**17/ES**

**WP 248 rev.01**

# Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679

**Adoptadas el 4 de abril de 2017**

**Revisadas por última vez y adoptadas el 4 de octubre de 2017**

Este grupo de trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Dirección General de Justicia de la Comisión Europea, B-1049, Bruselas, Bélgica, Oficina n.º MO-59 03/075.

Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm

**EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES**

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

vistos los artículos 29 y 30 de dicha Directiva,

visto su Reglamento interno,

**HA ADOPTADO LAS PRESENTES DIRECTRICES:**

# Índice

## I. Introducción

El Reglamento (UE) 2016/679[1] (RGPD) se aplicará a partir del 25 de mayo de 2018. El artículo 35 del RGPD introduce el concepto de evaluación de impacto relativa a la protección de datos (EIPD[2]), al igual que la Directiva (UE) 2016/680[3].

Una EIPD es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales[4] evaluándolos y determinando las medidas para abordarlos. Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento (véase asimismo el artículo 24)[5]. En otras palabras, **una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento**.

En virtud del RGPD, el incumplimiento de los requisitos de la EIPD puede dar lugar a la imposición de multas por parte de la autoridad de control competente. No llevar a cabo una EIPD cuando el

[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).

[2] El término «evaluación de impacto relativa a la intimidad» (EII) se utiliza a menudo en otros contextos para referirse al mismo concepto.

[3] El artículo 27 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, también establece que se llevará a cabo una evaluación de impacto relativa a la intimidad cuando sea probable que el tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas».

[4] El RGPD no define formalmente el concepto de EIPD como tal, pero

- el artículo 35, apartado 7, especifica su contenido mínimo de la siguiente manera:
  - «*a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;*
  - *b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;*
  - *c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y*
  - *d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas*»;
- su significado y función se aclaran en el considerando 84 de la siguiente manera: «*A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo*».

[5] Véase también el considerando 84: «*El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento*».

tratamiento requiera una evaluación de este tipo (artículo 35, apartados 1, 3 y 4), llevar a cabo una EIPD de forma incorrecta (artículo 35, apartados 2, 7, 8 y 9) o no consultar a la autoridad de control competente cuando sea necesario [artículo 36, apartado 3, letra e)] puede dar lugar a una multa administrativa de hasta 10 millones EUR o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

## II. Ámbito de aplicación de las directrices

Estas directrices tienen en cuenta:

- la Declaración 14/EN WP 218[6] del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29);
- las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243[7];
- el Dictamen del GT29 sobre la limitación de la finalidad, 13/EN WP 203[8];
- normas internacionales[9].

En consonancia con el enfoque basado en el riesgo introducido por el RGPD, no resulta obligatorio realizar una EIPD en todas las operaciones de tratamiento. Solo se exige cuando sea probable que el tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas» (artículo 35, apartado 1). A fin de garantizar una interpretación coherente de las circunstancias en las que resulta obligatoria una EIPD (artículo 35, apartado 3), las presentes directrices tienen como primer objetivo aclarar esta noción y ofrecer criterios para las listas que deben adoptar las autoridades de protección de datos (APD) en virtud del artículo 35, apartado 4.

Según el artículo 70, apartado 1, letra e), el Comité europeo de protección de datos (CEPD) podrá emitir directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del RGPD. La finalidad de este documento es anticipar esa labor futura del CEPD y, por tanto, aclarar las disposiciones pertinentes del RGPD para ayudar a los responsables del tratamiento a cumplir la legislación y ofrecer seguridad jurídica a aquellos que deben llevar a cabo una EIPD.

Estas directrices también pretenden fomentar el desarrollo de:

- una lista común de la Unión Europea de operaciones de tratamiento que requieren una EIPD (artículo 35, apartado 4);

---

[6] Declaración 14/EN WP 218 del GT29 sobre la función de un enfoque basado en el riesgo de los marcos jurídicos sobre protección de datos de 30 de mayo de 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243, adoptadas el 13 de diciembre de 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Dictamen 03/2013 del GT29 sobre la limitación de la finalidad, 13/EN WP 203, adoptado el 2 de abril de 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] P. ej., ISO 31000:2009, *Gestión de Riesgos — Principios y directrices*, Organización Internacional de Normalización (ISO); ISO/CEI 29134 (proyecto), *Tecnologías de la información – Técnicas de seguridad – Evaluación de impacto relativa a la intimidad – Directrices*, Organización Internacional de Normalización (ISO).

- una lista común de la Unión Europea de operaciones de tratamiento que no requieren una EIPD (artículo 35, apartado 5);
- criterios comunes sobre la metodología utilizada para realizar una EIPD (artículo 35, apartado 5);
- criterios comunes para especificar cuándo se consultará a la autoridad de control (artículo 36, apartado 1);
- recomendaciones, si es posible, basadas en la experiencia adquirida en los Estados miembros de la UE.

## III. EIPD: explicación del Reglamento

El RGPD requiere que los responsables del tratamiento apliquen medidas adecuadas para garantizar y poder demostrar el cumplimiento de dicho reglamento, teniendo en cuenta entre otros «los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (artículo 24, apartado 1). La obligación de los responsables del tratamiento de llevar a cabo una EIPD en determinadas circunstancias debe entenderse en el contexto de su obligación general de gestionar adecuadamente los riesgos[10] derivados del tratamiento de datos personales.

