PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Directrices sobre cuestiones éticas y jurídicas de la protección de datos en la investigación e innovación en materia de TIC

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) – PRINCIPALES HERRAMIENTAS Y ACCIONES

Esta obra está bajo una licencia de Creative Commons Reconocimiento-No comercial-Sin obras derivadas 4.0 Internacional.

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 788039. Este documento refleja únicamente las opiniones de los autores, y la Agencia no se hace responsable del uso que pueda hacerse de la información contenida en él.

5 Principales herramientas y acciones

5.1 Creación o acceso a un conjunto de datos

Frederic Tronnier (GUF)

Esta parte de Las Directrices fue revisada por Aurélie Pols e Iñigo de Miguel Beriain.

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

Esta sección proporciona directrices para los investigadores que deseen obtener acceso a una base de datos externa o para los controladores que deseen proporcionar acceso a sus bases de datos a cambio de una compensación. Se basa en varias hipótesis fundamentales:

- Las bases de datos son, en general, valiosas. Este valor proviene de dos fuentes diferentes:
  - La información que contienen
  - La estructura y la organización en que se basan. Una base de datos bien organizada, documentada y estructurada es mucho más valiosa que una base de datos caótica.
- Se trata de datos personales. Esto es:
  - Los datos en cuestión no son datos anónimos. Los datos anónimos no son datos personales y, por tanto, quedan fuera del ámbito de aplicación del RGPD[218], por lo que estos datos pueden venderse o comprarse como cualquier otra mercancía. No nos centramos ahora en este tipo de datos;
  - Los datos personales, independientemente de si han sido seudonimizados o no, están protegidos por el RGPD y deben ser tratados de acuerdo con esta normativa.
  - Los datos sobre personas fallecidas no se consideran datos[219] personales. Por lo general, no están sujetos a las obligaciones establecidas por el RGPD (considerando 27), aunque pueden aplicarse posibles interpretaciones locales (véanse los informes nacionales que complementan estas directrices). Además, es importante tener en cuenta que si los datos se obtienen de personas fallecidas y se utilizan para obtener información sobre familiares vivos (datos genéticos, por ejemplo), estos datos podrían considerarse datos personales de los familiares.[220]

[218] Considerando26 del RGPD para más información.
[219] Véase el considerando 27 del RGPD.
[220] Sin embargo, hay que tener en cuenta la normativa nacional. Existen grandes diferencias entre los distintos Estados miembros. Véase nuestro análisis D21, Cuestiones y lagunas sobre el consentimiento informado en el contexto de la investigación e innovación en materia de TIC

- La situación puede ser totalmente diferente si el tercero va a utilizar la base de datos con fines de investigación bajo el paraguas del artículo 89 del RGPD o no (véase la sección sobre protección de datos e investigación científica). Esta diferencia se refiere principalmente al principio de limitación de la finalidad (artículo 5(b) del RGPD).

5.1.1 Valor en la estructura: Derechos *sui generis* de la base de datos

Una base de datos bien estructurada tiene valor. Este valor se deriva del trabajo realizado por un controlador que se ha esforzado en ordenar los datos. **Como creadores de una base de datos, los investigadores son titulares de derechos *sui generis sobre* las bases de datos.** Estos derechos fueron aplicados por la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, relativa a la protección jurídica de las bases de datos, modificada posteriormente por la directiva[221] sobre "derechos de autor". Reconocen el derecho del fabricante de una base de datos "a impedir la extracción y/o reutilización de la totalidad o de una parte sustancial, evaluada cualitativa y/o cuantitativamente, del contenido de dicha base".[222] Mediante los derechos sui generis sobre las bases de datos, los investigadores, actuando como controladores, pueden proteger el contenido de la base de datos, siempre que 1) puedan demostrar que ha habido una inversión cualitativa y/o cuantitativa sustancial en la obtención, verificación o presentación de los contenidos y 2) los investigadores estén radicados en la UE o sean residentes en ella.

El derecho tiene una duración de 15 años una vez completada la base de datos, pero puede renovarse continuamente durante 15 años si se realizan inversiones sustanciales en la base de datos.

Los derechos sui generis de las bases de datos pueden divulgarse y licenciarse como los derechos de autor. Pedir un pago por la licencia de una base de datos es, por tanto, perfectamente lícito. Sin embargo, la divulgación de estos derechos suele implicar el acceso al contenido de la base de datos a un tercero. Por lo tanto, los responsables del tratamiento deben asegurarse de que cuentan con una base jurídica para dicho tratamiento.

Existen otros derechos que también pueden proteger una base de datos, principalmente las obligaciones de derechos de autor (posibles, quizá no probables) y los derechos relacionados con la protección de datos. Por lo tanto, antes de acceder a una base de datos o de divulgarla, el propietario de la misma debe asegurarse de si alguno de ellos es aplicable o no.

---

[221] Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativa a los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE

[222] Apartado 1 del artículo 7 de la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. Esta Directiva fue

5.1.2 Pagar por el acceso/pedir el pago: las cuestiones legales

Si ahora nos centramos en conjuntos de datos individuales, y no en bases de datos, ya no deberíamos hablar de derechos sui generis, ya que el escenario sería totalmente diferente. Ahora estamos hablando de vender/comprar datos como tales. Como se ha dicho anteriormente, esto sólo es lícito si los datos no son en absoluto datos personales. Así pues, los investigadores que estén dispuestos a vender los datos recogidos deben anonimizar los conjuntos de datos antes de venderlos (véase "Identificación", "Pseudonimización" y "Anonimización", dentro de la sección "Conceptos principales" de la Parte II). Esto se debe a que los datos anónimos no entran en los requisitos del RGPD (como se describe en la sección anterior).

Si la anonimización no es posible, la cuestión que queda por resolver es si el **acceso a los datos personales podría concederse a un tercero con fines comerciales o si un investigador podría acceder a dicha base de datos pagando una cuota**, a través de una licencia de uso de los datos o compartiendo toda la base de datos. Esta cuestión requiere una cuidadosa consideración de al menos los siguientes **factores:**

(1) La venta o compra de acceso a datos personales se considera "tratamiento" en virtud del art. 4(2) porque es una forma de "difusión" o puesta a disposición de los datos por parte de terceros. 4(2) porque es una forma de "difusión" o de poner los datos a disposición de un tercero. Al igual que con todos los demás tipos de tratamiento, deben observarse los requisitos del RGPD;

(2) La base jurídica más común para el tratamiento con una finalidad distinta de aquella para la que se han recogido inicialmente los datos personales es el consentimiento del interesado o una ley de la Unión o de un Estado miembro, que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar los objetivos mencionados en el artículo 23, apartado 1[223];

(3) Si estas condiciones no se aplican (...) los responsables del tratamiento, para determinar si el tratamiento para otro fin es compatible con el fin para el que se recogieron inicialmente los datos personales, **realizarán una prueba de compatibilidad tal como se describe en el artículo 29 del LB[224].** Para llevar a cabo dicha prueba, deberán tenerse en cuenta, entre otros, los siguientes criterios (art. 6.4)

   i. **Cualquier vínculo** entre los fines para los que se han recogido los datos personales y los fines del tratamiento posterior previsto (lo que se denomina "factor de vinculación")

   ii. El **contexto** en el que se han recogido los datos, en particular **en lo que respecta a la relación entre los interesados y el responsable del tratamiento** (el "factor de contexto")

   iii. La **naturaleza** de los datos personales, en particular si se tratan categorías especiales de datos personales, por ejemplo, datos biométricos (el "factor de datos")

[223] Véase el artículo 6 (4) del RGPD

[224] Grupo del Artículo 29, Dictamen 03/2013 sobre la limitación de la finalidad adoptado el 2 de abril de 2013 (WP 203). En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Consultado: 27 de mayo de 2020)

iv. Las **posibles consecuencias** del tratamiento posterior previsto para los interesados (el "factor de consecuencia"), es decir, la probabilidad y la gravedad de las consecuencias negativas que podrían derivarse del tratamiento posterior para el interesado
v. La existencia de **garantías** adecuadas, que pueden incluir el cifrado o la seudonimización (el "factor de salvaguardia"), es decir, cómo se podrían proteger los datos

Todos estos factores son necesarios para evaluar si la finalidad del nuevo tratamiento es compatible con la finalidad del tratamiento actual para el que se recogieron inicialmente los datos. Cuanto más estrecha sea la relación entre la finalidad inicial y la finalidad del nuevo tratamiento, y cuanto menores sean las posibles consecuencias negativas, mayor será la probabilidad de que la transmisión de la base de datos sea lícita. Sin embargo, muchos de los factores anteriores pueden utilizarse claramente para argumentar en contra de la legalidad de una divulgación no consentida de una base de datos, lo que se explicará a continuación:

i. Si la divulgación no está relacionada con el proyecto original (por ejemplo, si su proyecto de investigación está terminado y después llega a la conclusión de que le gustaría monetizar los datos), no se da el **factor de vinculación**.
ii. El **factor del contexto** puede interpretarse en el sentido de que cuanto más *previsible, es* decir, evidente, sea la finalidad del tratamiento ulterior (desde la perspectiva de los interesados), más probable será que se considere compatible con la finalidad original y, por tanto, *lícita* con arreglo al artículo 6. 6. Si los interesados no han sido informados de que los datos van a ser revelados a un tercero, y los interesados no han dado su consentimiento, el factor del contexto actuará claramente en contra de la legalidad del tratamiento.
iii. El **factor de los datos** puede interpretarse como una indicación de que cuanto más sensibles sean los datos, más improbable será que el tratamiento posterior (en este caso, la venta) sea compatible con la finalidad original. Dicho de otro modo, si el conjunto de datos contiene categorías especiales de datos personales, como los datos biométricos o los datos relativos a la orientación sexual del interesado, sólo se puede facilitar el acceso a terceros si se aplica un fundamento jurídico para dicho tratamiento, de acuerdo con el artículo 9 de la RGPD. 9 de la RGPD. El art. 9 prohíbe el tratamiento de estas "categorías especiales" a menos que se den circunstancias específicas, como el consentimiento explícito al tratamiento (art. 9(2)(a)).
iv. El **factor de la consecuencia** sugiere que el impacto potencial de la venta del conjunto de datos sobre los sujetos de los datos tiene que considerarse para determinar si esa operación de venta es compatible con los fines iniciales para los que se procesaron los datos. Normalmente, las empresas compran datos para ampliar sus bases de clientes. En consecuencia, intentarán ponerse en contacto con los sujetos de los datos para sus necesidades comerciales. Es probable que esta interferencia con el derecho a la intimidad del cliente se considere un "impacto" significativo que habla en contra de la legalidad de la divulgación de una base de datos.

v. El **factor de salvaguardia** requiere diferentes consideraciones. En general, cuanto mayores sean los riesgos para los interesados, más fuertes deben ser las salvaguardias. Esto significa que los datos deben estar encriptados, protegidos y seudonimizados lo mejor posible.

Por lo tanto, antes de facilitar el acceso a los datos personales, la mejor opción **es obtener el consentimiento de los interesados o asegurarse de que se aplica una ley de la Unión o de un Estado miembro** que constituya una medida necesaria y proporcionada en una sociedad democrática para salvaguardar los objetivos mencionados en el artículo 23**.** En ausencia de cualquiera de estas circunstancias, la legalidad del tratamiento sería injustificable.

También significa que es necesario que las partes implicadas y entre ellas se planteen cuestiones para poder someterse a la prueba de compatibilidad. Además, los contratos deben respaldar la transferencia entre las partes para garantizar el cumplimiento de las obligaciones legales de cada una de ellas.

Algunos ejemplos de pruebas de tratamiento de compatibilidad

Es posible un tratamiento posterior

Un banco tiene un contrato con un cliente para proporcionarle una cuenta bancaria y un préstamo personal. Al final del primer año, el banco utiliza los datos personales del cliente para comprobar si puede optar a un tipo de préstamo mejor y a un plan de ahorro. Se informa al cliente. El banco puede volver a procesar los datos del cliente ya que los nuevos fines son compatibles con los iniciales.

No es posible el procesamiento posterior

El mismo banco quiere compartir los datos del cliente con empresas de seguros, basándose en el mismo contrato de cuenta bancaria y préstamo personal. Ese tratamiento no está permitido sin el consentimiento explícito del cliente, ya que la finalidad no es compatible con la finalidad original para la que se trataron los datos.[225]

[225] Fuente: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en (dirigido al 27 de mayo de 2020)

5.1.3 Divulgación de datos con fines de investigación y principio de limitación de la finalidad

Si los datos se utilizan con fines de investigación, no es necesario el consentimiento del interesado para su divulgación. Según el artículo 5, letra b), del RGPD, la utilización de los datos recogidos con fines de investigación es lícita y compatible con los fines para los que se recogieron inicialmente los datos personales (siempre que se adopten medidas técnicas y organizativas que garanticen el respeto de los derechos y libertades del interesado y que se aplique el artículo 89, apartado 1) (véase el "Principio de limitación de la finalidad" en la sección "Principios" de la Parte II de las presentes directrices).

