Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

ORIENTACIONES PARA EL ANÁLISIS DEL IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES DE LOS PROYECTOS DE DISPOSICIONES NORMATIVAS

versión 1.0 junio 2024

Índice

1. INTRODUCCIÓN

El desarrollo de la normativa en materia de protección de datos o la previsión o determinación de un tratamiento de datos personales en una disposición normativa pueden suponer una limitación al derecho fundamental a la protección de datos personales. Dicha limitación debe ser analizada de forma sistemática para garantizar el cumplimiento de la norma con el marco regulatorio en protección de datos[1].

La aplicación del principio de protección de datos desde el diseño recogido en el artículo 25 RGPD en el ámbito de la elaboración de disposiciones normativas convierte en especialmente relevante la necesidad de que en los mismos se contemple un adecuado análisis de los tratamientos de los datos personales, incluyendo las previsiones y garantías que exige la normativa sobre protección de datos. Dicho análisis, junto con el informe preceptivo emitido por la Comisión Consultiva del Consejo de Transparencia y Protección de Datos de Andalucía, en los casos en que corresponda, conformarían una "Memoria relativa a la protección de datos" que, bien como documento autónomo o bien integrado en la "Memoria de Análisis de Impacto Normativo", debería formar parte de la documentación necesaria para la aprobación de la norma.

La presente guía[2] proporciona orientaciones para realizar el análisis del impacto en la protección de datos personales (AIPD) en los proyectos de disposiciones normativas[3].

2. ANÁLISIS DEL IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES DE LOS PROYECTOS DE DISPOSICIONES NORMATIVAS

Con carácter general, consideraremos que una disposición normativa puede afectar al derecho fundamental a la protección de datos cuando prevea o determine un tratamiento de datos personales.

Además, consideraremos que existe dicha afección cuando desarrolle normas de protección de los datos personales o cuando regule medidas para garantizar el cumplimiento de la normas de protección de datos. Será así, entre otros supuestos, cuando la norma especifique, complete o limite derechos relativos a la protección de datos de los interesados, obligaciones de los responsables del

1 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

2 Su contenido se basa en el documento «Orientaciones de la Agencia Española de Protección de Datos (AEPD) para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo» disponible en: https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf

3 En el proceso de validación del análisis diseñado se ha contado con las valiosas aportaciones de los DPDs de la ATRIAN y de la Generalitat Valenciana.

tratamiento o modifique el marco competencial de la autoridad de control en materia de protección de datos.

Para el análisis del impacto en la protección de datos personales de los proyectos de disposiciones normativas:

- Debe asegurarse la participación y el asesoramiento del Delegado de Protección de Datos (DPD) desde el principio del proceso de elaboración de la norma y en el proceso de verificación necesario para la elaboración del análisis del impacto.
- Debe realizarse un análisis del impacto en la protección de datos personales, en los términos establecidos en las presentes orientaciones.
- Debe solicitarse informe preceptivo, con carácter previo a su aprobación, a la Comisión Consultiva del Consejo de Transparencia y Protección de Datos de Andalucía (en adelante el Consejo)[4].

2.1 Procedimiento de análisis. Esquema general.

Paso 1	Identificar responsable de la elaboración del AIPD	**En todo caso**
Paso 2	Identificar al DPD y el alcance de su intervención	**En todo caso**
Paso 3	Verificar la previsión de tratamiento de datos personales en la norma o como consecuencia de su aplicación	**En todo caso**
Paso 4	Verificar que la norma incluye los elementos del tratamiento necesarios en materia de protección de datos	**Sólo si se prevé o contempla un tratamiento de datos personales**
Paso 5	Validar que los tratamientos están previstos en la ley y la finalidad legítima de los mismos	
Paso 6	Evaluar la necesidad y proporcionalidad de los tratamientos	
Paso 7	Analizar los riesgos de los tratamientos para los derechos y libertades de la personas	
Paso 8	Verificar la existencia de medidas apropiadas para garantizar que los tratamientos son conformes con la normativa de protección de datos	
Paso 9	Verificar la coherencia jurídica de la norma con el marco regulatorio en protección de datos	**En todo caso**

4 Art. 15.1.d) de los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA), aprobados por Decreto 434/2015, de 29 de septiembre.