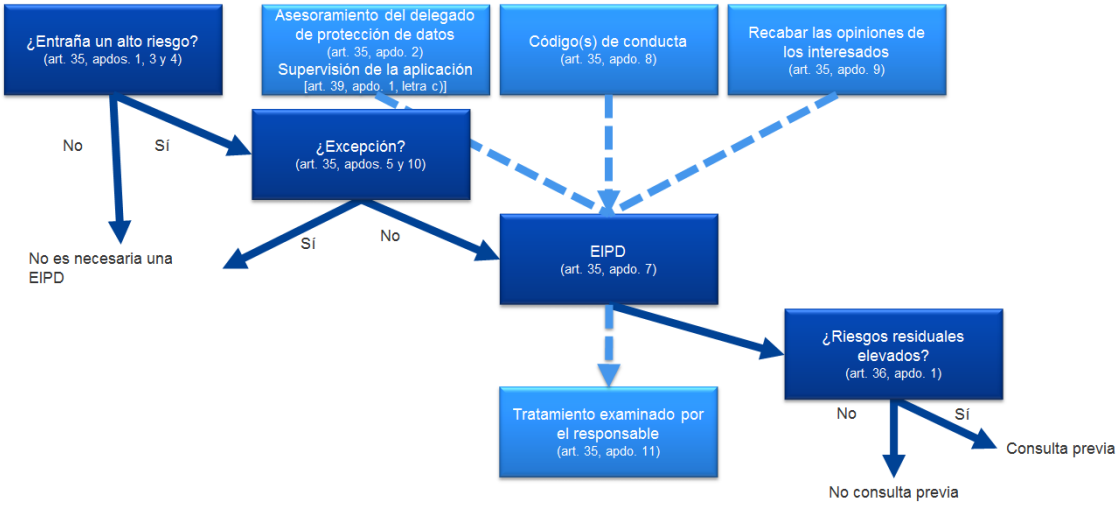
Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad. Por otra parte, la «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

El artículo 35 se refiere a un probable alto riesgo «para los derechos y libertades de las personas». Como se indica en la declaración del Grupo de Trabajo sobre protección de datos del artículo 29 sobre la función de un enfoque basado en el riesgo de los marcos jurídicos sobre protección de datos, la referencia a «los derechos y libertades» de los interesados atañe principalmente a los derechos a la protección de datos y a la intimidad, pero también puede implicar otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

En consonancia con el enfoque basado en el riesgo introducido por el RGPD, no resulta obligatorio realizar una EIPD en todas las operaciones de tratamiento. Por el contrario, solo se requiere «[c]uando sea probable que un tipo de tratamiento [...] entrañe un alto riesgo para los derechos y libertades de las personas físicas» (artículo 35, apartado 1). No obstante, el mero hecho de que las condiciones que dan lugar a la obligación de llevar a cabo una EIPD no se hayan cumplido no disminuye la obligación general de los responsables del tratamiento de aplicar medidas para gestionar adecuadamente los riesgos para los derechos y libertades de los interesados. En la práctica, esto significa que los responsables deben evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuando es probable que un tipo de tratamiento entrañe «un alto riesgo para los derechos y libertades de las personas físicas».

[10] Cabe señalar que, a fin de gestionar los riesgos para los derechos y libertades de las personas físicas, dichos riesgos deben identificarse, analizarse, estimarse, evaluarse, tratarse (p. ej., mitigarse) y revisarse con regularidad. Los responsables del tratamiento no pueden eludir su responsabilidad cubriendo los riesgos con pólizas de seguros.

El siguiente gráfico ilustra los principios básicos relacionados con la EIPD en el RGPD:




A. ¿Qué aborda una EIPD? Una única operación de tratamiento o un conjunto de operaciones de tratamiento similares.

**Una EIPD puede afectar a una única operación de tratamiento de datos**. Sin embargo, el artículo 35, apartado 1, establece que «[u]na única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares». El considerando 92 añade que «[h]ay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyectan introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado».

**Puede utilizarse una única EIPD para evaluar múltiples operaciones de tratamiento que sean similares** en términos de naturaleza, alcance, contexto, fines y riesgos. De hecho, las EIPD pretenden examinar sistemáticamente nuevas situaciones que puedan comportar riesgos elevados para los derechos y libertades de las personas físicas, y no hay necesidad de realizar EIPD en casos (es decir, operaciones de tratamiento realizadas en un contexto específico y para un fin concreto) que ya han sido examinados. Este puede ser el caso cuando se utiliza tecnología similar para recopilar el mismo tipo de datos para los mismos fines. Por ejemplo, un grupo de autoridades municipales que instala cada una un sistema de CCTV similar podría realizar una única EIPD que cubriera el tratamiento realizado por estos diferentes responsables, o un operador ferroviario (responsable del tratamiento único) podría cubrir la videovigilancia de todas sus estaciones con solo una EIPD. Esto sería igualmente aplicable a operaciones de tratamiento similares aplicadas por varios responsables. En esos casos, debe compartirse o hacerse pública una EIPD de referencia, deben aplicarse las medidas descritas en ella y debe ofrecerse una justificación de la realización de una única EIPD.

Cuando la operación de tratamiento implica a corresponsables, estos deben definir de forma precisa sus respectivas obligaciones. Su EIPD debe establecer qué parte es responsable de las distintas medidas destinadas a abordar los riesgos y proteger los derechos y libertades de los interesados. Cada responsable del tratamiento debe expresar sus necesidades y compartir información de utilidad sin poner en peligro secretos (p. ej., protección de secretos comerciales, propiedad intelectual, información comercial confidencial) o desvelar vulnerabilidades.

**Una EIPD también puede servir para evaluar el impacto relativo a la protección de datos de un producto tecnológico**, por ejemplo un elemento de *hardware* o *software*, cuando sea probable que distintos responsables utilicen dicho producto para realizar diferentes operaciones de tratamiento. Por supuesto, el responsable del tratamiento que instala el producto sigue teniendo la obligación de llevar a cabo su propia EIPD relativa a la aplicación específica, pero esta puede basarse en una EIPD preparada por el proveedor del producto, si procede. Un ejemplo podría ser la relación entre fabricantes de contadores inteligentes y empresas de servicios públicos. Todos los proveedores o transformadores de productos deben compartir información de utilidad sin poner en peligro secretos ni provocar riesgos de seguridad desvelando vulnerabilidades.

B. ¿Qué operaciones de tratamiento deben someterse a una EIPD? Salvo excepciones, todas aquellas que «probablemente entrañen alto riesgo».

Esta sección describe en qué casos es obligatoria una EIPD, y cuándo no es necesario realizar una.

**A menos que la operación de tratamiento cumpla una excepción (III.B.a), se debe realizar una EIPD cuando una operación de tratamiento «entrañe probablemente un alto riesgo» (III.B.b).**

a) ¿Cuándo resulta obligatoria una EIPD? Cuando el tratamiento «entrañe probablemente un alto riesgo».

El RGPD no requiere que se realice una EIPD para cada operación de tratamiento que pueda entrañar riesgos para los derechos y libertades de las personas físicas. La realización de una EIPD es únicamente obligatoria cuando el tratamiento «entrañe probablemente un alto riesgo para los derechos y libertades de las personas físicas» (artículo 35, apartado 1, ilustrado en el artículo 35, apartado 3 y complementado por el artículo 35, apartado 4). Es especialmente pertinente cuando se introduce una nueva tecnología de tratamiento de datos[11].