Tampoco parece necesaria una mayor previsión normativa, a pesar de que el artículo 9.2.j) menciona explícitamente la necesidad de que el tratamiento esté "basado en el Derecho de la Unión o de los Estados miembros, que deberá ser proporcionado al objetivo perseguido, respetar la esencia del derecho a la protección de datos y prever medidas adecuadas y específicas para garantizar los derechos fundamentales y los intereses del interesado". Los considerandos 159 y 33 introducen la noción de consentimiento amplio para la investigación científica, lo que significa que el tratamiento exacto no debe especificarse completamente por adelantado. Sin embargo, los interesados deben tener la opción de dar su consentimiento para áreas específicas de la investigación y retirar el consentimiento para otras partes del objetivo de la investigación. (véase "Protección de datos e investigación científica" en la sección "Conceptos principales" de la Parte II).

5.1.4 Acuerdos

Aunque un responsable del tratamiento consiga encontrar una base jurídica para dar acceso a los datos a terceros, esto no significa que las garantías y los requisitos del RGPD no se apliquen a estos conjuntos de datos. Del mismo modo, un investigador que obtenga acceso a una base de datos debe ser consciente de las implicaciones jurídicas que su nueva posición (como responsable del tratamiento, corresponsable del tratamiento o encargado del tratamiento) puede acarrear (véase la sección "Principales actores" de la Parte II de estas Directrices). Además, habrá que volver a cumplir el requisito de equidad y transparencia. Esto significa que los interesados deben ser informados de sus derechos en cuanto a este tratamiento posterior. Todos los demás principios del RGPD deberán cumplirse también en relación con este tratamiento posterior.

Para aclarar las funciones que deben desempeñar las distintas partes implicadas en los acuerdos de transferencia de datos y garantizar que las disposiciones del RGPD se apliquen adecuadamente, es necesario y aconsejable celebrar contratos. Estos contratos deben abarcar todos los detalles de las operaciones de tratamiento de datos, incluido el objeto (datos que deben tratarse), la duración del tratamiento, la finalidad del tratamiento de datos, la naturaleza del tratamiento, la naturaleza de los datos, las categorías de interesados, etc. Deben especificar cómo se protegerán los derechos de los interesados y quién lo hará. Todo el mundo debe ser plenamente consciente de las funciones, las responsabilidades y los derechos de cada parte implicada. Ni que decir

tiene que los contratos deben incluir también cláusulas sobre las medidas de seguridad, el almacenamiento de datos, los derechos de auditoría, la notificación de infracciones y, en general, todas las cuestiones delicadas que contempla el RGPD. Estas cláusulas deben aclarar las diferentes obligaciones que asume cada parte firmante.

También existen contratos estándar para los diferentes casos, incluyendo, por ejemplo, la corresponsabilidad. Los investigadores que proporcionen acceso a sus bases de datos deberán incluir cláusulas detalladas dedicadas a la gestión del consentimiento para el tratamiento posterior, ya que son el controlador inicial que transmite los datos personales.

Independientemente de si el proyecto es de naturaleza académica o comercial, los responsables del tratamiento deben proporcionar a los interesados la misma información que se proporciona cuando los datos se recogen directamente de los interesados, incluyendo, entre otras cosas, quién es el responsable del tratamiento y cómo ponerse en contacto con él, los fines del tratamiento y la base jurídica del mismo, así como los derechos del interesado. Además, los interesados deben ser informados de la fuente de la que proceden los datos personales y de si proceden de fuentes de acceso público. La obligación de información debe cumplirse en un plazo razonable desde la obtención de los datos, pero a más tardar en un mes. Se aplican excepciones a esta obligación (por ejemplo, si el interesado ya dispone de la información). Los detalles completos sobre el alcance de esta obligación y las excepciones aplicables figuran en el artículo 14 del RGPD (véase "Derecho a la información" en la parte II, sección "Derechos del interesado").

5.1.5 Ámbito territorial de los datos

Si la organización está establecida en el EEE, el tratamiento de los datos personales entrará en el régimen del RGPD, independientemente de que los datos se refieran a interesados de fuera del EEE o de que hayan sido recogidos/tratados fuera del EEE o no (artículo 3, apartado 1). Además, el RGPD también se aplicará si la oferta de bienes y servicios, así como el seguimiento del comportamiento, tiene lugar dentro del EEE (art. 3(2)(a) y art. 3(2)(b)), independientemente de que el responsable o el encargado del tratamiento estén situados en el EEE. El RGPD también se aplica al tratamiento de datos personales en lugares en los que "se aplique el Derecho de los Estados miembros en virtud del Derecho internacional público" (art. 3.3), aunque el responsable del tratamiento no esté situado en la UE.

Si los datos se transfieren fuera del EEE, también debe notificarse al interesado, y esta transferencia internacional de datos debe estar respaldada por algún mecanismo que la haga legal (art. 14(1) (f)) (Véase "Transferencia de datos a terceros" en la sección de la Parte II "Principales herramientas y acciones")

Lo que hay que hacer

- Antes de acceder a una base de datos, un contrato entre el proveedor y el

receptor de los datos debe definir los derechos y responsabilidades de cada parte implicada en la transacción. Esto incluye la definición de si la finalidad del tratamiento por parte del receptor está en consonancia con el tratamiento que los interesados consintieron anteriormente (prueba de compatibilidad).

- Recopilar pruebas de que se han realizado inversiones sustanciales para la creación de su base de datos (no en la creación de datos como tal). Esto garantiza los derechos sui generis de la base de datos, que le otorgan el derecho a impedir que otros utilicen la base de datos o extraigan información de ella.
- Asegúrese de tener una base legal para la divulgación a terceros. Transmita las obligaciones a los receptores de los datos y establezca estipulaciones claras en los contratos entre las partes implicadas.
- Si está pensando en comercializar los datos, asegúrese de que los conjuntos de datos no contienen datos personales (de lo contrario, la comercialización sería ilegal). Antes de comercializar los datos por tu cuenta, deberías preguntar a tantos expertos como sea posible.
- Consulte con un responsable de la protección de datos (si se ha designado uno en su organización) o con especialistas en protección de datos personales antes de iniciar las operaciones de tratamiento.

Lo que no hay que hacer

- No utilice el paradigma de la propiedad de los datos: no encaja. Los derechos fundamentales de los interesados no pueden "venderse".
- No piense que si paga a un fabricante de bases de datos para utilizar su base de datos, quedará excluido de la responsabilidad en aquellos casos en los que el proveedor de los datos haya infringido otro derecho sobre una base de datos anterior. Cuestione siempre de forma crítica el origen de los datos a los que va a acceder, forma parte de las obligaciones de diligencia debida.
- No intentes recabar el consentimiento para todas las situaciones posibles. Un consentimiento amplio es aceptable, pero no puede considerarse un cheque en blanco.

- No intente influir o empujar a las personas para que le den sus datos personales. Recuerde que debe ofrecer a los participantes una opción real.
- No asuma nunca que los datos que ha recogido no son críticos. No se salte la aplicación del RGPD por la seudonimización de los datos personales. En la mayoría de los casos es mucho más fácil reidentificar a los sujetos de los datos de lo que usted cree (por ejemplo, debido a las tecnologías avanzadas que pueden correlacionar datos de múltiples fuentes y vincularlos a una persona específica). Sólo si los datos están realmente anonimizados, ya no es posible revertirlos a datos personales.

Lista de comprobación

- Las partes conocen bien la diferencia entre la concesión de licencias de derechos sui generis y la compra/venta de bases de datos como tales
- El tipo de datos en cuestión está claramente definido y el responsable del tratamiento se ha asegurado de si la GDRP es aplicable o no
- Se ha firmado un acuerdo entre el controlador y el tercero que aclara las funciones que debe desempeñar cada parte.
- Se han establecido las garantías adecuadas para proteger los derechos de los interesados y todas las partes son conscientes de sus obligaciones

5.1.6 Más información

- Grupo de trabajo del Artículo 29 Dictamen 03/2013 sobre la limitación de la finalidad Adoptado el 2 de abril de 2013 (WP 203). En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
- ICO: Principio (b): Limitación de la finalidad. En: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

5.2 Compartir datos

Frederic Tronnier (GUF)

Esta parte de Las Directrices fue revisada por Aurélie Pols e Iñigo de Miguel Beriain.

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

Esta parte de las Directrices ofrece consejos para los investigadores que quieran compartir datos procesados con otros investigadores u organizaciones de investigación después de haber realizado su tarea de investigación original. El hecho de compartir los datos con otros investigadores probablemente se considere una forma de "difusión" o de poner los datos "a disposición" de otros investigadores. En consecuencia, se consideraría un procesamiento (adicional) diferente al original, que implicaba que los datos se "utilizaran" para abordar una pregunta de investigación (véase "Obtener acceso a una base de datos" en la sección de la Parte II "Principales herramientas y acciones").

Partiendo de la base de que no se ha obtenido el consentimiento expreso de los interesados (de lo contrario, el requisito de legalidad sería más fácil de cumplir en virtud del artículo 6, apartado 1, letra a)). 6(1)(a), existen varios escenarios que exigen diferentes evaluaciones jurídicas (véase "Identificación", "Seudonimización" y "Anonimización" en la sección "Conceptos principales" de la Parte II de estas Directrices):

(1) Si los datos **se han seudonimizado** o se han establecido las salvaguardias adecuadas contra la reidentificación, puede ser más fácil que la "puesta en común" de los datos se considere legal en virtud del art. 6(4). 6(4).

(2) Incluso si los datos **no han** sido **seudonimizados,** siempre que la difusión de los datos se considere necesaria para fines de investigación científica o histórica (por ejemplo, no está destinada a satisfacer la curiosidad morbosa de otros investigadores, sino a ayudarles realmente a progresar en su campo), el tratamiento seguirá considerándose probablemente como operaciones de tratamiento lícito compatibles (considerando 50), aunque sigue siendo muy aconsejable obtener el consentimiento de los interesados para el tratamiento posterior. Los considerandos 159 y 33 introducen la noción de consentimiento amplio para la investigación científica, lo que significa que el tratamiento exacto no debe especificarse completamente por adelantado. Sin embargo, los sujetos de los datos deben tener la opción de dar su consentimiento para áreas específicas de la investigación y retirar el consentimiento para otras partes del objetivo de la investigación.

En cualquier caso, los responsables del tratamiento tendrán que satisfacer el principio **de equidad/transparencia** (véase "legalidad, equidad y transparencia" en la sección "Principios" del Patr. II de estas Directrices) de nuevo, haciendo que los interesados sean conscientes de sus derechos en cuanto a esta finalidad adicional (art. 14.4). Todos

los demás principios del RGPD deberán cumplirse también en relación con este tratamiento posterior.

Al igual que en el caso de la venta de datos personales, tenga en cuenta que usted puede tener un control conjunto con el destinatario de los datos y que sigue siendo responsable de la base de datos, es decir, responsable en caso de que el destinatario de los datos cometa infracciones (véase "Actores principales" en la Parte II de estas Directrices). Por lo tanto, al igual que en todas las transacciones, es necesario y aconsejable que haya contratos entre usted y el receptor de la base de datos para que todas las partes tengan claras las obligaciones y los derechos legales de cada una de ellas. Los contratos deben especificar la finalidad del receptor con los datos, así como el modo en que se protegerán los derechos de los interesados y quién lo hará.

Lo que hay que hacer

- Antes de adquirir el acceso a una base de datos, un contrato entre el proveedor y el receptor de los datos debe definir los derechos y responsabilidades de cada parte implicada en la transacción. Esto incluye definir si la finalidad del tratamiento por parte del receptor está en consonancia con el tratamiento que los interesados consintieron anteriormente.
- Trate todos los datos con el mismo cuidado que los datos personales y recuerde que los datos pueden ser agregados con datos adicionales de otras fuentes. Así, la anonimización de los datos personales es muy difícil.
- Si recaba el consentimiento para compartir datos, recuerde mantener un lenguaje claro y sencillo para atraer al mayor número de personas posible. Hágalo relevante para la vida de las personas; utilice ejemplos reales y cotidianos siempre que sea posible. Esto incluye explicar para qué se necesitan los datos, qué derechos tienen los interesados y cómo se protegen los datos y la privacidad del interesado. Asegúrese de recabar el consentimiento individual para cada uno de los fines para los que prevea la necesidad de procesar los datos personales.
- Recopilar pruebas de que se han realizado inversiones sustanciales para la creación de su base de datos (no en la creación de datos como tal). Esto garantiza los derechos sui generis de la base de datos, que le otorgan el derecho a impedir que otros utilicen la base de datos o extraigan información de ella.