Si la norma prevé o determina un tratamiento de datos personales será necesario analizar el impacto en la protección de datos personales completando todos los pasos **(del 1 al 9)**.

Si la norma no prevé o contempla dicho tratamiento se completarán los pasos **1, 2, 3 y 9**.

2.2 Documentar el análisis del impacto en la protección de datos personales.

El análisis realizado deberá quedar oportunamente documentado. Para ello se recomienda seguir el modelo de análisis de impacto en la protección de datos personales anexo a las presentes orientaciones.

2.3 Solicitud de informe preceptivo a la Comisión Consultiva del Consejo.

De conformidad con sus Estatutos, deberá solicitarse preceptivamente informe a la Comisión Consultiva del Consejo sobre los anteproyectos de leyes y proyectos de disposiciones generales que afecten a la materia de protección de datos.

3. PROCEDIMIENTO DE ANÁLISIS DEL IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

Constaría de los siguientes pasos;

Paso 1. Identificar responsable de la elaboración del AIPD

Será **responsable de la elaboración del AIPD** el órgano o centro directivo **impulsor y responsable** de la **propuesta normativa**, sin perjuicio de las acciones de coordinación con otros órganos que fueran necesarias.

No debe confundirse el **Responsable de la elaboración de la evaluación del impacto** en la protección de datos personales con el responsable del tratamiento que prevea o determine en la norma.

Será **responsable del tratamiento**[5], la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**. En la administración pública, habitualmente será el centro directivo que decida cómo y por qué se recogen y utilizan los datos personales.

5 Puede profundizarse en la definición del concepto en las "Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD" del Comité Europeo de Protección de Datos y en la STJUE de 11 de enero de 2024, asunto C-231/22 .

Estas **decisiones sobre el tratamiento** en la administración pública suelen estar determinadas por la necesidad de cumplir una obligación legal (art. 6.1.c) RGPD) o de ejecutar una misión realizada en interés público o en el ejercicio de poderes públicos (art. 6.1.e) del RGPD).

Paso 2. Identificar al DPD y el alcance de su intervención

Para asegurar que la norma en elaboración cumple con el marco vigente en materia de protección de datos será **imprescindible contar con el asesoramiento del DPD** tanto en el proceso de elaboración de la norma como de la elaboración del análisis del impacto en la protección de datos personales de la misma.

Por tanto, debe asegurarse y documentarse la participación y asesoramiento del DPD **desde el principio del proceso de elaboración de la norma**.

Paso 3. Verificar la previsión de tratamiento de datos personales en la norma o como consecuencia de su aplicación

Los conceptos "datos personales"[6] y "tratamiento"[7] tienen un alcance muy extenso y será difícil encontrar un proyecto de disposición normativa que no prevea o determine directa o de forma implícita a un tratamiento de datos personales.

Datos personales	Cualquier información relativa a una persona física identificada o identificable	
Ejemplos	• nombre y apellidos • DNI • voz, imagen • matrícula de vehículo • dirección IP	• número de teléfono • seudónimos • huella dactilar • datos sobre enfermedades • datos de afiliación sindical

6 Art. 4.1 RGPD: "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";

7 Art. 4.2 RGPD: 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;

Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de ellos
Ejemplos	• recoger • almacenar • comunicar, publicar, difundir • leer • transformar

Ejemplos prácticos de tratamientos de datos personales recogidos en la normativa	• El Registro de Profesionales Taurinos de Andalucía. • El Registro de Profesionales Sanitarios Objetores de Conciencia a la prestación de ayuda para morir en Andalucía. • La concesión de subvenciones dirigidas al fomento del empleo de personas con problemas de adicciones. • La publicación en la sede electrónica general de la Junta de Andalucía de la lista provisional de personas admitidas y excluidas en un proceso selectivo. • La provisión de puestos y movilidad para personas con discapacidad. • La expedición del carnet de vinculación entre la persona y el perro de asistencia.