En los casos en los que no esté claro si se requiere una EIPD, el GT29 recomienda realizar una, ya que esta evaluación representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos.

Aunque en otras circunstancias pueda requerirse una EIPD, el artículo 35, apartado 3 ofrece algunos ejemplos de cuando una operación de tratamiento «es probable que entrañe un alto riesgo»:

- «*a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar*[12];
- *b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10*[13], *o*

[11] Para consultar más ejemplos, véanse los considerandos 89 y 91 y el artículo 35, apartados 1 y 3.

[12] Véase el considerando 71: «*en los casos en los que se evalúen 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*».

[13] Véase el considerando 75: «*en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de*

- *c) observación sistemática a gran escala de una zona de acceso público*».

Las palabras «en particular» indicadas en la frase introductoria del artículo 35, apartado 3 del RGPD se refieren a una lista no exhaustiva. Pueden existir operaciones de tratamiento de «alto riesgo» que no estén incluidas en esta lista pero que supongan unos riesgos similarmente elevados. Estas operaciones de tratamiento también deben someterse a una EIPD. Por este motivo, los criterios desarrollados a continuación van, en ocasiones, más allá de una simple explicación de lo que debería entenderse a partir de los tres ejemplos indicados en el artículo 35, apartado 3 del RGPD.

Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo, teniendo en cuenta los elementos particulares del artículo 35, apartado 1, y del artículo 35, apartado 3, letras a) a c), la lista que debe adoptarse a nivel nacional en virtud del artículo 35, apartado 4, y los considerandos 71, 75 y 91, y otras referencias del RGPD a operaciones de tratamiento[14] que «probablemente entrañen un alto riesgo», se deben considerar los nueve criterios siguientes:

1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes, o a una empresa de biotecnología que ofrezca pruebas genéticas directamente a los consumidores para evaluar y predecir los riesgos de enfermedad/salud, o a una empresa que elabore perfiles de comportamiento o de mercadotecnia basados en el uso o navegación en su sitio web.
2. Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar» [artículo 35, apartado 3, letra a)]. Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas. El tratamiento con poco o ningún efecto sobre las personas no coincide con este criterio específico. Las futuras directrices sobre elaboración de perfiles del GT29 contendrán más explicaciones sobre estas nociones.
3. Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso público» [artículo 35, apartado 3, letra c)][15]. Este tipo de observación

*datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas*».

[14] Véanse los ejemplos de los considerandos 75, 76, 92, 116.

[15] El GT29 interpreta «sistemática» en uno o más de los siguientes sentidos (véanse las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243):

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;
- que tiene lugar como parte de un plan general de recogida de datos;
- que se lleve a cabo como parte de una estrategia.

El GT29 interpreta «zona de acceso público» como cualquier sitio abierto a cualquier persona, por ejemplo, una plaza, centro comercial, calle, mercado, estación de tren o biblioteca pública.

representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamiento en espacios públicos (o espacios de acceso público).

4. Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales.
5. Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala[16]:
    a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
    b. el volumen de datos o la variedad de elementos de datos distintos que se procesan;
    c. la duración, o permanencia, de la actividad de tratamiento de datos;
    d. el alcance geográfico de la actividad de tratamiento.
6. Asociación o combinación de conjuntos de datos, por ejemplo procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamiento distintos de una manera que exceda las expectativas razonables del interesado[17].
7. Datos relativos a interesados vulnerables (considerando 75): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se

[16] Véanse las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243.
[17] Véase el Dictamen del GT29 sobre la limitación de la finalidad, 13/EN WP 203, p. 24.

pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento.

8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. El RGPD deja claro (artículo 35, apartado 1, y considerandos 89 y 91) que el uso de una nueva tecnología, definida «en función del nivel de conocimientos técnicos alcanzado» (considerando 91), puede hacer necesario realizar una EIPD. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a entender y abordar tales riesgos. Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD.
9. Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato» (artículo 22 y considerando 91). Esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo.

En la mayoría de los casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD. En general, el GT29 considera que cuantos más criterios cumpla el tratamiento, más probable será que represente un alto riesgo para los derechos y libertades de los interesados y, por tanto, requiera una EIPD independientemente de las medidas que el responsable contemple adoptar.

Sin embargo, en algunos casos, **un responsable del tratamiento puede considerar que un tratamiento que cumpla solo uno de estos criterios requiere una EIPD.**

Los siguientes ejemplos ilustran cómo deben utilizarse los criterios para evaluar si una operación de tratamiento concreta requiere una EIPD:

| **Ejemplos de tratamiento** | **Posibles criterios pertinentes** | **¿EIPD probablemente necesaria?** |
|---|---|---|
| Un hospital que trata los datos genéticos y sanitarios de sus pacientes (sistema de información hospitalaria). | - Datos sensibles o datos muy personales.<br>- Datos relativos a interesados vulnerables.<br>- Tratamiento de datos a gran escala. | Sí |
| El uso de un sistema de cámaras para controlar el comportamiento al volante en las autovías. El responsable del tratamiento contempla el uso de un sistema inteligente de análisis de vídeo para seleccionar coches y reconocer matrículas automáticamente. | - Observación sistemática.<br>- Uso innovador o aplicación de soluciones tecnológicas u organizativas. | |
| Una empresa que observa sistemáticamente las actividades de sus empleados, incluida la observación del puesto de trabajo de los | - Observación sistemática.<br>- Datos relativos a interesados vulnerables. | |

| Ejemplos de tratamiento | Posibles criterios pertinentes | ¿EIPD probablemente necesaria? |
|---|---|---|
| empleados, la actividad en internet, etc. | | |
| La recogida de datos de los medios sociales públicos para elaborar perfiles. | - Evaluación o puntuación.<br>- Tratamiento de datos a gran escala.<br>- Asociación o combinación de conjuntos de datos.<br>- Datos sensibles o datos muy personales: | |
| Una institución que crea una base de datos nacional de calificación crediticia o sobre fraudes. | - Evaluación o puntuación.<br>- Toma de decisiones automatizada con efecto jurídico significativo o similar.<br>- Impide a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato.<br>- Datos sensibles o datos muy personales: | |
| Conservación con fines de archivo de datos personales y sensibles seudonimizados relativos a interesados vulnerables de proyectos de investigación o ensayos clínicos. | - Datos sensibles.<br>- Datos relativos a interesados vulnerables.<br>- Impide a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato. | |
| Un tratamiento de «datos personales de pacientes o clientes por un solo médico, otro profesional de la salud o abogado» (considerando 91). | - Datos sensibles o datos muy personales.<br>- Datos relativos a interesados vulnerables. | No |
| Una revista en línea que use una lista de distribución para enviar un resumen diario genérico a sus suscriptores. | - Tratamiento de datos a gran escala. | |
| Un sitio web de comercio electrónico que muestra anuncios de piezas de coches clásicos que supone una elaboración de perfiles limitada basada en elementos vistos o adquiridos en su propio sitio web. | - Evaluación o puntuación. | |