- Registra todo lo que haces y explica el motivo.
- Asegúrese de tener una base legal para la divulgación a terceros. Transmita las obligaciones a los receptores de los datos y establezca estipulaciones claras.
- Si tiene dudas sobre la comercialización de datos, pregunte al mayor número posible de expertos antes de comercializarlos por su cuenta.
- Infórmese sobre el RGPD leyéndolo. Es necesario comprender claramente los términos básicos: "datos personales", "tratamiento", "encargado del tratamiento", "responsable del tratamiento" y "interesado" es necesario, pero tenga en cuenta que el cumplimiento del RGPD va más allá de estos términos. Por lo tanto, consulte con un responsable de la protección de datos (si se ha designado uno en su organización) o con especialistas en protección de datos personales antes de iniciar las operaciones de tratamiento.
- Para la investigación científica, utilice el dictamen del SEPD sobre protección de datos e investigación científica[226]

Lo que no hay que hacer

- No utilice el paradigma de la propiedad de los datos: no encaja. Los derechos fundamentales de los interesados no pueden "venderse".
- No piense que si paga a un fabricante de bases de datos para utilizar su base de datos, quedará excluido de la responsabilidad en aquellos casos en los que el proveedor de los datos haya infringido otro derecho sobre una base de datos anterior. Cuestiona siempre de forma crítica el origen de los datos que vas a comprar.
- No intente recabar el consentimiento para todas las situaciones posibles, la gente desconfiará de usted. Sin embargo, tampoco recojas un consentimiento para más de un propósito de procesamiento. Además, no utilices una jerga para ocultar la

[226] SEPD, 2020. Dictamen preliminar sobre la protección de datos y la investigación científica. Disponible en: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

intención o asustar a la gente.

- No advierta de las consecuencias económicas de la retirada del consentimiento o de la negativa a darlo. Recuerde que debe ofrecer a los participantes una opción real.
- No asuma nunca que los datos que ha recogido no son críticos. No se salte la aplicación del RGPD por la seudonimización de los datos personales. En la mayoría de los casos es mucho más fácil reidentificar a los sujetos de los datos de lo que usted piensa (por ejemplo, debido a las tecnologías avanzadas que pueden correlacionar datos de múltiples fuentes y vincularlos a una persona específica). Sólo si los datos están realmente anonimizados, ya no es posible revertirlos a datos personales.

5.3. Evaluación de Impacto relativa a la Protección de Datos (EIPD)

Bud P. Bruegger (ULD)

La versión final de esta sección ha sido validada por Hans Graux, profesor invitado de derecho de las TIC y de protección de la intimidad en el Instituto de Derecho, Tecnología y Sociedad de Tilburg (TILT) y en la AP Hogeschool Antwerpen. Presidente del Vlaamse Toezichtscommissie (Comité Flamenco de Supervisión), que supervisa el cumplimiento de la protección de datos en los organismos del sector público flamenco.

En determinados casos, el RGPD exige a los responsables del tratamiento que lleven a cabo una Evaluación de Impacto sobre la Protección de Datos (EIPD). A continuación, se describe este concepto respondiendo a algunas preguntas clave

Las respuestas se basan principalmente en el propio RGPD y en las directrices proporcionadas por el Grupo de Trabajo de Protección de Datos del Artículo 29 sobre el tema (wp248rev.01)[227] que ha sido aprobado[228] formalmente por el Comité[229] Europeo de Protección de Datos.

---

[227] wp248rev.01, GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto de la protección de datos (EIPD) y la determinación de si el tratamiento es "susceptible de provocar un alto riesgo" a los efectos del Reglamento 2016/679, Adoptado el 4 de abril de 2017, Según la última revisión y adopción del 4 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (última visita el 14/01/2020).

Lista de comprobación

- Verifique si necesita realizar una EIPD para su actividad de tratamiento.
    - Véase más abajo *¿En qué casos debo realizar una EIPD?*
- Documente esta verificación (independientemente de que sea afirmativa o no).

Si es necesaria una EIPD:

- Empezar lo antes posible (siguiendo el principio de la protección de datos por diseño).
    - Consulte a continuación en *qué momento es necesario realizar/actualizar la EIPD*.
- Obtenga una visión general de lo que es una EIPD. Véase más abajo:
    - *¿Qué es una EIPD?*
    - *¿Cuáles son los objetivos de una EIPD?*
    - *¿A qué público va dirigido un informe de EIPD?*
    - *Quién es el responsable de llevar a cabo una EIPD* a continuación
    - *¿Qué pasa si no lo llevo a cabo?*
- Utilice, siempre que sea posible, las orientaciones y plantillas facilitadas por la Autoridad de Supervisión de Protección de Datos (DPA) competente.
- Si no es así (su APD no proporciona dicho material o tiene que atender a muchos ámbitos de competencia de diferentes APD), siga las orientaciones proporcionadas por el Grupo de Trabajo de Protección de Datos del Artículo 29 en wp248rev.01.
    - Véase *más* abajo la sección *"Lecturas complementarias"*.
    - Véase *¿Existe un método estandarizado para llevar a cabo una EIPD?* para obtener una visión general y ayuda para interpretar el WP248rev.01.
- Reunir el equipo necesario para realizar la EIPD.
    - Véase más abajo *Quién debe participar en la realización de una EIPD*.
- Considere la posibilidad de facilitar su trabajo.

---

[228] Aprobación de las directrices del WP29 del RGPD por parte del Comité Europeo de Protección de Datos (CEPD), https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en, Bruselas, 25 de mayo de 2018, punto 6.

[229] https://edpb.europa.eu/

- Véase más abajo *Qué puede facilitar la realización de una EIPD*.

Lo que hay que hacer

- Empiece a trabajar en la EIPD lo antes posible.
- Destacar y documentar el proceso (continuo), no sólo el resultado (informe).
- Utilice la EIPD como herramienta de decisión para usted.
- Implicar al DPD y a todas las demás partes obligatorias.
- Centrarse en medidas técnicas y organizativas que reduzcan los riesgos a un nivel aceptable.
- Implementar un calendario para revisar y actualizar la EIPD cuando sea necesario

Lo que no hay que hacer

- No confunda la EIPD con la gestión de riesgos de seguridad informática.
- No considere los riesgos para su organización y sus activos; considere los riesgos para los interesados y otras personas físicas que se ven afectadas por su tratamiento.
- No entienda el riesgo como un acontecimiento indeseable (como un atentado o una catástrofe natural); considere su tratamiento como fuente de riesgo, incluso si todo sale como está previsto.

Más información

- Orientación y plantillas proporcionadas posiblemente por su Autoridad de Supervisión de Protección de Datos competente, que es el principal destinatario de la EIPD. (Lo que está disponible exactamente depende de su ubicación)
- WP248rev.01, Grupo de Trabajo de Protección de Datos del Artículo 29, Directrices sobre la evaluación de impacto de la protección de datos (EIPD) y la determinación de si el tratamiento es "probable que dé lugar a un alto riesgo" a los efectos del Reglamento 2016/679, Adoptado el 4 de abril de 2017, Tal como fue revisado y adoptado por última vez el 4 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (última visita el 14/01/2020).

5.2.1 ¿Qué es una EIPD?

La EIPD es un **proceso continuo** [230]que orienta y supervisa la realización de una actividad de tratamiento de datos de forma que se cumplan todos los requisitos de protección de datos y se minimice el impacto sobre las personas físicas. Este proceso se documenta en el **informe de la EIPD.**

La figura 1 muestra una ilustración del proceso proporcionada por el Grupo[231] de Trabajo del Artículo 29.

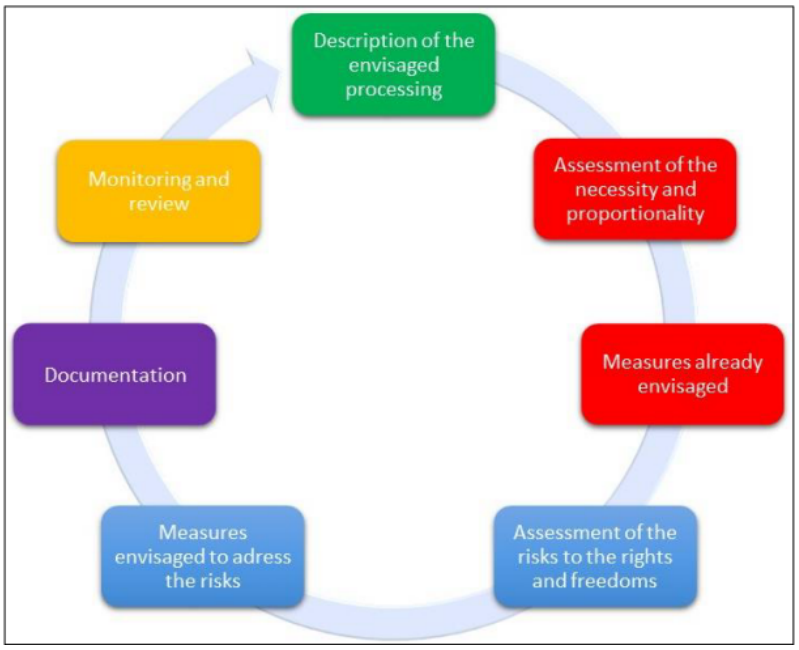


Figura 7: Proceso iterativo genérico para realizar una EIPD según el Grupo de Trabajo del Artículo 29.

5.2.2 ¿Cuáles son los objetivos de una EIPD?

La EIPD tiene dos objetivos principales[232]:

(i) **el cumplimiento de la construcción** y
(ii) **demostrando el cumplimiento**.

(i) El primero se refiere a un **proceso interno** que acompaña el diseño y las operaciones de una actividad de tratamiento. Al alcanzar el cumplimiento de los requisitos del RGPD, se identifican y mitigan los riesgos que las actividades de tratamiento suponen para los interesados. El proceso de llevar a cabo una EIPD instala la protección de datos como un principio

[230] wp248rev.01, página 14, Sección III.D.a), 3rd párrafo: "La realización de una DPIA es un proceso continuo, no un ejercicio único".
[231] wp248rev.01, página 16, sección III.D.3), 2nd párrafo.
[232] wp248rev.01, página 4, Sección I, 2 ndpárrafo: "En otras palabras, una EIPD es un proceso para construir y
demostrando el cumplimiento".

rector que informa las decisiones[233] de manera que se minimicen los riesgos de protección de datos y el impacto del tratamiento para las personas afectadas. Esto afecta en particular a las decisiones sobre los fines y los medios del tratamiento. Asegura que los requisitos de protección de datos se tengan en cuenta a lo largo de todas las fases del ciclo de vida de la actividad y no sólo como una "idea a posteriori" cuando ya se han tomado todas las decisiones. En otras palabras, evita que los datos personales puedan ser procesados sin haber identificado sus riesgos e impacto y sin aplicar las salvaguardias y medidas de mitigación adecuadas.

(ii) Este último se refiere al **informe de la EIPD** como una herramienta de responsabilidad[234] que se utiliza para demostrar que una determinada actividad de tratamiento cumple con el RGPD.

5.2.3 ¿A qué público va dirigido un informe de EIPD?

El informe de la EIPD se dirige a los siguientes destinatarios:

(i) Personas que participarán en las actividades de tratamiento **(normalmente del** responsable del tratamiento y (opcionalmente) de los encargados del mismo)

(ii) incluido el **Delegado de Protección de Datos (DPD)**

(iii) la **autoridad de supervisión** competente, y

(iv) (siempre que sea posible) al **público**.

(i) Teniendo en cuenta que la EIPD orienta las decisiones del responsable del tratamiento y (opcionalmente) del encargado del tratamiento, el informe de la EIPD (en varias versiones y fases de realización) sirve como herramienta de comunicación para el personal implicado. Esto es especialmente importante si se tiene en cuenta el posible carácter interdisciplinar del trabajo, en el que, por ejemplo, se requiere un tipo de experiencia para identificar los riesgos y otra para encontrar las medidas técnicas de mitigación adecuadas. Su función es aún más importante cuando el personal cambia y cuando la actividad de tratamiento evoluciona con el tiempo.

(ii) Los Delegados de Protección de Datos (DPD) tienen responsabilidades que se refieren directamente a la EIPD. En particular, tienen la tarea de asesorar cuando se les solicite sobre la EIPD y supervisar su funcionamiento[235].

(iii) Una autoridad de control que investigue si una determinada actividad de tratamiento es conforme con el RGPD, puede pedir que se le envíe un informe de la EIPD (cuando sea necesario) como prueba de que se ha cumplido la obligación del

---

[233] wp248rev.01, página 14, sección III.D.a), primer párrafo: "La EIPD debe considerarse una herramienta de ayuda a la toma de decisiones sobre el tratamiento".

[234] wp248rev.01, página 4, Sección I, 2 [nd]párrafo: "Las EIPD son herramientas importantes para la **rendición de cuentas**, ya que ayudan a los responsables del tratamiento no solo a cumplir los requisitos del RGPD, sino también a **demostrar** que se han tomado las medidas adecuadas para **garantizar el** cumplimiento del Reglamento (véase también el artículo 24). [Subrayado añadido por los autores].

[235] Artículo 35(1)(c) del RGPD.

artículo 35, y más en general para evaluar el cumplimiento del RGPD. Más bien, un informe de EIPD bien redactado contiene todas las pruebas necesarias para demostrar que la actividad de tratamiento es realmente conforme.

(iv) La transparencia es un requisito clave del RGPD. En consecuencia, el Grupo de Trabajo del Artículo 29 recomienda considerar la publicación de al menos una versión redactada de la EIPD [236].

5.2.4 ¿En qué se diferencia una EIPD de una evaluación de seguridad?

Muchas personas están más familiarizadas con la seguridad informática que con la protección de datos y utilizan metáforas de seguridad para pensar también en la protección de datos. Dado que esto es muy engañoso y puede dar lugar a EIPD inaceptables, esta sección explica la diferencia entre la protección de datos y las evaluaciones de impacto sobre la seguridad.