Paso 4. Verificar que la norma incluye los elementos del tratamiento necesarios en materia de protección de datos

La **norma incluirá todos** aquellos **elementos adecuados** a la naturaleza, alcance y finalidades del tratamiento, de acuerdo con los principios de **transparencia y responsabilidad proactiva**.

Se considera **indispensable que la norma recoja**:
- Responsable del tratamiento
- Finalidad del tratamiento
- Base jurídica legitimadora
- Categorías de interesados y de datos personales

Como mínimo, se realizarán las **comprobaciones siguientes** respecto a cada tratamiento y se **valorará cuáles deben incluirse explícitamente** en la norma:

Atribución de responsabilidades	Deben identificarse: • Responsable(s) del tratamiento: derivado normalmente de un análisis de los hechos o circunstancias contemplados en la definición (art.4.7 RGPD)[8]. • Corresponsables del tratamiento, en su caso: deben asignarse responsabilidades recogidas en un acuerdo documentado (art. 26 RGPD). • Encargado(s) del tratamiento, en su caso: debe analizarse si es necesario especificar requisitos (art. 28 RGPD).
Finalidad del tratamiento	Motivo u objetivo específico para el cual se recogen y tratan los datos personales; es la razón por que se se necesitan utilizar los datos personales. Debe ser determinada, explícita y legítima y no se podrán contemplar tratamientos posteriores incompatibles (art. 5.1.b) y 6.4 RGPD). Importante: una tecnología no es una finalidad, es un medio.
Base jurídica legitimadora	Si el tratamiento está fundado en una obligación legal, el interés público o el ejercicio de poderes públicos, se debe identificar expresamente la norma con rango de Ley que lo habilita o que atribuye la competencia (art.6.1 RGPD y art. 8 LOPDGDD). El "interés legítimo" no es una base válida para las Administraciones Públicas (art. 6.1.f) RGPD). El consentimiento no es, con carácter general, la base jurídica adecuada para un tratamiento establecido por norma debido al desequilibro claro entre el interesado y una autoridad pública responsable. No obstante, si resultara adecuado, deberá asegurarse que sea libre, específico, informado e inequívoco (art.7 RGPD).
Minimización de datos	Los datos personales tratados serán adecuados, pertinentes y limitados a lo necesario (art.5.1.c) RGPD).
Plazos para supresión	Se identificarán los plazos previstos para la supresión de las diferentes categorías de datos, utilizando entre otros instrumentos, las tablas de valoración elaboradas por la Comisión Andaluza de Valoración de Documentos o en su defecto, los criterios que se adoptarán para determinar los plazos. Los datos tratados no se mantienen más tiempo del necesario para el cumplimiento de los fines del tratamiento (art. 5.1.e) RGPD).

8 Directrices del Comité Europeo de Protección de Datos 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD.

Categorías de interesados y categorías de datos personales	Se prestará especial atención a si existen categorías de datos especiales (art. 9 RGPD), personas vulnerables, en particular niños o una gran cantidad de datos personales o que afecte a un gran número de interesados. Si hay datos de categorías especiales, se identifica la excepción (de las contempladas en art. 9.2. RGPD) que habilita para su tratamiento.
Categorías de destinatarios	Si existen, se identificarán las entidades[9] que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación. Se garantizará: • comunicación de datos concretos, evitándose comunicaciones indiscriminadas. • el dato solicitado será pertinente y necesario. • comunicación sólo para la finalidad del tratamiento. • controlado y supervisado por el cedente.
Transferencias internacionales	En el caso de que se contemplen, se explicitarán y se identificará al menos una de las siguientes circunstancias: • existencia de decisión de adecuación (art. 45 RGPD). • garantías adecuadas para la transferencia (art. 46 RGPD). • situación específica que permita la transferencia (art. 49 RGPD).
Decisiones automatizadas incluida la elaboración de perfiles[10]	Las decisiones automatizadas representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano. La elaboración de perfiles suele emplearse para hacer predicciones sobre las personas, utilizando datos de distintas fuentes para inferir algo sobre un individuo, sobre la base de las cualidades de otros que parecen similares estadísticamente. En el caso de que se contemplen, se explicitarán y se identificarán (art. 22 RGPD): • la norma que lo autoriza y las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. • Mecanismos, en su caso, para ejercer el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a

9 En el caso de órganos judiciales, intervención, inspección u otros, habrá que tener en cuenta si se está en el marco de una investigación concreta de conformidad con el artículo 4.9 del RGPD.