**En cambio, aunque una operación de tratamiento se corresponda con los casos anteriormente mencionados, puede que un responsable no considere que dicho tratamiento «entraña probablemente un alto riesgo». En estos casos, el responsable debe justificar y documentar los motivos por los que no se realiza una EIPD e incluir/registrar las opiniones del delegado de protección de datos.**

Además, como parte del principio de responsabilidad proactiva, todos los responsables del tratamiento «llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad» incluido, entre otras cosas, los fines del tratamiento, una descripción de las categorías de datos y los destinatarios del tratamiento y, «cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1» (artículo 30, apartado 1) y deben evaluar si es probable un alto riesgo, incluso si finalmente deciden no realizar la EIPD.

Nota: las autoridades de control deben establecer, hacer pública y comunicar una lista de las operaciones de tratamiento que requieren una EIPD al Comité Europeo de Protección de Datos (CEPB) (artículo 35, apartado 4)[18]. Los criterios establecidos anteriormente pueden ayudar a las autoridades de control a constituir dicha lista, a la que se añadirá nuevo contenido específico en su momento si procede. Por ejemplo, el tratamiento de cualquier tipo de datos biométricos o de los correspondientes a niños también podría considerarse pertinente para la elaboración de una lista de conformidad con el artículo 35, apartado 4.

b) ¿Cuándo no se requiere una EIPD? Cuando «no sea probable que el tratamiento entrañe un alto riesgo», exista una EIPD similar, el tratamiento se haya autorizado antes de mayo de 2018, tenga una base jurídica o se encuentre en la lista de operaciones de tratamiento para las que no se requiere una EIPD.

El GT29 considera que no se requiere una EIPD en los siguientes casos:

- **cuando «no sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas»** (artículo 35, apartado 1);
- **cuando la naturaleza, el alcance, el contexto y los fines del tratamiento sean muy similares al tratamiento para el que se ha realizado la EIPD.** En esos casos, se pueden utilizar los resultados de la EIPD de tratamientos similares (artículo 35, apartado 1[19]);
- cuando las operaciones de tratamiento hayan sido comprobadas por la autoridad de control antes de mayo de 2018 en condiciones específicas que no hayan cambiado[20] (véase III.C);
- **cuando una operación de tratamiento**, de conformidad con el artículo 6, apartado 1, letra c) o e), **tenga una base jurídica** en el Derecho de la Unión o en el Derecho del Estado miembro, cuando tal Derecho regule la operación específica de tratamiento **y cuando ya se haya realizado una EIPD** en el contexto de la adopción de dicha base jurídica (artículo 35, apartado 10)[21], excepto si un Estado miembro considera necesario proceder a dicha evaluación previa a las actividades de tratamiento;
- **cuando el tratamiento se incluya en la lista opcional (establecida por la autoridad de control) de operaciones de tratamiento** para las que no se requiere una EIPD (artículo 35, apartado 5). Dicha lista puede contener actividades de tratamiento que cumplen las condiciones especificadas por dicha autoridad, en particular mediante directrices, decisiones o autorizaciones específicas, normas de cumplimiento, etc. (p. ej., en Francia, autorizaciones,

[18] En este contexto, «la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión» (artículo 35, apartado 6).

[19] «Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares».

[20] «Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas» (considerando 171).

[21] Cuando una EIPD se lleve a cabo en la fase de elaboración de la legislación que prevé una base jurídica para un tratamiento, es probable que requiera una revisión antes de la entrada en funcionamiento, ya que la legislación adoptada puede diferir de la propuesta en aspectos que afecten a cuestiones asociadas a la privacidad y la protección. Además, puede que no haya suficiente información técnica disponible en relación con el propio tratamiento en el momento de la adopción de la legislación, incluso si este estuvo acompañado de una EIPD. En tales casos, puede que siga siendo necesario realizar una EIPD específica antes de llevar a cabo las propias actividades de tratamiento.

exenciones, normas simplificadas, paquetes de cumplimiento, etc.). En tales casos, y sin perjuicio de una reevaluación por parte de la autoridad de control, no se requiere una EIPD, pero solo si el tratamiento se ciñe estrictamente al alcance del procedimiento pertinente mencionado en la lista y sigue cumpliendo plenamente todos los requisitos correspondientes del RGPD.

C. ¿Qué pasa con las operaciones de tratamiento ya existentes? En determinadas circunstancias se requieren EIPD.

**El requisito de realizar una EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.**

No será necesaria una EIPD para operaciones de tratamiento que hayan sido comprobadas por una autoridad de control o el delegado de protección de datos, de conformidad con el artículo 20 de la Directiva 95/46/CE, y que se realicen de una forma que no haya cambiado desde la anterior comprobación. De hecho, «[l]as decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas» (considerando 171).

En cambio, esto significa que deberán someterse a una EIPD los tratamientos cuyas condiciones de aplicación (alcance, fin, datos personales recogidos, identidad de los responsables o destinatarios del tratamiento, periodo de conservación de datos, medidas técnicas u organizativas, etc.) hayan cambiado desde la anterior comprobación realizada por la autoridad de control o el delegado de protección de datos y que probablemente entrañen un alto riesgo.