En el RGPD, la protección de datos y, por tanto, su cumplimiento, requiere la aplicación **de medidas técnicas y organizativas**[237]. Resulta un tanto engañoso que los *registros de tratamiento* que deben demostrar el cumplimiento[238] incluyan únicamente información sobre las medidas de **seguridad técnicas y organizativas**[239]. Por lo tanto, es importante tener en cuenta que una EIPD va más allá de la mera descripción de las medidas y que las medidas de las que se informa en una EIPD (artículo 35, apartado 7, letra d) del RGPD) no se limitan en absoluto a los aspectos de seguridad.

Desde el punto de vista de la seguridad, los datos deben estar protegidos contra los ataques externos e internos y los acontecimientos indeseables (como los fallos técnicos). A menudo se habla de proteger los datos en reposo, en tránsito y en uso. El hecho de que un riesgo residual sea aceptable se decide en función de la organización del responsable del tratamiento. Esta perspectiva no es aplicable a la protección de datos, aunque la expresión "proteger los datos contra los ataques" pueda entenderse como tal.

Aunque la protección de datos también contempla la protección contra ataques y sucesos indeseables, es decir, la seguridad[240], este aspecto sólo abarca uno [241]de los

---

[236] wp248rev.01, página 18, sección III.D.d), segundo párrafo: "Publicar una DPIA no es un requisito legal del RGPD, es decisión del responsable del tratamiento hacerlo. Sin embargo, los responsables del tratamiento deberían considerar la posibilidad de publicar al menos partes, como un resumen o una conclusión de su DPIA."

[237] El artículo 24, apartado 1, del RGPD establece que "...el responsable del tratamiento aplicará las **medidas técnicas y organizativas** apropiadas para **garantizar y** poder **demostrar** que el tratamiento se realiza **de conformidad con el presente Reglamento**." (Subrayado añadido por los autores).

[238] El considerando 82 del RGPD establece que "**Para demostrar el** cumplimiento del presente Reglamento, el responsable o el encargado del tratamiento deben **mantener registros de las actividades de tratamiento** bajo su responsabilidad." (Resaltado añadido por los autores).

[239] La letra g) del apartado 1 del artículo 30 establece que los registros de las actividades de tratamiento contendrán, "siempre que sea posible, una descripción general de las medidas de **seguridad** técnicas y organizativas mencionadas en el apartado 1 del artículo 32". (Subrayado añadido por los autores).

[240] En particular, el artículo 32 del RGPD "Seguridad del tratamiento" se refiere a la seguridad.

[241] Véase el artículo 5(1)(f) del RGPD, que enumera la seguridad como uno de los seis principios de la protección de datos.

seis[242] principios de la protección de datos (véase "Integridad y confidencialidad" en la sección "Principios" de la Parte II de estas Directrices). En otras palabras, la seguridad informática es un requisito previo para el tratamiento conforme, pero dista mucho de la conformidad total.

Si miramos más allá de la seguridad, los principales riesgos para los derechos y libertades de las personas físicas se originan en el tratamiento **tal y como está previsto, es decir,** incluso en ausencia de acontecimientos y ataques indeseables. La protección de datos exige que se minimicen los impactos negativos del tratamiento para las personas afectadas. Por lo tanto, una EIPD tiene que demostrarlo justificando que todas las operaciones de tratamiento son realmente **necesarias y proporcionales en relación con los fines**. Evidentemente, esto es muy diferente de una evaluación de seguridad: una actividad de tratamiento puede ser muy segura contra incidentes y ataques y, sin embargo, entrañar riesgos inaceptables para los derechos y libertades de las personas.

En materia de seguridad, las medidas de mitigación son en su mayoría técnicas y evitan los ataques o mitigan el efecto de eventos indeseables en los activos del responsable del tratamiento. En cambio, en la protección de datos, las medidas organizativas son igualmente importantes y minimizan el impacto negativo en las personas afectadas. Algunos ejemplos de medidas organizativas son las campañas de formación y concienciación de los empleados, los acuerdos de no divulgación y las cláusulas contractuales específicas para la informática subcontratada a los encargados del tratamiento.

En seguridad, el riesgo de violar los derechos y libertades de sólo unas pocas personas puede tener un efecto insignificante en los activos de una organización y, por tanto, ser aceptable para un controlador. En la protección de datos, la atención se centra en las personas afectadas y, aunque sólo sean unos pocos los afectados, el riesgo puede no ser en absoluto aceptable para ellos[243].

Mientras que en la seguridad las medidas están diseñadas para defenderse de ataques y eventos, en la protección de datos minimizan el impacto negativo en las personas afectadas. Esto es evidente, por ejemplo, en la limitación del periodo de almacenamiento, que limita temporalmente el posible impacto. Del mismo modo, la seudonimización impide la fácil identificación de los interesados y, por lo tanto, disminuye el riesgo de los mismos. Otras medidas tienen por objeto crear transparencia, de modo que los interesados no estén indefensos ante las decisiones de los responsables del tratamiento, sino que tengan la posibilidad de proteger sus derechos en caso de que sus derechos y libertades se vean excesiva o ilegítimamente vulnerados. Las medidas que implementan los derechos de los interesados hacen posible que éstos intervengan para proteger sus derechos. Estos ejemplos de medidas de protección de datos ilustran el carácter ampliamente diferente en comparación con las medidas de seguridad.

---

[242] Los seis principios de la protección de datos se enumeran en las letras a) a f) del apartado 1 del artículo 5 del RGPD.

[243] El Grupo de Trabajo del Artículo 29 afirma: "Nota: la EIPD en el marco del RGPD es una herramienta para gestionar los riesgos para los derechos de los interesados y, por tanto, adopta su perspectiva, como ocurre en determinados ámbitos (por ejemplo, la seguridad de la sociedad). Por el contrario, la gestión de riesgos en otros ámbitos (por ejemplo, la seguridad de la información) se centra en la organización. ", wp248rev.01, página 17, sección III.D.c), tercer párrafo.

5.2.5 ¿Quién es el responsable de llevar a cabo una EIPD?

"El responsable del tratamiento es el encargado de garantizar la realización de la EIPD (apartado 2 del artículo 35). La realización de la EIPD puede ser llevada a cabo por otra persona, dentro o fuera de la organización, pero el responsable del tratamiento sigue siendo el responsable último de esa tarea."[244] Obsérvese que el DPD debe ser consultado para una EIPD en calidad de asesor, pero nunca es responsable.

5.2.6 ¿Quién debe participar en la realización de una EIPD?

A continuación, se ofrece en primer lugar una respuesta jurídica basada en el RGPD y, a continuación, una orientación adicional sobre quién puede tener que participar en el proceso de una evaluación de impacto.

Desde el punto de vista jurídico, el Grupo de Trabajo del Artículo 29 da el siguiente consejo autorizado:

- "El responsable del tratamiento también **debe** solicitar el asesoramiento **del Delegado de Protección de Datos (DPD)**, cuando sea designado (apartado 2 del artículo 35) y este asesoramiento, así como las decisiones adoptadas por el responsable del tratamiento, deben documentarse en la EIPD. El DPD también debe supervisar la realización de la EIPD (artículo 39.1.c)".[245]
- "Si el tratamiento es realizado total o parcialmente por un **encargado del tratamiento**, éste **deberá** asistir al responsable del tratamiento en la realización de la EIPD y proporcionar toda la información necesaria (de acuerdo con el artículo 28.3.f)." [246]
- "El responsable del tratamiento **debe "**recabar la opinión de los interesados o de sus representantes" (artículo 35.9), "cuando proceda". "[247]Esto puede adoptar diversas formas en función del contexto, incluidos los estudios genéricos, la participación de representantes (como las organizaciones de consumidores) y las encuestas. El consentimiento no es una forma válida.

Más allá de estas participaciones exigidas por la ley, el Grupo de Trabajo del Artículo 29 recomienda abarcar todas las disciplinas (conocimientos técnicos) y responsabilidades (decisiones) pertinentes[248]. Esto puede suponer la participación tanto de personal interno como de expertos externos. Esto puede incluir, por ejemplo, lo siguiente:

- La **unidad de negocio** que utiliza la aplicación, instruye a los empleados afectados, toma decisiones sobre los períodos de almacenamiento, el control de acceso, etc.

---

[244] wp248rev.01, página 14, sección III.D.b), primer párrafo
[245] wp248rev.01, página 15, sección III.D.b), primer párrafo, resaltado por los autores.
[246] wp248rev.01, página 15, sección III.D.b), segundo párrafo, resaltado por los autores.
[247] wp248rev.01, página 15, sección III.D.b), tercer párrafo, resaltado por los autores, comillas cambiadas para mejorar la legibilidad.
[248] wp248rev.01, página 15, sección III.D.b), segunda mitad de la página.

- El **departamento de Tecnología Informática** que instala y opera la aplicación y ciertas medidas técnicas de mitigación (como, por ejemplo, cortafuegos o sistemas de copia de seguridad).
- El **departamento de recursos humanos**, que puede organizar campañas de sensibilización y formación, así como gestionar los acuerdos de confidencialidad con los empleados.
- El **departamento jurídico** que redacta las cláusulas contractuales específicas para transmitir las obligaciones a los transformadores.
- La **casa de software** que proporciona la aplicación y puede ofrecer actualizaciones (de seguridad), mantenimiento y evolución.

Tal y como indica explícitamente el Grupo de Trabajo del Artículo 29 para los DPD, se recomienda documentar las interacciones con las partes implicadas, el asesoramiento prestado y las decisiones tomadas en la EIPD. Se trata de un aspecto importante para demostrar la conformidad con el artículo 5, apartado 2, del RGPD.

5.2.7 ¿En qué casos debo realizar una EIPD? ¿Existen listas de actividades de tratamiento que requieran una EIPD?

El Grupo de Trabajo del Artículo 29 ha proporcionado la orientación más universalmente aplicable a esta cuestión[249]. Sobre esta base, muchas autoridades de supervisión han publicado orientaciones más específicas en su idioma nacional, centradas en sus preocupaciones nacionales.

Las orientaciones ofrecen un **procedimiento** para determinar si una actividad de tratamiento "puede entrañar un alto riesgo para los derechos y libertades de las personas físicas", es decir, **si es necesaria una EIPD**. Consta de **nueve criterios** sobre la actividad de tratamiento. Para cada criterio, el responsable del tratamiento debe decidir (y documentar) si es pertinente para la actividad de tratamiento en cuestión. La guía del grupo de trabajo incluye ejemplos que ilustran esto.

En concreto, los nueve criterios se refieren a lo siguiente

1. Evaluación o puntuación;
2. Toma de decisiones automatizada con efectos legales o similares significativos;
3. Control sistemático;
4. Datos sensibles o de carácter muy personal;
5. Datos procesados a gran escala;
6. Cotejar o combinar conjuntos de datos;
7. Datos relativos a personas vulnerables;
8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas;

[249] Véase wp248rev.01, Sección III.B .,páginas 8-13. El enlace de descarga se encuentra en la nota a pie de página **¡Error! Marcador no definido.**.

9. Impide a los interesados ejercer un derecho o utilizar un servicio o un contrato;

A partir de la evaluación de estos criterios, se decide si el tratamiento puede suponer un riesgo elevado: "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**".[250] Sin embargo, esto es sólo indicativo, y un responsable del tratamiento puede decidir que:

- un tratamiento que sólo cumpla uno de estos criterios requiere una EIPD;[251]
- un tratamiento que cumpla (al menos) dos criterios no es probable que dé lugar a un riesgo[252] elevado.

En este último caso, el responsable del tratamiento debe **justificar** esta decisión. En cualquier caso, para demostrar el cumplimiento (artículo 5, apartado 2, del RGPD), **debe documentarse** el procedimiento para determinar si es necesaria una EIPD.

Como orientación adicional, las autoridades de control (nacionales) deben publicar una lista del tipo de operaciones de tratamiento que requieren una EIPD (artículo 35, apartado 4, del RGPD) y también pueden publicar una lista de operaciones en las que no es necesaria una EIPD (artículo 35, apartado 5, del RGPD). Estas listas se presentan al Comité Europeo de Protección de Datos y se publican a nivel de la UE[253]; en la práctica, estas publicaciones pueden actuar como un repositorio accesible de los requisitos y expectativas de la EIPD a nivel nacional.

Aconsejamos seguir el procedimiento nacional o el previsto por el Grupo de Trabajo del Artículo 29 y documentarlo aunque se demuestre que no es necesaria una EIPD.

5.2.8 ¿En qué momento hay que realizar/actualizar la EIPD?

En cualquier caso, si es probable que exista un riesgo elevado, debe realizarse una EIPD **antes del tratamiento** (artículo 35, apartado 1, del RGPD). Esto constituye una salvaguardia que garantiza que el tratamiento que implica un alto riesgo no puede realizarse, a menos que los riesgos se hayan identificado y mitigado suficientemente.