10 Puede profundizarse en la definición de estos conceptos en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de GT29.

	impugnar la decisión.
Medidas técnicas y organizativas de seguridad	Cuando proceda, se realizará una descripción general de las medidas técnicas y organizativas de seguridad, que deberán ser adecuadas al nivel de riesgo para los derechos y libertades de las personas físicas que suponga el tratamiento. Se determinan también atendiendo a las categorías de interesados y datos personales tratados (art. 32 RGPD).
Formularios en la norma	Si la norma incluye algún tipo de formulario destinado a los ciudadanos: • deberá cumplirse con el principio de minimización tanto en los campos del formulario como en los documentos que se soliciten. • de conformidad con el principio de protección de datos desde el diseño, se incluirá la información necesaria y claramente diferenciable del resto, de acuerdo con los anteriores apartados. Esta información deberá cumplir como mínimo con lo establecido en el art. 13 RGPD.

Paso 5. Validar que los tratamientos están previstos en la ley y la finalidad legítima de los mismos

Un tratamiento de datos personales fundado en una obligación legal, o en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos **obligatoriamente tiene que estar previsto por Ley o derivar de una competencia atribuida por Ley**[11].

Si la norma en elaboración es una Ley, se regulará el tratamiento con los requisitos y garantías oportunas contempladas en las presentes orientaciones.

Si la norma propuesta no tiene rango de Ley, será necesario, dependiendo de la base legitimadora:

Cumplimiento de una obligación legal	Identificar la norma o normas con rango de Ley que expresamente establecen la obligación legal. Solo cuando el tratamiento esté previsto en una Ley puede considerarse legitimado en el cumplimiento de una obligación legal.

11 Art. 8 LOPDGDD.

Misión realizada en interés público **o** **Ejercicio de poderes públicos**	Identificar la Ley que atribuye al responsable la competencia para realizar dicha misión o ejercer determinados poderes públicos. Solo la Ley puede atribuir la competencia de la que deriva un tratamiento de datos fundado en el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos.

Respecto a la identificación de la norma con rango de Ley que legitime el tratamiento, deben tenerse en cuenta los siguientes **elementos fundamentales** de tipo cualitativo:

- **No es necesario que cada tratamiento individual se recoja en una norma específica.**
- **Una misma norma podrá regular distintos tratamientos.**
- **La norma legal debe ser clara, precisa y su aplicación previsible para sus destinatarios.** Los ciudadanos deben disponer de suficiente información para conocer el tipo de tratamiento acudiendo a la norma legal.
- La **finalidad** de los tratamientos deberá estar **relacionada** con alguno de los **objetivos perseguidos** por la Ley que lo habilita.

Si fuese **necesario el tratamiento de categorías especiales** de datos personales **por razones de un interés público esencial**, dicho tratamiento deberá estar amparado en una **norma con rango de ley**, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

Dicha ley *"deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas. Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos."*[12]

En caso de no poder identificar la Ley, el tratamiento no será legítimo y no se puede continuar. Deberá proponerse la elaboración de una norma con rango de Ley que regule el tratamiento.

12 https://www.aepd.es/documento/2019-0031.pdf

Paso 6. Evaluar la necesidad y proporcionalidad de los tratamientos

Para que un tratamiento sea conforme a la normativa de protección de datos, es necesario realizar una ponderación motivada atendiendo a tres criterios:

Juicio de idoneidad	**¿la medida es susceptible de conseguir el objetivo propuesto?** El tratamiento da respuesta a determinadas carencias, demandas, exigencias, obligaciones u oportunidades objetivas y puede conseguir los objetivos propuestos con la eficacia suficiente.
Juicio de necesidad	**¿existe otra medida menos intrusiva para la consecución de tal propósito con igual eficacia?** Hay que determinar si la finalidad perseguida no puede alcanzarse mediante un tratamiento alternativo menos lesivo o invasivo que sea igualmente eficaz para el logro de la finalidad perseguida.
Juicio de proporcionalidad en sentido estricto	**¿la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto?** Hay que ponderar el beneficio que el tratamiento de datos proporciona a la sociedad, manteniendo un equilibrio con la restricción que representa sobre los derechos fundamentales.