Además, podría requerirse una EIPD después de que se produzca un cambio de los riesgos a causa de las operaciones de tratamiento[22], por ejemplo debido a la puesta en marcha de una nueva tecnología o a que los datos personales se usan para un fin distinto. Las operaciones de tratamiento de datos pueden evolucionar rápidamente y pueden surgir nuevas vulnerabilidades. Por tanto, cabe señalar que la revisión de una EIPD no resulta útil solo para la mejora continua, sino que también es fundamental para mantener el nivel de protección de datos en un entorno que evoluciona con el tiempo. Una EIPD también puede resultar necesaria debido a cambios en el contexto organizativo o social de la actividad de tratamiento, por ejemplo debido a que los efectos de determinadas decisiones automatizadas hayan ganado importancia o a que nuevas categorías de interesados se vuelvan vulnerables a la discriminación. Cada uno de estos ejemplos podría ser un elemento que originase un cambio del riesgo resultante de la actividad de tratamiento en cuestión.

En cambio, ciertos cambios también podrían reducir el riesgo. Por ejemplo, una operación de tratamiento podría evolucionar de forma que las decisiones ya no fueran automatizadas o una actividad de observación ya no fuera sistemática. En ese caso, la revisión del análisis de riesgo realizada puede mostrar que ya no se requiere la realización de una EIPD.

[22] En términos de contexto, los datos recogidos, fines, funcionalidades, datos personales tratados, destinatarios, combinaciones de datos, riesgos (medios de apoyo, causas de riesgo, efectos posibles, amenazas, etc.), medidas de seguridad y transferencias internacionales.

Por razón de buenas prácticas, **una EIPD debe ser continuamente revisada y reevaluada con regularidad.** Por tanto, incluso si el 25 de mayo de 2018 no se requiere una EIPD, será necesario, en el momento oportuno, que el responsable del tratamiento lleve a cabo una evaluación de este tipo como parte de sus obligaciones generales de responsabilidad proactiva.

D. ¿Cómo se debe llevar a cabo una EIPD?

a) ¿En qué momento debe llevarse a cabo una EIPD? Antes del tratamiento.

**La EIPD debe realizarse «antes del tratamiento» (artículo 35, apartados 1 y 10, considerandos 90 y 93)[23]. Esto es coherente con los principios de protección de datos desde el diseño y por defecto (artículo 25 y considerando 78). La EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento.**

La EIPD debe iniciarse tan pronto como sea viable en el diseño de la operación de tratamiento incluso aunque algunas de las operaciones de tratamiento no se conozcan aún. La actualización de la EIPD a lo largo del proyecto de ciclo de vida garantizará que se tenga en cuenta la protección de los datos y la intimidad y propiciará la creación de soluciones que fomenten el cumplimiento. También puede resultar necesario repetir pasos concretos de la evaluación a medida que avance el proceso de desarrollo debido a que la selección de determinadas medidas técnicas u organizativas puede afectar a la gravedad o probabilidad de los riesgos que suponga el tratamiento.

El hecho de que pueda ser necesario actualizar la EIPD una vez iniciado el tratamiento no es un motivo válido para posponerla o no realizarla. La EIPD es un proceso continuo, especialmente cuando una operación de tratamiento es dinámica y está sujeta a cambios permanentes. **Llevar a cabo una EIPD es un proceso continuo, no una medida excepcional**.

b) ¿Quién está obligado a realizar una EIPD? El responsable, junto con el delegado de protección de datos y los encargados del tratamiento.

**El responsable del tratamiento debe garantizar que la EIPD se lleva a cabo (artículo 35, apartado 2)**. Cualquier otra persona, de dentro o fuera de la organización, puede llevar a cabo una EIPD, pero el responsable del tratamiento sigue respondiendo en última instancia por la tarea.

**El encargado del tratamiento recabará el asesoramiento del delegado de protección de datos**, si ha sido nombrado (artículo 35, apartado 2), y dicho asesoramiento, junto con las decisiones adoptadas por el responsable, debe ser documentado en la EIPD. El delegado de protección de datos también debe controlar la realización de la EIPD [artículo 39, apartado 1, letra c)]. Se ofrece más orientación en las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243.

Si un encargado lleva a cabo el tratamiento total o parcialmente, **dicho encargado debe ayudar al responsable a realizar la EIPD** y debe ofrecer la información necesaria [de acuerdo al artículo 28, apartado 3, letra f)].

**El responsable debe recabar «la opinión de los interesados o de sus representantes» (artículo 35, apartado 9), «[c]uando proceda».** El GT29 considera que:

[23] Excepto cuando es un tratamiento que ya existe y que ya ha sido comprobado por la autoridad de control, en cuyo caso la EIPD debe realizarse antes de que sufra cambios importantes.

- dichas opiniones pueden recabarse a través de una variedad de medios dependiendo del contexto (p. ej., un estudio genérico relacionado con el fin y los medios de la operación de tratamiento, una pregunta a los representantes de los empleados o encuestas habituales enviadas a los futuros clientes del responsable del tratamiento) garantizando que el responsable dispone de una base legal para llevar a cabo el tratamiento de cualquier dato personal necesario para la recogida de dichas opiniones. Aunque cabe destacar que, obviamente, autorizar el tratamiento no es una forma de recabar las opiniones de los interesados;
- si la decisión final del responsable del tratamiento difiere de las opiniones de los interesados, dicho responsable debe documentar sus motivos para seguir adelante o no;
- asimismo, el responsable debe documentar su justificación para no recabar las opiniones de los interesados si decide que esto no resulta adecuado, por ejemplo, si hacerlo pusiera en peligro la confidencialidad de los planes de negocio de las empresas, o si fuera desproporcionado o impracticable.