Como ya se ha dicho (véase más arriba *Qué es una EIPD*), una **EIPD es un proceso continuo** que orienta el diseño y la ejecución de una actividad de tratamiento. Para orientar con éxito las decisiones y garantizar el cumplimiento del RGPD, es evidente que "la EIPD debe **iniciarse tan pronto como sea posible en el diseño de la operación de tratamiento,** incluso si algunas de las operaciones de tratamiento son aún desconocidas. La **actualización de la EIPD a lo largo del ciclo de vida** [del] proyecto garantizará que se tengan en cuenta la protección de datos y la privacidad y fomentará la creación de soluciones que promuevan el cumplimiento."[254] Este enfoque es

[250] wp248rev.01, Sección III.B., página 11, 2º párrafo, resaltado añadido por los autores.
[251] wp248rev.01, Sección III.B., página 11, 3er párrafo.
[252] wp248rev.01, Sección III.B., página 12, 2º párrafo.
[253] Ver https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en
[254] wp248rev.01, página 14, sección III.D.a), segundo párrafo, el subrayado y el texto entre paréntesis han sido añadidos por los autores.

evidentemente exigido por la obligación de **protección de datos desde el diseño** (artículo 25, apartado 1, del RGPD).

El proceso de una EIPD tampoco se da por concluido una vez que se ha iniciado el tratamiento. Más bien, "[c]uando sea necesario, el responsable del tratamiento llevará a cabo una **revisión** para evaluar si el tratamiento se realiza de conformidad con la [EADP] al menos cuando se produzca un **cambio en el riesgo** que representan las operaciones de tratamiento". (Artículo 35(11) del RGPD). Hay varios factores que pueden cambiar el riesgo, entre ellos los siguientes:

- La actividad de procesamiento cambia,
- la eficacia de las medidas de mitigación cambia.

En el primer caso, un cambio podría estar causado por un cambio en el uso previsto de los datos (nuevos fines del tratamiento), cambios en el alcance de la recopilación y el tratamiento de datos, cambios en el número de personas afectadas (por ejemplo, debido al éxito de la actividad), un cambio en el software de la aplicación (por ejemplo, una nueva versión con funcionalidad adicional), un cambio en la infraestructura técnica (por ejemplo, una migración a la nube) o un cambio en la situación legal (por ejemplo, una decisión judicial que afecta a la interpretación del RGPD).

En este último caso, un cambio podría estar causado por el descubrimiento de nuevas vulnerabilidades en las medidas de mitigación (por ejemplo, vulnerabilidades de software), un aumento de las amenazas y la capacidad de los *hackers* (por ejemplo, nuevos métodos para reidentificar datos seudónimos o anónimos), o un cambio organizativo que amenace la eficacia de las medidas (por ejemplo, nuevo personal que no es consciente de lo que se puede revelar).

5.2.9 ¿Existe un método estandarizado para llevar a cabo una EIPD? ¿Existen esquemas, plantillas o herramientas de apoyo a la realización de una EIPD?

Dado que la EIPD es un instrumento relativamente nuevo introducido a nivel de la UE con el RGPD, todavía se discute mucho sobre cómo debe llevarse a cabo exactamente una EIPD y existen varias escuelas de pensamiento. Algunas autoridades nacionales de supervisión han publicado orientaciones sobre el tema, o incluso herramientas y plantillas específicas. Aunque una EIPD es evaluada principalmente por la autoridad de supervisión competente (es decir, típicamente nacional), la orientación que aquí se ofrece no puede ir en mérito de lo que está disponible en todos los Estados miembros. En su lugar, la orientación se basa en el dictamen del Grupo de Trabajo de Protección de Datos del Artículo 29 sobre la EIPD (wp248rev.01)[255] que ha sido adoptado[256]

---

[255] wp248rev.01, GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto de la protección de datos (EIPD) y la determinación de si el tratamiento es "susceptible de provocar un alto riesgo" a los efectos del Reglamento 2016/679, Adoptado el 4 de abril de 2017, Según la última revisión y adopción del 4 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (última visita el 14/01/2020).

[256] Aprobación de las directrices del WP29 del RGPD por parte del Comité Europeo de Protección de Datos (CEPD), https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en, Bruselas, 25 de mayo de 2018, punto 6.

formalmente por el Comité[257] Europeo de Protección de Datos. Según el apartado 1 del artículo 70 del RGPD, "el Comité velará por la aplicación coherente del presente Reglamento" y es, por tanto, la mejor fuente de asesoramiento a nivel europeo.

La figura que ilustra el proceso iterativo para llevar a cabo una EIPD que proporciona el Grupo de Trabajo ya se ha mostrado en la Figura 1 anterior. Se trata de un ciclo que contiene los siguientes pasos:

1) Descripción del tratamiento previsto.
2) Evaluación de la necesidad y la proporcionalidad.
3) Medidas ya previstas.
4) Evaluación de los riesgos para los derechos y libertades [de las personas físicas].
5) Medidas previstas para hacer frente a los riesgos.
6) Documentación.
7) Seguimiento y revisión.

El Grupo de Trabajo explica que hay **flexibilidad** en la forma de estructurar una EIPD:

"El RGPD ofrece a los responsables del tratamiento de datos **flexibilidad para determinar la estructura y la forma precisas de la EIDP, a fin de permitir que** ésta se ajuste a las prácticas de trabajo existentes. Hay una serie de procesos establecidos en la UE y en todo el mundo que tienen en cuenta los componentes descritos en el considerando 90. Sin embargo, **sea cual sea su forma**, la **EIPD debe ser una auténtica evaluación de los riesgos que permita a los responsables del tratamiento adoptar medidas para hacerles frente**." [258]

El Grupo de Trabajo da ejemplos de enfoques conocidos en la actualidad en su Anexo I[259]. Estos incluyen "marcos" de EIPD **genéricos, nacionales** y específicos **del sector**. "El [**Grupo de Trabajo**] **alienta** el desarrollo de marcos de EIPD **específicos del sector**".[260]

Así pues, los responsables del tratamiento son libres de elegir la estructura y el formato más adecuados para una EIPD, siempre **que se cumplan determinados requisitos**: "Corresponde al responsable del tratamiento de datos elegir una metodología, pero ésta debe ajustarse a los **criterios previstos en el anexo 2**".[261] El Grupo de Trabajo "propone [estos] criterios que los responsables del tratamiento pueden utilizar para evaluar si una EIPD, o una metodología para llevar a cabo una EIPD, es suficientemente completa para cumplir con el RGPD"[262].

---

257 https://edpb.europa.eu/
258 wp248rev.01, página 17, Sección III.D.c), 4º párrafo, resaltado por los autores.
259 Anexo I de wp248rev.01, página 21.
260 wp248rev.01, página 17, Sección III.D.c), 6º párrafo, resaltado por los autores.
261 wp248rev.01, página 17, Sección III.D.c), 6º párrafo, resaltado por los autores.
262 wp248rev.01, página 22, anexo II, primer párrafo.

Normalmente, las diferentes metodologías vienen con esquemas, plantillas y/o herramientas.

Por lo tanto, el resto de esta sección se concentra en estos **criterios para una EIPD aceptable** proporcionados por el Grupo de Trabajo.

Los criterios reflejan en su mayor parte la estructura y el contenido del apartado 7 del artículo 35, pero aportan detalles e interpretaciones adicionales. A continuación, se presenta el contenido con algunos cambios de redacción y una pequeña reestructuración para mayor claridad[263]:

1. **Descripción sistemática del tratamiento** *(artículo 35, apartado 7, letra a) del RGPD)*
2. **Evaluación de la necesidad y la proporcionalidad** *(artículo 35, apartado 7, letras b) y d) del RGPD)*
3. **Gestión de los riesgos** para los derechos y libertades de los interesados *(artículo 35, apartado 7, letras c) y d) del RGPD)*
4. **Participación de las partes interesadas** (*artículos 35(2) y 35(9) del RGPD)*

Cada uno de ellos se analiza con más detalle en las subsecciones siguientes.

¿Puedo seguir el enfoque estándar de la ISO?

ISO ha publicado la norma internacional **ISO/IEC 29134:2017 " Tecnología de la información - Técnicas de seguridad - Directrices para la evaluación del impacto sobre la privacidad. "**Como es habitual en las normas ISO, el texto de la norma no está disponible públicamente, sino solo para los clientes de pago. Las normas ISO son de carácter global y, por tanto, atienden a diversos conceptos de "privacidad". Es poco probable que la norma adopte un punto de vista jurídico e imposible que una sola norma satisfaga los requisitos legales necesariamente diferentes de las distintas legislaciones. En caso de que el enfoque de la ISO sea adecuado para un determinado responsable del tratamiento, se aconseja, por tanto, que además se consulten paralelamente las orientaciones jurídicas específicas del RGPD.

De relevancia general para todas estas subsecciones es la segunda frase del considerando 90 del RGPD. Se presenta aquí con el resaltado y la estructura (viñetas) añadidos por los autores:

[263] Los criterios se proporcionan en una redacción es la del criterio de evaluación. En este documento, la redacción se cambia por títulos que reflejan la estructura. Por ejemplo, "se proporciona una descripción sistemática del tratamiento" se cambia por "descripción sistemática del tratamiento". Asimismo, la única entrada de nivel superior correspondiente a las letras c) y d) del apartado 7 del artículo 35 se divide en dos entradas separadas.

"Esa evaluación de **impacto** debe incluir, en particular, las **medidas, salvaguardias** y **mecanismos** previstos para:

- mitigar ese **riesgo,**
- garantizar la **protección de los datos personales** y
- **demostrando el cumplimiento** del presente Reglamento".

En otras palabras:

- La EIPD se **centra** en las **medidas, las salvaguardias** y el **mecanismo**.
- Se aplican a:
  - **riesgos**,
  - la protección de los datos personales, es decir, el **cumplimiento del** RGPD, y
  - **demostración de cumplimiento**.

Es importante señalar que la EIPD no sólo se centra en la identificación, evaluación y mitigación de los riesgos, sino también en el cumplimiento y la demostración del mismo. Esto último es especialmente evidente en la letra (b) del apartado 7 del artículo 35 y en la subsección correspondiente "2. Evaluación de la necesidad y la proporcionalidad" que se describe a continuación.

5.2.9.1 Descripción sistemática del tratamiento

Al detallar el artículo 35(7)(a) del RGPD, el Grupo de Trabajo desglosa la descripción del tratamiento en los siguientes elementos[264]:

- **Naturaleza**, **alcance**, **contexto** y **fines** del tratamiento *(considerando 90 del RGPD)*;
- **datos personales**, **destinatarios** y **periodo de almacenamiento**;
- **descripción funcional** de la operación de tratamiento;
- **los medios técnicos** y humanos empleados en el tratamiento (hardware, software, redes, personas, papel o canales de transmisión en papel);
- el cumplimiento de los **códigos de conducta** aprobados *(artículo 35, apartado 8, del RGPD)*.

Es importante tener en cuenta, en relación con el primer punto, que el artículo 35, apartado 7, letra a), dice: "**fines del** tratamiento, incluido, en su caso, el **interés legítimo perseguido por el responsable del tratamiento**".

Aunque la mayoría de los conceptos enumerados aquí se entienden bien, el significado exacto de *(i) naturaleza*, *(ii) alcance* y *(iii) contexto* puede ser más difícil de entender. Dado que no existe una interpretación autorizada de estos términos, a continuación, se ofrece una posible interpretación con la esperanza de que resulte útil.

[264] Adaptado de wp248rev.01, página 22, Anexo II.

(i) **Naturaleza**: Pueden existir múltiples aspectos relacionados con la **naturaleza** del tratamiento, entre ellos los siguientes:

- El **paradigma del procesamiento**;
- el **paradigma de las infraestructuras**;
- **nivel de automatización;**
- **forma de "efecto"**;
- el **nivel de innovación**.

Los paradigmas de procesamiento pueden ir desde el imperativo (es decir, las aplicaciones "tradicionales"), pasando por el basado en reglas/declarativo (por ejemplo, los sistemas expertos), hasta la inteligencia artificial basada en el aprendizaje automático.

El ***paradigma de la infraestructura*** puede ir desde una aplicación de escritorio, pasando por una aplicación cliente-servidor, hasta una solución basada en la nube, todas ellas con diferentes niveles de distribución.

El ***nivel de automatización*** puede ir desde el apoyo a los agentes humanos hasta el funcionamiento totalmente automático sin posibilidad de intervención humana.

La ***forma de "efecto"*** describe el "resultado" del tratamiento. Puede ir desde la pura información (en los sistemas de información), pasando por la creación de un estatus (por ejemplo, el derecho a voto) que determina las posibles acciones de una persona, hasta la gestión de los activos virtuales de una persona (por ejemplo, una cuenta bancaria), o los sistemas ciberfísicos que afectan directamente al mundo físico en el que vive la persona o a la propia persona.

El ***nivel de innovación*** puede ir desde mantenerse dentro del realismo, donde los riesgos y su mitigación se conocen bien, hasta desplegar nuevas tecnologías y métodos cuyas consecuencias aún no se han descubierto y que pueden venir con efectos secundarios y riesgos aún desconocidos.

(ii) **Alcance**: Lo que está dentro y fuera del **ámbito de** la actividad de tratamiento determina su impacto. En la protección de datos, el ámbito de aplicación debe considerarse en relación con las personas afectadas. Esto abarca múltiples aspectos, entre ellos los siguientes:

- ¿Cuáles y cuántas son las personas afectadas?
- ¿Qué aspectos de la vida de estas personas se ven afectados?
    - ¿Durante qué tiempo y con qué frecuencia se captan estos aspectos?
    - ¿Con qué precisión se captan estos aspectos?