El **nivel de detalle** de esta evaluación será **el adecuado al impacto del tratamiento** para los derechos y libertades de las personas físicas.

Paso 7. Analizar los riesgos de los tratamientos para los derechos y libertades de las personas

Todo tratamiento para ser conforme a la normativa de protección de datos debe contar con las medidas técnicas y organizativas apropiadas que prevengan los riesgos para los derechos y libertades de la personas. El RGPD establece la obligación en sus artículos 24 (*"Responsabilidad del responsable del tratamiento"*) y 25 (*"Protección de datos desde el diseño y por defecto"*) de efectuar un análisis de riesgos de todo tratamiento que se prevea o determine en la norma.

Los riesgos pueden referirse a los daños y perjuicios físicos, materiales o inmateriales que pudiera provocar el tratamiento de datos personales.

Para el análisis de riesgos de los tratamientos puede acudirse a los diversos recursos publicados por la AEPD. En todo caso, durante dicho análisis debe prestarse especial atención a los **siguientes factores del riesgo**:

Doble dimensión del riesgo en las AAPP	• Riesgo para los derechos y libertades de las personas físicas. • Riesgo para la propia sociedad (o para un grupo representativo de ella). Los tratamientos de las AAPP **pueden afectar a grandes colectivos sociales**.
Factores agravantes de los riesgos	• Uso de inteligencia artificial • Decisiones automatizadas/elaboración de perfiles • Biometría • Vigilancia masiva • Centralización a gran escala de datos • Tratamiento masivo de datos • Categorías especiales de datos • Datos de menores o de personas vulnerables
Brechas de seguridad de los datos personales	En la determinación de los riesgos hay que tener en cuenta la posibilidad de que existan brechas, incluso masivas, de datos personales. La pregunta debe ser **¿qué puede ir mal y qué podemos hacer para que el impacto sea el menor posible?**

Cada tratamiento supondrá unos determinados riesgos para los derechos y libertades de las personas físicas. Estos riesgos deberán ser analizados en **mayor profundidad cuanto mayor impacto supongan**.

Con carácter general, debe establecerse una distinción entre la utilización de datos "estáticos" de la persona interesada (como la edad o el sexo o el padecimiento de una determinada patología) y la utilización de datos "conductuales" (análisis de patrones comportamentales para facilitar el desarrollo de servicios predictivos basados en las conductas individuales). Esta última utilización supone, una intrusión mayor en los derechos del interesado.

Por otra parte, en lo que atañe a los datos "conductuales", puede establecerse una distinción adicional entre la recogida de datos relativos a un comportamiento "activo" (como la acción de hacer clic en un botón para activar un chat o una videollamada) y la recogida de datos relativos a un

comportamiento “pasivo” (como la simple apertura de la puerta de un electrodoméstico o entrar y salir del domicilio), pues esta última resulta aún más intrusiva para el usuario.

Por todo ello, se deberán analizar los riesgos y reflejar documentalmente de forma más amplia y detallada cuanto mayor sea el contexto particular de riesgo para los derechos del interesado que tratamiento suponga.