Finalmente, resulta una buena práctica definir y documentar otras funciones y responsabilidades específicas, dependiendo de la política interna, los procesos y las normas, p. ej.:

- en el caso de que unidades empresariales específicas propusieran llevar a cabo una EIPD, dichas unidades deberían aportar información a la EIPD y participar en el proceso de validación de dicha evaluación;
- en su caso, se recomienda recabar el asesoramiento de expertos independientes de distintas profesiones[24] (abogados, expertos en TI, expertos en seguridad, sociólogos, expertos en ética, etc.).
- las funciones y responsabilidades de los encargados del tratamiento deben definirse contractualmente; y la EIPD debe llevarse a cabo con la ayuda del encargado, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del primero [artículo 28, apartado 3, letra f)];
- el responsable principal de la seguridad de la información (CISO), en caso de ser nombrado, así como el delegado de protección de datos, podrían sugerir que el responsable llevara a cabo una EIPD sobre una operación de tratamiento específica, y deberían ayudar a las partes interesadas en la metodología, ayudar a evaluar la calidad de la evaluación de riesgo y si el riesgo residual es aceptable, y a desarrollar conocimientos específicos para el contexto del responsable del tratamiento;
- el responsable principal de la seguridad de la información (CISO), en caso de ser nombrado, o el servicio informático, deberían ofrecer ayuda al responsable y podrían proponer la realización de una EIPD sobre una operación de tratamiento específica, dependiendo de las necesidades de seguridad y operativas.

c) ¿Cuál es la metodología para llevar a cabo una EIPD? Se usan diferentes metodologías pero criterios comunes.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (Recomendaciones para un marco de evaluación de impacto relativa a la intimidad para la Unión Europea, documento D3):*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

El RGPD establece las características mínimas de una EIPD (artículo 35, apartado 7, y considerandos 84 y 90):

- «una descripción [...] de las operaciones de tratamiento previstas y de los fines del tratamiento»;
- «una evaluación de la necesidad y la proporcionalidad» del tratamiento;
- «una evaluación de los riesgos para los derechos y libertades de los interesados»;
- «las medidas previstas para:
    - afrontar los riesgos»;
    - «demostrar la conformidad con el presente Reglamento».

El siguiente gráfico ilustra el proceso iterativo genérico para realizar una EIPD[25]:


El cumplimiento de un código de conducta (artículo 40) debe tenerse en cuenta (artículo 35, apartado 8) a la hora de evaluar el impacto de la operación de tratamiento de datos. Esto puede resultar de utilidad para demostrar que se han elegido o aplicado medidas adecuadas, siempre que el código de conducta sea apropiado para la operación de tratamiento. Asimismo, deben tenerse en cuenta las certificaciones, sellos y marcas destinados a demostrar el cumplimiento de lo dispuesto en el RGPD en

[25] Cabe destacar que el proceso descrito aquí es iterativo: en la práctica, es probable que se reexamine varias veces cada una de las fases antes de poder completar una EIPD.

las operaciones de tratamiento de los responsables y los encargados (artículo 42), así como las normas corporativas vinculantes.

Todos los requisitos pertinentes establecidos en el RGPD ofrecen un marco amplio y genérico para diseñar y llevar a cabo una EIPD. La aplicación práctica de una EIPD dependerá de los requisitos establecidos en el RGPD que pueden verse complementados con una orientación práctica más detallada. Por tanto, la aplicación de la EIPD es escalable. Esto significa que incluso un pequeño responsable del tratamiento puede diseñar y aplicar una EIPD que sea apta para sus operaciones de tratamiento.

El considerando 90 del RGPD describe una serie de componentes de la EIPD que se solapan con componentes bien definidos de gestión del riesgo (p. ej., ISO 31000[26]). En términos de gestión del riesgo, una EIPD pretende «gestionar riesgos» para los derechos y libertades de las personas físicas, usando los siguientes procesos:

- estableciendo el contexto, es decir, «teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo»;
- evaluando los riesgos: «valorar la particular gravedad y probabilidad del alto riesgo»;
- tratando los riesgos: «mitigar el riesgo», «garantizar la protección de los datos personales» y «demostrar la conformidad con el presente Reglamento».

Nota: La EIPD con arreglo al RGPD es un instrumento destinado a gestionar riesgos para los derechos de los interesados y, por tanto, asume sus perspectivas como es el caso en determinados ámbitos (p. ej., seguridad de la sociedad). En cambio, la gestión del riesgo en otros ámbitos (p. ej., seguridad de la información) se centra en la organización.

El RGPD ofrece flexibilidad a los responsables del tratamiento para determinar la estructura y forma precisas de la EIPD con el fin de permitir que esta se ajuste a las prácticas de trabajo ya existentes. Existe una serie de distintos procesos establecidos dentro de la UE y en todo el mundo que tienen en cuenta los componentes descritos en el considerando 90. No obstante, sin importar su forma, una EIPD debe representar una auténtica evaluación de los riesgos que permita a los responsables tomar medidas para abordarlos.

Se pueden usar diferentes metodologías (véase el anexo 1 para consultar ejemplos de metodologías de evaluación del impacto relativas a la protección de datos y la intimidad) para ayudar a la aplicación de los requisitos básicos establecidos en el RGPD. Se han identificado criterios comunes con el fin de permitir la existencia de estos distintos enfoques, al tiempo que se permite a los responsables del tratamiento cumplir con el RGPD (véase el anexo 2). Aclaran los requisitos básicos del Reglamento, pero ofrecen un alcance suficiente para las diferentes formas de aplicación. Estos criterios pueden usarse para mostrar que una metodología de EIPD particular cumple los estándares exigidos por el RGPD. **Depende del responsable del tratamiento elegir una metodología, pero esta debe cumplir los criterios establecidos en el anexo 2.**

El GT29 promueve el desarrollo de marcos relativos a la EIPD específicos para cada sector. Esto se debe a que dichos marcos pueden aprovechar conocimientos específicos del sector, lo cual implica que

[26] Procesos de gestión del riesgo: comunicación y consulta, establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, supervisión y revisión (véanse los términos y definiciones, así como un índice, en la vista previa de la norma ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

la IEPD puede abordar los aspectos concretos de un tipo particular de operación de tratamiento (p. ej., tipos particulares de datos, activos empresariales, efectos posibles, amenazas, medidas). Esto significa que la EIPD puede abordar las cuestiones que se plantean en un sector económico concreto, o cuando se usan tecnologías particulares o se llevan a cabo tipos específicos de operaciones de tratamiento.

Por último, «[e]n caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento» (artículo 35, apartado 11[27]).

d) ¿Exista la obligación de publicar la EIPD? No, pero publicar un resumen podría fomentar la confianza, y se debe comunicar la EIPD completa a la autoridad de control en caso de consulta previa o si así lo solicita la APD.

**La publicación de una EIPD no representa un requisito jurídico del RGPD, ya que es una decisión que corresponde al responsable del tratamiento. Sin embargo, los responsables deben considerar al menos la publicación de algunas partes, como un resumen o una conclusión de su EIPD.**

El fin de dicho proceso sería ayudar a fomentar la confianza en las operaciones de tratamiento del responsable, y demostrar responsabilidad proactiva y transparencia. Cuando las personas se ven afectadas por la operación de tratamiento, la publicación de una EIPD supone una práctica particularmente positiva. Este podría ser en concreto el caso cuando un autoridad pública lleva a cabo una EIPD.

