asunto C-203/22, señala, respecto a qué comprende suministrar información significativa sobre la lógica aplicada en las decisiones automatizadas, indica que,

*“56 En efecto, si las personas afectadas por una decisión automatizada, incluida la elaboración de perfiles, no pudieran comprender las razones que llevaron a tal decisión antes de expresar su punto de vista o de impugnarla, esos derechos no podrían, por tanto, cumplir plenamente su finalidad de proteger a esas personas contra los riesgos específicos para sus derechos y libertades que supone el tratamiento automatizado de sus datos personales [véase, en este sentido, la sentencia de 7 de diciembre de 2023, SCHUFA Holding y otros (Scoring), C-634/21, EU:C:2023:957, apartado 57].*