En cualquier caso, **deberá analizarse, como mínimo, si el tratamiento implica alguno de los siguientes riesgos**:

Riesgos prioritarios	Discriminación
	Usurpación de identidad o fraude
	Daño para la reputación
	Pérdida de confidencialidad de datos sujetos al secreto profesional
	Reversión no autorizada de la seudonimización
	Perjuicios económicos o sociales significativos
	Privación a los interesados de sus derechos y libertades
	Impedimento en el ejercicio del control del interesado sobre sus datos personales
	Revelación del origen étnico o racial, de las opiniones políticas, de la religión o creencias filosóficas, de la militancia en sindicatos y del tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas
	Evaluación de aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales
	Tratamiento de datos personales de personas vulnerables, en particular niños
	Tratamiento que implique una gran cantidad de datos personales y afecte a un gran número de interesados

Por otra parte, existen riesgos que aparecen de forma habitual en cualquier tratamiento de datos personales y que deberán tenerse en cuenta:

Riesgos habituales	Acceso no autorizado: Riesgo de que datos personales sean accedidos por personas no autorizadas.
	Divulgación indebida: Riesgo de compartir información personal con terceros sin la base legal adecuada o sin cumplir con los principios de minimización de datos.

	Pérdida de datos: Riesgo de pérdida de datos personales debido a fallos técnicos, errores humanos afectando la disponibilidad y la integridad de los datos.
	Incumplimiento de derechos de los interesados: Riesgo de no respetar los derechos de acceso, rectificación, oposición o supresión de los datos de los interesados.

De conformidad con el art. 35 RGPD, cuando sea probable que un tipo de tratamiento 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.

Por tanto, si en el momento de la evaluación de impacto de protección de datos personales ya se detectase como consecuencia del análisis de riesgos efectuado que alguno de los tratamientos previstos o determinados en la norma suponen un alto riesgo, dicha circunstancia deberá quedar reflejada en la evaluación y ser tenida en cuenta en la planificación de recursos asociada a la puesta en marcha del tratamiento.

En relación con esto último, la Agencia Española de Protección de Datos ha publicado la lista orientativa de los tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos (EIPD) según el art. 35.4 RGPD, en virtud de la cual, "será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista".

Paso 8. Verificar la existencia de medidas apropiadas para garantizar que los tratamientos son conformes con la normativa de protección de datos

Debe garantizarse y acreditarse que cualquier tratamiento de datos personales sea conforme con la normativa de protección de datos y con la legislación sectorial aplicable.

A tal fin es necesario que se identifiquen en la norma las **medidas apropiadas de tipo técnico y organizativo.**

Estas deberán tener en cuenta los riesgos que puedan suponer los tratamientos para los derechos y libertades de las personas y, en concreto, **para el derecho a la protección de datos,** cumpliendo con las siguientes **características**:

Objetivos	• prevenir los riesgos y mitigar sus efectos. • asegurar transparencia, supervisión y la tutela judicial efectiva.

	• los datos no se recojan de forma desproporcionada. • los datos no se utilicen para fines distintos de los que justificaron su obtención.
Naturaleza y alcance	Dependerá de: • el tipo de tratamiento de datos. • la naturaleza de los datos tratados. • riesgos de abuso y de utilización ilícita.
Ejemplos de medidas válidas	• seudonimizar los datos personales. • limitar de forma expresa y clara la finalidad del tratamiento. • caducidad total o parcial de los tratamientos en la misma norma. • obligación de realizar una EIPD o consulta previa a los sujetos obligados por la norma a implementar el tratamiento. • evaluación periódica de las salvaguardas establecidas. • auditorías sobre la implementación concreta de los tratamientos por terceros independientes. • limitar la conservación de los datos, incluyendo la anonimización, seudonimización, eliminación selectiva de atributos sensibles. • limitar la extensión de los individuos afectados. • incorporar garantías adicionales en caso de decisiones automatizadas. • limitar las categorías de datos recogidos. • limitar las operaciones posibles en el tratamiento (p.ej. con relación a analizar, combinar y comunicar la información. • registro detallado de los accesos y comunicaciones de datos personales • establecer políticas de acceso restrictivas a los datos. • exigir que se desplieguen medidas concretas de seguridad técnicas. • exigir nivel de cumplimiento del Esquema Nacional de Seguridad adecuado al riesgo. • establecer separación técnica y funcional entre distintos grupos o departamentos en contextos de tratamientos independientes. • exigir compromiso expreso de confidencialidad, deber de secreto o sigilo profesional. • Obligar puesta a disposición de la documentación en lugar de la remisión.