La EIPD publicada no necesita contener toda la evaluación, especialmente cuando podría presentar información específica relativa a riesgos de seguridad para el responsable del tratamiento o revelar secretos comerciales o información comercialmente sensible. En estas circunstancias la versión publicada podría consistir en un resumen de las principales conclusiones de la EIPD o incluso únicamente en una declaración que afirmarse que esta se ha llevado a cabo.

Además, cuando una EIPD revele unos elevados riesgos residuales, se exigirá al responsable del tratamiento realizar una consulta a la autoridad de control antes de proceder al tratamiento (artículo 36, apartado 1). En este contexto, se debe facilitar toda la EIPD [artículo 36, apartado 3, letra e)]. La autoridad de control puede facilitar su asesoramiento[28], y no pondrá en peligro secretos comerciales ni revelará vulnerabilidades de seguridad, sujeto a los principios aplicables en cada Estado miembro sobre acceso público a documentos oficiales.

E. ¿Cuándo debe consultarse a la autoridad de control? Cuando los riesgos residuales sean elevados.

Como se explica anteriormente:

- se exige una EIPD cuando «sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas» (artículo 35, apartado 1, véase III.B.a). Como ejemplo, se considera que el tratamiento de datos sanitarios a gran escala entraña probablemente un alto riesgo y requiere una EIPD;

[27] El artículo 35, apartado 10, solo excluye explícitamente la aplicación del artículo 35, apartados 1 a 7.

[28] Solo resulta necesario asesorar por escrito al responsable cuando la autoridad de control considere que el tratamiento previsto no se ajusta al Reglamento tal como establece el artículo 36, apartado 2.

- por tanto, corresponde al responsable del tratamiento evaluar los riesgos para los derechos y libertades de los interesados e identificar las medidas[29] previstas para reducirlos hasta un nivel aceptable y demostrar el cumplimiento del RGPD (artículo 35, apartado 7, véase III.C.c). Un ejemplo podría ser la utilización de medidas de seguridad técnicas y organizativas apropiadas para la conservación de datos personales en ordenadores portátiles (cifrado completo de disco efectivo, sólida gestión de claves, copias de seguridad garantizadas, etc.), además de la aplicación de las políticas existentes (notificación, consentimiento, derecho de acceso, derecho de oposición, etc.).

En el ejemplo anterior sobre ordenadores portátiles, si el responsable del tratamiento ha considerado que los riesgos son suficientemente reducidos y teniendo en cuenta el artículo 36, apartado 1, y los considerandos 84 y 94, el tratamiento puede seguir adelante sin necesidad de consultar a la autoridad de control. El responsable del tratamiento debe consultar a la autoridad de control en los casos en que dicho responsable no pueda abordar suficientemente los riesgos identificados (es decir, los riesgos residuales se mantienen elevados).

Un ejemplo de riesgo residual elevado inaceptable incluye casos en los que los interesados pueden encontrarse con consecuencias importantes, o incluso irreversibles, de las que no puedan recuperarse (p. ej.: un acceso ilegítimo a datos que suponga una amenaza para la vida de los interesados, un despido, un peligro financiero) o cuando parezca obvio que existirá un riesgo (p. ej.: por no poder reducir el número de personas que acceden a los datos debido a sus modos de intercambio, uso o distribución, o cuando no se corrige una vulnerabilidad conocida).

**Cuando el responsable del tratamiento no pueda hallar suficientes medidas para reducir los riesgos hasta un nivel aceptable (es decir, los riesgos residuales siguen siendo elevados), se debe consultar a la autoridad de control[30].**

Además, los responsables del tratamiento deberán consultar a la autoridad de control siempre que el Derecho de los Estados miembros les obligue a consultar a dicha autoridad o a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública (artículo 36, apartado 5).

No obstante, debe señalarse que, independientemente de si se debe consultar o no a la autoridad de control a causa del nivel de riesgo residual, siguen estando vigentes las obligaciones de conservar un registro de la EIPD y la actualización de este a su debido tiempo.

## IV. Conclusiones y recomendaciones

Las EIPD son una forma útil de que los responsables del tratamiento apliquen sistemas de tratamiento de datos que cumplan con el RGPD y pueden ser obligatorias para determinados tipos de operaciones

[29] Entre las que se incluyen, tener en cuenta la orientación existente del CEPB y las autoridades de control así como el estado de la técnica y los costes de aplicación, tal como dispone el artículo 35, apartado 1.

[30] Nota: «la seudonimización y el cifrado de datos personales» (así como la minimización de datos, los mecanismos de supervisión, etc.) no son necesariamente medidas apropiadas. Solo representan algunos ejemplos. Las medidas apropiadas dependen del contexto y los riesgos, específicos de las operaciones de tratamiento.

de tratamiento. Son escalables y pueden adoptar diferentes formas, pero el RGPD establece los requisitos básicos de una EIPD eficaz. Los responsables del tratamiento deben percibir la realización de una EIPD como una actividad útil y positiva que ayuda a cumplir con la legalidad.

El artículo 24, apartado 1, establece la obligación básica del responsable en términos de cumplimiento del 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, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario*.».

La EIPD representa una parte fundamental del cumplimiento del Reglamento cuando se planifican o realizan operaciones de tratamiento de alto riesgo. Esto significa que los responsables del tratamiento deben usar los criterios establecidos en el presente documento para determinar si se debe realizar una EIPD. La política interna de los responsables del tratamiento puede ampliar esta lista más allá de los requisitos jurídicos del RGPD. Esto debe ofrecer una mayor confianza de los interesados u otros responsables del tratamiento.