Cuáles y cuántas personas se ven afectadas determinan evidentemente el impacto de la actividad de tratamiento. El tipo de personas afectadas es interesante para saber si algunas de ellas son **vulnerables** y requieren un tipo de protección especial. Además

del **número absoluto** de personas, las **cifras relativas** corresponden a zonas geográficas o grupos de usuarios.

Los aspectos de la vida ***afectados*** están estrechamente relacionados con las categorías de datos implicadas. Evidentemente, los diferentes aspectos de la vida conllevan diferentes niveles de sensibilidad y, por tanto, de riesgo. En el RGPD, las categorías **especiales de datos** (artículo 9) junto con los datos sobre condenas penales (artículo 10) se identifican como especialmente sensibles. El impacto del tratamiento de datos no sólo depende de los tipos de aspectos que se encuentran en el ámbito del tratamiento, sino también de qué **gama de aspectos** de una persona se abordan. Un aspecto aislado suele tener un impacto mucho menor que el tratamiento de un perfil que proporciona una imagen completa de la vida de una persona.

El ***ámbito temporal***, sobre todo la **duración** en la que se capturan estos aspectos, también determina el impacto. Esto está estrechamente relacionado con los periodos de almacenamiento y el borrado de los datos. Cuando un determinado tipo de datos se recoge más de una vez, la **frecuencia** también es importante. Esto es más evidente cuando se consideran los datos de localización, donde un seguimiento una vez cada pocos días es muy diferente de un seguimiento cada pocos minutos.

La ***precisión*** con la que se captan los aspectos de la vida de una persona también determina el impacto de la actividad de tratamiento. Esto es evidente, por ejemplo, cuando se analiza la ubicación, ya que saber el país en el que se encuentra una persona tiene un impacto mucho menor que conocer las coordenadas precisas. Del mismo modo, saber que una persona no tiene edad tiene un impacto mucho menor que conocer la fecha de nacimiento.

(iii) **Contexto**: Entender una actividad de tratamiento y sus riesgos es a menudo imposible sin conocer su **contexto**. Diferentes aspectos del contexto pueden ser, entre otros:

- Legal;
- Técnica
- Económico;
- Social.

Parte del contexto ***legal*** es la **base legal** para el tratamiento según el artículo 6 del RGPD y posiblemente el artículo 9 del RGPD. También son relevantes aquí las posibles **certificaciones según el** artículo 42 del RGPD, los **códigos de conducta** aprobados según el artículo 40 del RGPD (véase el artículo 35, apartado 8) y las **normas corporativas vinculantes** según el artículo 47 del RGPD. El contexto jurídico también puede incluir los **dictámenes autorizados del Comité Europeo de Protección de Datos, de** conformidad con el artículo 64 del RGPD, o las decisiones judiciales que sean pertinentes para la evaluación del impacto. Obsérvese que el Grupo de Trabajo ha incluido los códigos de conducta en un elemento separado, probablemente porque así lo exige explícitamente el artículo 35, apartado 8, del RGPD.

Hay dos aspectos que contribuyen al contexto ***técnico:***

- **Otras actividades de tratamiento** realizadas por el mismo o por diferentes responsables que interactúan con la actividad de tratamiento, y
- **El estado de la tecnología** para defender y atacar.

En algunos casos, es imposible evaluar una actividad de procesamiento de forma aislada. Este es el caso típico de los **sistemas distribuidos en** los que diferentes controladores operan diferentes componentes. Un buen ejemplo es la gestión de identidades federadas, en la que un *proveedor de identidades maneja* un componente que sólo puede entenderse si se tienen en cuenta también *los usuarios* y, por tanto, *las partes confiantes*. Aquí, y en muchos casos, la privacidad suele estar determinada por los protocolos de comunicación utilizados entre los componentes y, por tanto, por las actividades de procesamiento. Esto se ilustra con la existencia de protocolos[265] específicamente diseñados para mejorar la privacidad. Si se evaluara el impacto sin tener en cuenta el contexto, estos protocolos especialmente relevantes caerían en las lagunas de los controladores y, por tanto, de las EIPD.

Es evidente que hay que tener en cuenta el estado de la técnica para comprender el impacto del tratamiento. En consecuencia, el RGPD obliga a tener en cuenta el estado de la técnica tanto en el artículo 32, relativo a la seguridad del tratamiento, como en el artículo 25, relativo a la protección de datos desde el punto de vista del diseño y por defecto (véase "Protección de datos desde el punto de vista del diseño y por defecto" en la parte II de estas directrices, sección "Conceptos principales"). En materia de seguridad (que es uno de los aspectos de la protección de datos), para comprender los riesgos es fundamental entender el panorama actual de las amenazas, que describe la facilidad de los ataques y la disponibilidad y eficacia de las medidas defensivas. Para minimizar el impacto del tratamiento sobre los interesados de acuerdo con la protección de datos por diseño, es crucial conocer las posibilidades técnicas disponibles.

El contexto ***social*** describe la influencia que las personas y organizaciones pueden tener en las actividades de tratamiento. Esto incluye la cuestión de quién podría estar interesado en utilizar los datos procesados para otros fines. Esto incluye aspectos sobre la motivación y los recursos de los [266]posibles actores para hacerlo. Es importante señalar que el contexto no se limita a los agentes externos, sino que también incluye al personal interno que podría tener motivos para utilizar los datos con otros fines.

5.2.9.2 Evaluación de la necesidad y la proporcionalidad

Al detallar el artículo 35, apartado 7, letra b) del RGPD, el Grupo de Trabajo desglosa la evaluación de la necesidad y la proporcionalidad en varios subpuntos en dos grandes grupos[267]. Es importante señalar que todos estos puntos se refieren a las **medidas**

---

[265] Esto se ilustra con la técnica criptográfica de la intersección de conjuntos p+privados (véase https://en.wikipedia.org/wiki/Private_set_intersection).

[266] Los recursos incluyen aquí la capacidad técnica y la capacidad económica, así como la disponibilidad de información adicional accesible para un jugador.

[267] Adaptado de wp248rev.01, página 22, Anexo II.

previstas **para cumplir con el RGPD**.[268] Para facilitar la comprensión, estos puntos se clasifican aquí como sigue:

Puntos relacionados con:

(i) Obligaciones genéricas del capítulo 2 "**Principios**" del RGPD (véase "Principios principales" en la parte II de estas directrices)

(ii) Obligaciones específicas del capítulo 3 del RGPD "**Derechos del interesado**" (véase "Derechos del interesado" en la parte II de estas directrices)

(iii) Obligaciones específicas del capítulo 4 del RGPD "**Responsable y encargado del tratamiento**"

(iv) Obligaciones específicas del capítulo 5 del RGPD "**Transferencias de datos personales a terceros países u organizaciones internacionales**" (véase "Transferencias de datos a terceros países" en la sección de la Parte II "Principales herramientas y acciones")

A continuación, se describen con más detalle:

(i) ***Principios***:

Los puntos proporcionados por el Grupo de Trabajo del Artículo 29 en esta sección se corresponden estrechamente con los principios genéricos (a) a (f) de la protección de datos previstos en el artículo 5(1) del RGPD, con las siguientes diferencias:

- En cambio, se utiliza el artículo 6, más concreto, para cubrir la legalidad, en lugar del propio artículo 5(1)(a).
- Se omite la letra d) del apartado 1 del artículo 5, relativa a la "exactitud", probablemente porque el derecho de rectificación del interesado cubre los mismos aspectos de manera más concreta.
- Se omite la letra f) del apartado 1 del artículo 5, relativa a la seguridad ("integridad y confidencialidad"), probablemente porque se trata más adelante en la "gestión de los riesgos para los derechos y libertades de los interesados"

La EIPD se exige ahora para cada principio (véase "Principios principales" en la Parte II de estas Directrices), qué **medidas se** han tomado para cumplirlo. A continuación, se ofrece una selección incompleta de ejemplos de dichas medidas:

Las medidas para demostrar el cumplimiento de la "**limitación de los fines**" descrita en el artículo **5 (1) (b) consisten** en **especificar** los **fines explícitos** del tratamiento. Esta descripción debe ser precisa y concreta. Para demostrar el cumplimiento, debe **justificarse** por qué estos fines son **legítimos** y que el impacto sobre los interesados se ha minimizado manteniendo los fines tan limitados **como sea necesario**.

Otro aspecto importante del artículo 5, apartado 1, letra b), es que los datos "no serán tratados posteriormente de manera incompatible con dichos fines". Dado que la

[268] Véase wp248rev.01, página 22, anexo 2, 1st punto bajo "se evalúan la necesidad y la proporcionalidad".

divulgación se considera tratamiento (véase el artículo 4 (2) del RGPD), esto significa que los datos personales sólo se divulgarán a las personas y partes **que sean necesarias y estén justificadas por los fines establecidos**. Las medidas que demuestran el cumplimiento de este requisito incluyen la documentación de quién (empleados del responsable del tratamiento y terceros destinatarios) necesita acceder a los datos y al tratamiento y cómo se gestionan y actualizan en la práctica los derechos de acceso. Esto complementa las medidas para mitigar las amenazas de acceso ilegítimo que forman parte de la sección "gestión de riesgos" que se describe más adelante.

Las medidas para garantizar la **legalidad** del tratamiento consisten en la **documentación** de la **base jurídica** elegida, de acuerdo con los artículos 6 (1) y posiblemente 9 (2) del RGPD.

Cuando se utilice el artículo **6, apartado 1, letra a), "consentimiento" como** base jurídica, la documentación deberá incluir la forma en que se recogió este consentimiento (por ejemplo, un formulario o un diálogo) junto con una **justificación de** cómo se cumplen **los requisitos de** consentimiento establecidos en los **artículos 7 y 8** del RGPD. En el caso de que se opte por el "**consentimiento explícito"** del artículo **9, apartado 2, letra a)**, debe añadirse una justificación de cómo se cumplen los requisitos de esta forma especial de consentimiento. El mejor apoyo para esto lo proporciona el Grupo de Trabajo del Artículo 29 en sus "Directrices sobre el Consentimiento"[269].

Cuando se opta por el artículo **6, apartado 1, letra f), "intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero", es muy importante tener en cuenta que su base jurídica establece "**salvo que sobre** dichos intereses prevalezcan **los intereses o los derechos y libertades fundamentales del interesado** que requieran la protección de los datos personales, en particular cuando el interesado sea un niño". Para asegurarse de que los intereses del interesado no prevalecen sobre el interés legítimo del responsable del tratamiento, se requiere una "prueba de **equilibrio**" adicional (véase "Interés legítimo y prueba de equilibrio" en la parte II, sección "Principales herramientas y acciones"). El Grupo de Trabajo del Artículo 29 describió en su Dictamen WP217[270] en qué consiste dicha prueba de sopesamiento y cómo llevarla a cabo.

Las medidas para demostrar el cumplimiento de la letra c) del apartado 1 del artículo 5 "minimización **de datos**" son **justificaciones** de que los **datos personales** recogidos y tratados son **adecuados**, **pertinentes** y se **limitan a lo necesario** para alcanzar los **fines establecidos** (véase "Minimización de datos" en la sección "Principios" de la Parte II de estas Directrices).

---

269 wp259rev.01, GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre el consentimiento en virtud del Reglamento 2016/679, adoptadas el 28 de noviembre de 2017, revisadas y adoptadas por última vez el 10 de abril de 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (última visita el 29/01/2020)

270 wp217, PARTIDO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 06/2014 sobre la noción de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE, Adoptado el 9 de abril de 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (última visita el 29/01/2020). Obsérvese que, si bien este dictamen se refiere en gran medida a la Directiva de protección de datos y no al RGPD, los conceptos y métodos deberían aplicarse igualmente.

Las medidas para demostrar el cumplimiento del artículo 5(1)(e) "limitación **del almacenamiento**" (véase "Limitación del almacenamiento" en la Parte II, sección "Principios") consisten en la documentación que **justifica** que los datos se **almacenan sólo el tiempo necesario para los fines** (y luego se borran) y que la seudonimización y la anonimización que reducen/eliminan la identificabilidad de los sujetos de los datos se **aplica lo antes posible** para los fines (véase "Identificación", "Seudonimización" y "Anonimización" en la Parte II de estas Directrices, sección "Conceptos principales").

Aunque el Grupo de Trabajo no la incluyó explícitamente entre sus puntos, una medida adicional deseable sería la documentación de **las personas** y los destinatarios **a los que se revelan** legítimamente **los datos**.

(ii) ***Derechos del interesado***: (véase la sección "Derechos del interesado" dentro de la Parte II)

Los puntos proporcionados por el Grupo de Trabajo del Artículo 29 en esta sección abarcan casi todo el conjunto de artículos del Capítulo 3 "Derechos del interesado". Esto incluye los artículos 12 a 14 del RGPD, que se refieren principalmente a la transparencia, así como los artículos 15 a 21, que se refieren a los derechos específicos del interesado.

Las medidas para demostrar el cumplimiento de las obligaciones relativas al capítulo 3 consisten en una documentación de la información que se proporciona a los interesados y de los medios técnicos u organizativos de que disponen los interesados para ejercer estos derechos.