Paso 9. Verificar la coherencia jurídica de la norma con el marco regulatorio en protección de datos

Con independencia de si la norma prevé o determina un tratamiento de datos personales, en todo caso deberá **verificarse la coherencia jurídica** de la misma con el **marco regulatorio en protección de datos**. Para ello, debe garantizarse que cualquier disposición contenida en la norma o regulación de medidas para garantizar el cumplimiento del marco regulatorio en protección de datos se realiza con pleno respeto y dentro de los límites establecidos en el mismo.

Para ello, se comprobará al menos si la norma contempla disposiciones o medidas que afecten a alguno de los siguientes **ámbitos del marco de protección de datos**:

Ámbitos de verificación	Decisiones individuales automatizadas, incluida la elaboración de perfiles (art. 22 RGPD).
	Limitaciones de derechos (art. 23 RGPD).
	Responsabilidad del responsable del tratamiento (art. 24, 25 y 29 RGPD, art. 28 y 29 LOPDGDD).
	Encargado del tratamiento (art. 28 RGPD, art. 33 LOPDGDD).
	Registro de las actividades de tratamiento (art. 30 RGPD, art. 31 LOPDGDD).
	Cooperación con la autoridad de control (art. 31 RGPD).
	Gestión de violaciones de la seguridad de los datos personales a la autoridad de control (art. 33 y 34 RGPD).
	Delegado de protección de datos (art. 37 a 39 RGPD, art. 34 a 37 LOPDGDD).
	Autoridades de control independientes (art. 51 a 59 RGPD, art. 57 a 59 LOPDGDD, art. 43 a 49 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía).
	Dictámenes u orientaciones de las autoridades de control (art.58.3.b RGPD).
	Ámbito laboral (art. 88 RGPD).

4. DOCUMENTAR EL ANÁLISIS DEL IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

El análisis realizado deberá quedar oportunamente documentado. Para ello se seguirá el modelo de análisis de impacto en la protección de datos personales anexo a las presentes orientaciones.

La profundidad y formalidad del análisis deberá ser acorde al riesgo (por ejemplo, atendiendo a si el tratamiento se refiere únicamente a datos "estáticos" o también contempla datos "conductuales") y al nivel de injerencia introducido por la norma para los derechos y libertades de los interesados.

Por todo ello, se deberá justificar documentalmente de forma más amplia y detallada cuanto mayor sea el contexto particular de injerencia a los derechos del interesado que la norma suponga.

El análisis realizado debe servir de base para la adopción de las medidas que sean adecuadas para llevar a cabo los tratamientos que prevea o determine la norma, así como cuando la misma desarrolle normas de protección de los datos personales; en particular, deberán incorporarse a la norma que se está elaborando aquellos aspectos del análisis que puedan contribuir desde la misma al mejor cumplimiento de la normativa de protección de datos.

5. SOLICITUD DE INFORME PRECEPTIVO A LA COMISIÓN CONSULTIVA DEL CONSEJO

El apartado 1.d) del artículo 15, sobre las funciones de la Comisión Consultiva de la Transparencia y la Protección de Datos, de los Estatutos del Consejo establece que será función de ésta:

"*d) Informar, con carácter preceptivo, los anteproyectos de leyes y proyectos de disposiciones generales sobre las materias competencia del Consejo.*"

Por tanto, de conformidad con sus Estatutos, el órgano o centro directivo impulsor y responsable de la propuesta normativa deberá solicitar preceptivamente informe a la Comisión Consultiva del Consejo sobre los anteproyectos de leyes y proyectos de disposiciones generales que prevean o determinen un tratamiento de datos personales, que desarrollen normas relativas a la protección de los datos personales o cuando regulen medidas para garantizar el cumplimiento de la normas de protección de datos.

Con carácter general, siempre que el AIPD realizado de conformidad con las presentes orientaciones haya concluido que existe algún impacto en la protección de datos personales, se deberá solicitar el citado informe a la Comisión Consultiva, acompañándose el proyecto de disposición normativa del AIPD cuando éste exista. En caso de existir dudas, el órgano directivo impulsor de la propuesta normativa podrá realizar consulta formal al Consejo sobre la necesidad de informe preceptivo.