Cuando se planifica un tratamiento que probablemente sea de alto riesgo, el responsable del mismo debe:

- elegir una metodología de EIPD (véanse los ejemplos del anexo 1) que satisfaga los criterios del anexo 2, o especificar y aplicar un proceso sistemático de EIPD que:
  - cumpla con los criterios del anexo 2;
  - esté integrado en los procesos existentes de diseño, desarrollo, cambio, riesgo y revisión del funcionamiento de acuerdo con los procesos internos, el contexto y la cultura;
  - implique a las partes interesadas apropiadas y defina claramente sus responsabilidades (responsable, delegado de protección de datos, interesados o sus representantes, empresas, servicios técnicos, encargados, responsable de la seguridad de la información, etc.);
- ofrecer un informe relativo a la EIPD a la autoridad de control competente cuando sea necesario hacerlo;
- consultar a la autoridad de control cuando no consiga determinar medidas suficientes para mitigar los altos riesgos;
- examinar periódicamente la EIPD y el tratamiento que esta evalúa, al menos cuando se produzca un cambio del riesgo que representa el tratamiento de la operación;
- documentar las decisiones que se tomen.

## Anexo 1 – Ejemplos de marcos relativos a EIPD existentes en la UE

El RGPD no especifica qué proceso de EIPD debe seguirse sino que, en su lugar, permite a los responsables del tratamiento introducir un marco que complemente sus prácticas de trabajo existentes, siempre que tengan en cuenta los componentes descritos en el artículo 35, apartado 7. Dicho marco puede diseñarse a la medida del responsable del tratamiento o puede ser común a una industria particular. Otros marcos publicados anteriormente y desarrollados por las APD de la UE y marcos de sectores específicos de la UE incluyen (pero no están limitados a):

Ejemplos de marcos genéricos de la UE:

- DE: Standard Data Protection Model (modelo estándar de protección de datos), V.1.0 – versión de prueba, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA) (evaluación de impacto relativa a la intimidad)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice (realización de evaluaciones de impacto relativas a la intimidad: código de práctica)*, Oficina del Comisario de Información (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Ejemplos de marcos de sectores específicos de la UE:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications (marco de evaluación de impacto relativo a la intimidad y la protección de datos para las aplicaciones RFID)[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente[33]

---

[31] Reconocido de manera unánime y positiva (con la abstención de Baviera) por los 92.º Conferencia de las autoridades de protección de datos independientes del Bund y el Länder en Kühlungsborn, 9 y 10 de noviembre de 2016.

[32] Véase también:

- Recomendación de la Comisión, de 12 de mayo de 2009, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID).
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_es.pdf

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Asimismo, una norma internacional ofrecerá directrices sobre las metodologías utilizadas para llevar a cabo la EIPD (ISO/CEI 29134[34]).

[33] Véase también el Dictamen 07/2013 sobre el modelo de evaluación del impacto relativa a la protección de datos para redes inteligentes y para sistemas de medición inteligentes preparado por el Grupo de expertos 2 del Grupo especial sobre redes inteligentes de la Comisión. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_es.pdf

[34] ISO/CEI 29134 (proyecto), *Tecnologías de la información – Técnicas de seguridad – Evaluación de impacto relativa a la intimidad – Directrices*, Organización Internacional de Normalización (ISO).

## Anexo 2 – Criterios para una EIPD aceptable

El GT29 propone los siguientes criterios que los responsables del tratamiento pueden usar para evaluar si una EIPD, o una metodología usada para realizar una EIPD, es suficientemente exhaustiva para cumplir con el RGPD:

- ☐ se ofrece una descripción sistemática del tratamiento [artículo 35, apartado 7, letra a)]:
  - ☐ se tienen en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento (considerando 90);
  - ☐ se registran los datos personales, los destinatarios y el periodo durante el cual se conservarán dichos datos;
  - ☐ se ofrece una descripción funcional de la operación de tratamiento;
  - ☐ se identifican los medios de los que dependen los datos personales (hardware, software, redes, personas, papel o canales de transmisión del papel);
  - ☐ se tiene en cuenta el cumplimiento de los códigos de conducta aprobados (artículo 35, apartado 8);
- ☐ se evalúan la necesidad y la proporcionalidad [artículo 35, apartado 7, letra b)];
  - ☐ se determinan las medidas previstas para cumplir el Reglamento [artículo 35, apartado 7, letra d), y considerando 90], teniendo en cuenta:
    - ☐ las medidas que contribuyen a la proporcionalidad y la necesidad del tratamiento sobre la base de:
      - ☐ fines determinados, explícitos y legítimos [artículo 5, apartado 1, letra b)];
      - ☐ legalidad del tratamiento (artículo 6);
      - ☐ datos adecuados, pertinentes y limitados a lo necesario [artículo 5, apartado 1, letra c)];
      - ☐ duración limitada de la conservación [artículo 5, apartado 1, letra e)];
    - ☐ medidas que contribuyen a los derechos de los interesados:
      - ☐ información facilitada al interesado (artículos 12, 13 y 14);
      - ☐ derecho de acceso y a la portabilidad de los datos (artículos 15 y 20);
      - ☐ derecho de rectificación y de supresión (artículos 16, 17 y 19);
      - ☐ derecho de oposición y a la limitación del tratamiento (artículos 18, 19 y 21);
      - ☐ relaciones con los encargados del tratamiento (artículo 28);
      - ☐ garantías concurrentes en las transferencias internacionales (capítulo V);
      - ☐ consulta previa (artículo 36).
- ☐ se gestionan los riesgos para los derechos y libertades de los interesados [artículo 35, apartado 7, letra c)]:
  - ☐ se aprecian el origen, la naturaleza, la particularidad y la gravedad de los riesgos (véase el considerando 84) o, más concretamente, de cada riesgo (acceso ilegítimo, modificación no deseada y desaparición de datos) desde la perspectiva de los interesados;
    - ☐ se tienen en cuenta los orígenes de los riesgos (considerando 90);
    - ☐ se identifican efectos posibles sobre los derechos y libertades de los interesados en caso de que se produzcan hechos que incluyan el acceso ilegítimo, la modificación no deseada o la desaparición de datos;
    - ☐ se identifican las amenazas que pueden provocar el acceso ilegítimo, la modificación no deseada o la desaparición de datos;
    - ☐ se estiman la probabilidad y la gravedad (considerando 90);
  - ☐ se determinan las medidas previstas para tratar esos riesgos [artículo 35, apartado 7, letra d), y considerando 90];
- ☐ participan las partes interesadas:

- ☐ se recaba el asesoramiento del delegado de protección de datos (artículo 35, apartado 2);
- ☐ se recaban las opiniones de los interesados o sus representantes (artículo 35, apartado 9).