Sorprendentemente, el Grupo de Trabajo no incluyó el artículo 22 del RGPD entre sus puntos, aunque la "toma de decisiones individuales automatizadas, incluida la elaboración de perfiles" conlleva obviamente grandes riesgos para los interesados. Por lo tanto, se recomienda abordar el cumplimiento de este artículo de todos modos, si procede. Una medida adecuada podría ser documentar cómo el interesado puede acceder al "derecho a obtener intervención humana" que se menciona en el artículo 22, apartado 3.

(iii) ***Obligaciones del responsable y del encargado del tratamiento***:

Los puntos proporcionados por el Grupo de Trabajo del Artículo 29 en esta sección consisten únicamente en dos artículos del capítulo 4 del RGPD "**Responsable y encargado del tratamiento**", a saber, los artículos 28 y 36.

El artículo 28 se refiere a **los transformadores**. Las medidas que demuestran el cumplimiento de este artículo son, por ejemplo[271], las siguientes:

- Documentación de las **garantías ofrecidas por el encargado del tratamiento** "para aplicar las medidas técnicas y organizativas apropiadas de forma que el tratamiento cumpla los requisitos del presente Reglamento" (artículo 28.1 del RGPD).

[271] La lista de ejemplos no pretende ser exhaustiva.

- Medidas (como cláusulas contractuales) que **garanticen** que "el **encargado del tratamiento [no] contrate a otro encargado sin autorización previa**, específica o general, por escrito, del responsable del tratamiento" (artículo 28, apartado 2, del RGPD).
- Documentación de un "**contrato u otro acto jurídico"** que rija el tratamiento por parte de los encargados del mismo. Esto incluye las **cláusulas** que garantizan los **requisitos establecidos** en las **letras a) a h) del apartado 3 del** artículo **28**.

El artículo 36 se refiere a la "**consulta previa"** a la autoridad de supervisión competente si el riesgo residual después de aplicar las medidas de mitigación adecuadas sigue siendo elevado. La medida para demostrar el cumplimiento de este artículo es documentar dicha consulta y su resultado.

Más allá de los dos artículos del capítulo 3 del RGPD que fueron enumerados explícitamente entre los puntos por el Grupo de Trabajo, hay medidas adicionales que son posibles y deseables. Algunos ejemplos son los siguientes:

- Las medidas para demostrar el cumplimiento del artículo 25 "protección de datos desde **el diseño y por defecto**" pueden incluir la documentación de cómo se integró la protección de datos ya en la concepción y el diseño de la actividad de tratamiento. Esto puede consistir, por ejemplo, en los requisitos de protección de datos que se establecieron para un desarrollo o una licitación a medida, o en un análisis del cumplimiento de la protección de datos durante un proceso de selección (véase "Protección de datos desde el diseño y por defecto" en la sección "Conceptos principales" de la Parte II de estas Directrices).
- Las medidas para demostrar el cumplimiento de los artículos 33 y 34 sobre la notificación y la comunicación de las **violaciones de datos** podrían consistir en la documentación de los procedimientos internos para gestionar estas situaciones.

(iv) ***Transferencias de datos personales a terceros países u organizaciones internacionales:***

En esta sección, el Grupo de Trabajo del Artículo 29 proporciona un único punto que hace referencia a todo el capítulo 5 del RGPD. Las medidas para demostrar el cumplimiento en esta sección documentan las salvaguardias existentes que protegen a los interesados en caso de que sus datos se transfieran a zonas en las que el RGPD no es directamente aplicable. Entre las medidas concretas están la documentación de que existe una decisión de adecuación de la Comisión (artículo 45 del RGPD), la adhesión a normas corporativas jurídicamente vinculantes (artículo 47 del RGPD), o el uso de otro instrumento jurídicamente vinculante y aplicable (artículo 46 del RGPD) (véase "Transferencias de datos a terceros países" en la parte II, sección "Principales herramientas y acciones" de estas directrices).

5.2.9.3 Gestión de los riesgos para los derechos y libertades de los interesados

El artículo 35, apartado 7, letra c), exige la "evaluación de los riesgos para los derechos y libertades de los interesados". El considerando 84 establece además que el responsable del tratamiento que realice una EIPD debe "evaluar, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo". Sobre esta base, el Grupo de Trabajo del Artículo 29 subraya que dicha evaluación debe realizarse desde la perspectiva del interesado y ofrece el siguiente enfoque:

- Una lista de riesgos que deben ser evaluados y
- una serie de pasos que constituyen dicha evaluación

Por lo tanto, una EIPD debe abordar estos pasos para cada uno de los riesgos.

El grupo de trabajo enumera los siguientes riesgos:

1. acceso ilegítimo [a los datos personales],
2. modificación no deseada [de los datos personales], y
3. desaparición de datos.

Evidentemente, estos riesgos parafrasean la redacción del artículo 5.1.f) sobre el principio de "integridad y confidencialidad". También es coherente con "la confidencialidad, la integridad, la disponibilidad y la capacidad de recuperación de los sistemas y servicios de tratamiento" que se enuncia en el artículo 32, apartado 1, letra b) del RGPD. También es posible ver una equivalencia directa con los objetivos de protección utilizados en la seguridad informática, a saber, *la confidencialidad*, la *integridad* y la *disponibilidad*.

Para la evaluación de cada riesgo, el Grupo de Trabajo establece los siguientes componentes:

1. identificación de las fuentes de riesgo (de acuerdo con el considerando 90)
2. identificar los impactos potenciales de cada riesgo para los derechos y libertades de las personas físicas
3. identificar las amenazas que podrían provocar estos riesgos
4. estimar la probabilidad y la gravedad de los riesgos (de acuerdo con el considerando 90).

Sobre esta base, y teniendo en cuenta la probabilidad y la gravedad estimadas de cada riesgo, deben concebirse, aplicarse y documentarse en la EIPD las medidas de mitigación apropiadas (según lo dispuesto en la letra d) del apartado 7 del artículo 35 y en el considerando 90).

Dado que los principios de "integridad y confidencialidad" (véase "Integridad y confidencialidad" en la sección "Principios" de la Parte II de estas Directrices). así como las amenazas enumeradas son típicas de la seguridad informática, las medidas aquí documentadas son bien conocidas de esa disciplina. La principal diferencia con la seguridad es la estimación de la gravedad o los impactos que se evalúan en relación con las personas afectadas mucho más que con la organización responsable del tratamiento.

El hecho de que sólo esta sección se refiera a la seguridad informática ilustra aún más la diferencia que ya se ha tratado anteriormente.

5.2.9.4 Participación de las partes interesadas

Según el apartado 2 del artículo 35, "el responsable del tratamiento solicitará el asesoramiento del delegado de protección de datos, cuando sea designado, al realizar una evaluación de impacto sobre la protección de datos".

Asimismo, según el apartado 9 del artículo 35, "cuando proceda, el responsable del tratamiento recabará la opinión de los interesados o de sus representantes sobre el tratamiento previsto, sin perjuicio de la protección de los intereses comerciales o públicos o de la seguridad de las operaciones de tratamiento."

Esta sección de la EIPD documenta que el responsable del tratamiento ha cumplido efectivamente estos dos requisitos. Cuando se hayan recabado las opiniones de los interesados o de sus representantes, la documentación deberá justificar por qué dichas opiniones deben considerarse razonablemente representativas de los interesados en cuestión. Cuando no se hayan recabado las opiniones, la documentación deberá aclarar por qué no fue útil o posible hacerlo.

5.2.10 ¿Qué puede facilitar la realización de una EIPD?

A continuación, se enumeran algunas formas que podrían facilitar la realización de una EIPD.

- En algunos casos en los que el tratamiento tiene una **base jurídica basada en el Derecho de la Unión o de los Estados miembros** (es decir, el artículo 6, apartado 1, letras c) o e) del RGPD), es posible que el legislador ya haya realizado una EIPD. En este caso, a menos que un Estado miembro considere necesaria una EIPD por parte de cada responsable del tratamiento, o a menos que la legislación deje un margen significativo de aplicación al responsable del tratamiento que afecte a los riesgos para los interesados, la **EIPD no tiene que ejecutarse** (véase el artículo 35, apartado 10, del RGPD para más detalles).
    - Un ejemplo lo encontramos en la legislación[272] austriaca sobre "organizaciones de investigación", que ya prevé la realización de EIPD [273] en sus artículos.
- "Hay circunstancias en las que puede ser razonable y económico que el objeto de una evaluación de impacto sobre la protección de datos sea más amplio **que un solo proyecto**" (considerando 90 del RGPD). Obviamente, esto facilita las

[272] véase la Ley federal sobre todos los derechos generales de los ciudadanos, según el artículo 89 de la DSGVO, y la organización de investigación (FOG). 89 DSGVO y la organización de investigación (Forschungsorganisationsgesetz - FOG)
StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB) (NR: GP XV RV 214 AB 778 S. 81. BR: S. 413.), en alemán, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514 (última visita: 30/01/2020).

[273] Véanse los apéndices 4 a 21.

actividades de tratamiento único que pueden remitirse a la " EIPD amplia". Esto se confirma además en el artículo 35, apartado 1, que establece: "Una única evaluación podrá referirse a un conjunto de operaciones de tratamiento similares que presenten riesgos elevados similares". El Grupo de Trabajo del Artículo 29 ofrece aquí una orientación[274] adicional al afirmar que "[una] única EIPD podría utilizarse para evaluar múltiples operaciones de tratamiento que sean similares en **términos de naturaleza, alcance, contexto, finalidad y riesgos**". Además, afirma que "**la EIPD tiene por objeto estudiar sistemáticamente las nuevas situaciones** que podrían entrañar riesgos elevados para los derechos y las libertades de las personas físicas, y **no es necesario realizar una EIPD en los casos** (es decir, las operaciones de tratamiento realizadas en un contexto y con una finalidad específicos) que **ya se han estudiado**". En estos casos, es posible recurrir a la " EIPD amplia" o al menos delegar en ella partes importantes de una EIPD individual. Si no se dispone de una "EIPD amplia", aún pueden existir EIPD individuales de actividades de tratamiento similares que ayuden a realizar una propia.

- El Grupo de Trabajo afirma que "una EIPD también puede ser útil para **evaluar el impacto en la protección de datos de un producto tecnológico**"[275]. Por lo tanto, si un proveedor de tecnología ya ha realizado una EIPD, "el responsable del tratamiento de datos que despliega el producto sigue estando obligado a realizar su propia EIPD en relación con la aplicación específica, pero ésta puede basarse en una EIPD preparada por el proveedor del producto".
- El Grupo de Trabajo señala la posibilidad de que la EIPD se vea facilitada por la existencia de un marco de **EIPD sectorial**: "El Grupo de Trabajo 29 fomenta el desarrollo de marcos de EIPD específicos del sector. Esto se debe a que pueden basarse en conocimientos sectoriales específicos, lo que significa que la EIPD puede abordar las especificidades de un tipo concreto de operación de tratamiento (por ejemplo: tipos particulares de datos, activos corporativos, impactos potenciales, amenazas, medidas)."[276]
- Otra forma posible de facilitar la EIPD es aprovechar **los enfoques sistemáticos que se** utilizan en múltiples actividades de tratamiento. El artículo 24, apartado 2, ofrece el ejemplo de las "**políticas de protección de datos"** en toda la empresa. El artículo 24, apartado 3, añade la "**certificación aprobada**" (según el artículo 42 del RGPD) y los "**códigos de conducta aprobados**" (según el artículo 40 del RGPD). Este último también se menciona específicamente en el artículo 35, apartado 8, del RGPD.

5.2.11 ¿Qué pasa si no lo llevo a cabo? ¿Cuáles son las posibles consecuencias?

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

[274] wp248rev.01, página 7, Sección III. A., 2 ndpárrafo, resaltado añadido por los autores.
[275] wp248rev.01, página 8, sección III. A., 2 ndpárrafo.
[276] wp248rev.01, página 17, Sección III. D.c) .,2°nd párrafo.

cabo una EADP cuando el tratamiento está sujeto a una EADP (artículo 35, apartados 1 y 3 a 4), llevar a cabo una EADP de forma incorrecta (artículo 35, apartados 2 y 7 a 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 de euros o, en el caso de una empresa, de hasta el 2 % del volumen de negocios anual total a nivel mundial del ejercicio financiero anterior, lo que sea mayor."[277]

5.3 Plan de gestión de datos

Tom Lindemann (EUREC)

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

5.3.1 ¿Qué es un plan de gestión de datos?

Un plan de gestión de datos es un elemento clave de la buena gestión de datos y muestra un compromiso proactivo con la integridad científica.

Un Plan de gestión de datos cubre todo el ciclo de vida de la gestión de todos los datos recogidos, generados o procesados por un proyecto de investigación. Por lo general, un Plan de gestión de datos proporciona información sobre:

- el manejo de los datos de la investigación durante y después de un proyecto, incluidas las medidas para garantizar la confidencialidad, si procede;
- que los datos serán recogidos, generados y procesados;
- la metodología y las normas que se aplicarán;
- si los datos serán compartidos;
- cómo se conservarán y preservarán los datos, incluso después del proyecto;
- la ética y la propiedad intelectual.

En otras palabras, un plan de gestión de datos se centra en la recogida, organización, uso, almacenamiento, contextualización, conservación e intercambio de datos. Más concretamente, un plan de gestión de datos define los recursos que se asignan a la gestión de datos, identifica y asigna responsabilidades a los responsables y procesadores de datos y establece procedimientos para proteger, salvaguardar y compartir los datos. Por lo tanto, un Plan de gestión de datos asigna responsabilidades, asigna recursos, garantiza una adecuada protección y salvaguarda de los datos y especifica los mecanismos para compartir los datos de la investigación.

[277] wp248rev.01, página 4, Sección I, 3 rd párrafo.

En lo que respecta a la apertura de la investigación y a la puesta en común de los datos de investigación, los principios FAIR [278]sirven de directrices especialmente importantes. Los principios FAIR se aplican a los datos de investigación (es decir, los datos en los que se basan los procesos de razonamiento científico/las pruebas que respaldan las afirmaciones) y describen cómo los proyectos de investigación pueden garantizar que los datos de investigación sean lo más abiertos posible y lo más cerrados posible.

Esta última disposición es especialmente importante en lo que respecta a los datos personales. Los requisitos de protección de datos sustituyen a los principios FAIR y los invalidan si los datos de la investigación son datos personales. En Europa, los requisitos de protección de datos se derivan del RGPD, la legislación nacional e internacional pertinente y las directrices institucionales. Es importante destacar que el RGPD contiene exenciones para la investigación que facilitan el uso y el almacenamiento de datos con fines de investigación. Si los datos personales se anonimizan, pueden compartirse, ya que los datos anónimos son información que no se refiere a una persona física identificada o identificable, y por tanto el RGPD no se refiere al tratamiento de dicha información anónima, incluso con fines estadísticos o de investigación (véase "Identificación, seudonimización y anonimización" en la parte II, sección "Conceptos" de estas directrices). Dado que la relación entre la ciencia abierta y la protección de datos requiere una aclaración en el panorama normativo actual, los investigadores deben prestar mucha atención a la evolución en curso.[279]

A lo largo de un proyecto, el Plan de Gestión de Datos debe revisarse periódicamente y actualizarse cada vez que se produzcan cambios, por ejemplo, debido a la aparición de nuevos datos o a la incorporación de otros responsables o procesadores de datos. Mantener la información actualizada garantiza que el Plan de gestión de datos siga facilitando las buenas prácticas científicas durante todo el proyecto.

5.3.2 ¿Por qué debería escribir un Plan de Gestión de Datos?

Aunque los proyectos de investigación no están legalmente obligados a adoptar planes de gestión de residuos, deberían hacerlo al menos por tres razones:

- Los planes de gestión de datos ayudan a los investigadores a cumplir la legislación sobre protección de datos y a seguir las mejores prácticas en la apertura de los datos de investigación. De este modo, proporcionan orientación, reducen la incertidumbre y aumentan la transparencia.
- Los organismos de financiación de la investigación condicionan cada vez más la financiación a que se compartan los datos de la investigación, con el fin de apoyar una investigación fiable, transparente y acumulativa.

---

[278] Según los principios FAIR, los datos de investigación deben ser localizables, accesibles, interoperables y reutilizables. Se describen en un artículo de Wilkinson et al. que puede consultarse aquí.

[279] Esto puede hacerse, por ejemplo, consultando el sitio web del Supervisor Europeo de Protección de Datos o del Comité Europeo de Protección de Datos para obtener consejos o un dictamen sobre "protección de datos e investigación científica".

- Las directrices de muchas instituciones de investigación animan a los investigadores a redactar planes de gestión de proyectos.

5.3.3 ¿Estoy obligado legalmente a tener un plan de gestión de datos?

Aunque la redacción de un Plan de gestión de datos **no es actualmente un requisito legal** en el contexto de la investigación europea, se ha convertido en un elemento central de las buenas prácticas científicas. Muchos organismos de financiación de la investigación esperan que los beneficiarios de las subvenciones elaboren un Plan de gestión de datos para promover una buena gestión de los datos. Una de las razones es que la gestión de datos es cada vez más compleja, ya que cada vez se pueden procesar más datos y el número de proyectos multicéntricos sigue aumentando. En consecuencia, los proyectos de investigación que implican el procesamiento de datos deben contar con un Plan de gestión de datos que rija el procesamiento de datos de todo el proyecto. Por lo tanto, como ejemplo de buenas prácticas, debería haber un Plan de gestión de datos por proyecto al que todos los socios puedan remitirse para obtener orientación.

5.3.4 ¿Cuándo debo redactar un plan de gestión de datos?

Los planes de gestión de datos deben redactarse antes o al comienzo de un proyecto de investigación, y revisarse a intervalos regulares durante el proyecto. Los ajustes deben hacerse durante estas revisiones, o siempre que sea necesario debido a cambios significativos, como el uso de nuevos datos, el uso de datos para diferentes fines o la incorporación de nuevos controladores o procesadores de datos. Por ello, los planes de gestión de datos deben ser "documentos vivos" que evolucionan constantemente a lo largo de un proyecto. La gestión de datos, en otras palabras, debe ser una prioridad durante todo el proyecto.

5.3.5 ¿Quién, si es que hay alguien, revisa o aprueba mi plan de gestión de datos?

Un Plan de gestión de datos no suele necesitar la aprobación de un Delegado de Protección de Datos (DPD) o de una autoridad institucional. Sin embargo, las obligaciones precisas que imponen las organizaciones de financiación de la investigación o las directrices institucionales pueden variar. Dado que los planes de gestión de datos describen detalladamente las prácticas de gestión de datos de los proyectos de investigación y asignan responsabilidades, a menudo incluyen información sobre quiénes son los responsables de la protección de datos pertinentes, especialmente en los proyectos que procesan datos personales. En estos casos, suele tener sentido involucrar a los DPD en el proceso de redacción. Además, los DPD suelen ser una buena fuente de asesoramiento y a menudo pueden ayudar a los investigadores a cumplir todas las legislaciones y normas de buenas prácticas pertinentes.

Además, los organismos de financiación de la investigación pueden considerar los Planes de Gestión de Datos como productos formales del proyecto que deben

presentarse y que posteriormente son revisados por expertos que pueden solicitar cambios. Los mecanismos de aprobación, por tanto, varían según las circunstancias y las obligaciones contractuales.

5.3.6 ¿Cuál es la legitimidad y la fuerza coercitiva de los planes de gestión de datos?

Los planes de gestión de datos no son legalmente vinculantes. En cambio, proporcionan orientación, aumentan la transparencia y ayudan a los investigadores a seguir la legislación pertinente, como el RGPD. La fuerza coercitiva reside principalmente en los instrumentos jurídicos (por ejemplo, la ley de protección de datos o la normativa de ciberseguridad) y en los principios rectores acordados (por ejemplo, los principios FAIR de gestión de datos) que el PDC especifica para proyectos de investigación concretos, pero no en los Planes de Gestión de Datos en sí mismos.

Los organismos de financiación de la investigación condicionan cada vez más el desembolso de fondos a la correcta gestión de los datos de investigación, lo que añade "dientes" a los Planes de Gestión de Datos como instrumento. Sin embargo, esto no cambia su estatus legal formal.

5.3.7 ¿Dónde puedo obtener ayuda para redactar un plan de gestión de datos?

Dado que la buena gestión de datos se ha convertido en un elemento central de las buenas prácticas científicas, han proliferado los recursos que ayudan a los investigadores a elaborar planes de gestión de datos. Por ejemplo, los planes de gestión de datos para proyectos financiados por la Comisión Europea en el marco del programa de investigación e innovación Horizonte 2020 deben seguir la plantilla que se ofrece aquí e incluir la información que se explica aquí. Si presenta su propuesta a otro proveedor de fondos, debe comprobar si ofrecen orientación o han formulado requisitos específicos. Otras plantillas y directrices útiles son las proporcionadas, entre otros, por el Digital Curation Centre, DMPTool de la Universidad de California (centrado en EE.UU.), OpenAIRE, la iniciativa Go-FAIR, el Research Data Management Organiser y varias universidades. Antes de redactar un Plan de gestión de datos, conviene comprobar si su universidad o instituto de investigación ha elaborado una plantilla de Plan de gestión de datos. Los responsables de la protección de datos -en caso de que se trate de datos personales- o los Comités de Ética de la Investigación también podrían ayudar a formular su Plan de gestión de datos.

Hay vídeos útiles en YouTube, por ejemplo, OpenAIRE, la Biblioteca de Ciencias de la Salud de la Universidad de Nueva York y el Servicio de Datos del Reino Unido. El Consorcio de Archivos Europeos de Datos de Ciencias Sociales ofrece regularmente seminarios web y cursos de formación sobre la gestión de datos de investigación; véase aquí.

Sin embargo, es importante destacar que muchos de estos recursos contienen poca información sobre qué datos de la investigación deben considerarse datos personales y a los que, por tanto, los requisitos de la ciencia abierta sólo se aplican con importantes

salvedades. Recomendamos no seguir ciegamente las plantillas y recomendaciones enlazadas anteriormente, sino tener en cuenta sus propios requisitos particulares de protección de datos. El plan de gestión de datos debe indicar siempre qué datos se compartirán y cuáles no, y explicar por qué no es posible compartir estos últimos. Es importante que los datos personales anonimizados puedan compartirse, ya que no se consideran datos personales. Los datos personales, en cambio, no pueden compartirse a menos que una base legal lo permita. Las políticas existentes, como la "Política de Privacidad" de una institución, pueden mencionarse en el PDM para subrayar el compromiso de su institución con las cuestiones en cuestión.

5.3.8 ¿Quién debe redactar un PDM?

Cada investigador que trate con datos podría redactar un Plan de gestión de datos para facilitar su propia investigación, cumplir con los principios de integridad científica y hacer visibles desde el principio los posibles conflictos y problemas con la gestión de datos. En un consorcio de investigación, una persona debería ser responsable, pero especialmente en los proyectos de investigación inter y transdisciplinarios todos deberían participar, para tener en cuenta las diferentes perspectivas y necesidades disciplinarias.

Lo que hay que hacer

- Redactar un Plan de gestión de datos antes de iniciar un proyecto de investigación
- Revisar y actualizar su Plan de gestión de datos en el transcurso de un proyecto de investigación
- Esbozar cómo se manejarán los datos de la investigación durante y después de la finalización de un proyecto
- Describir los datos que se recogerán, generarán y procesarán
- Describir la metodología y las normas que se utilizarán
- Especifique si los datos serán compartidos
- respetar la legislación en materia de protección de datos
- Los datos anonimizados pueden compartirse porque no son datos personales
- Describir cómo se conservarán los datos, durante y después de la finalización del proyecto
- Consulte a su DPD en caso de duda
- Seguir la evolución de la legislación sobre protección de datos y la gestión de los datos de investigación
- Obedecer los principios FAIR: localizable, accesible, interoperable, reutilizable

Lo que no hay que hacer

- No siga las recomendaciones a ciegas: muchas recomendaciones generales sobre la gestión de datos de investigación no tienen suficientemente en cuenta los requisitos de protección de datos
- No comparta los datos personales a menos que esté seguro de que es legal hacerlo
- No se abstenga de redactar un PMD, aunque no esté obligado a hacerlo

Lista de comprobación

- ¿Describe mi Plan de gestión de datos con claridad la recogida, organización, uso, almacenamiento, contextualización, preservación y puesta en común de los datos?
- ¿He asignado suficientes recursos a la gestión de datos?
- ¿Están estos recursos claramente asignados?
- ¿Se han asignado las responsabilidades de forma clara e inequívoca?
- ¿Está claro quiénes son los responsables y los encargados del tratamiento de los datos?
- ¿Están claramente especificados los procedimientos de protección y salvaguarda de los datos?
- ¿Está claro qué datos se compartirán, con quién se compartirán y qué datos no se compartirán?
- ¿Se cumplen todos los requisitos de protección de datos?

5.4 Documentación del tratamiento de datos personales

Bud P. Bruegger (ULD)

La versión final de esta sección ha sido validada por Hans Graux, profesor invitado de derecho de las TIC y de protección de la intimidad en el Instituto de Derecho, Tecnología y Sociedad de Tilburg (TILT) y en la AP Hogeschool Antwerpen. Presidente del Vlaamse Toezichtscommissie (Comité Flamenco de Supervisión), que supervisa el cumplimiento de la protección de datos en los organismos del sector público flamenco.

Una organización que procesa datos personales (incluyendo tanto a los controladores[280] como a los procesadores[281]) necesita documentar sus actividades principalmente para el consumo de las Autoridades[282] de Supervisión de Protección de Datos (DPA) competentes. Esto incluye los ***registros de tratamiento***[283] que la organización mantiene de forma centralizada en todas sus actividades de tratamiento y la **documentación adicional** que se refiere a una actividad de tratamiento de datos individual. A continuación, se analizan por separado. El debate se centra en el caso más común para el público al que va dirigido, es decir, que se inicie una nueva actividad de tratamiento dentro de una organización que ya ha designado a un responsable de la protección de datos que ya mantiene registros de tratamiento.

5.4.1 Registros de procesamiento

Los registros del tratamiento pueden conservarse en forma escrita o electrónica[284]. Así que espere rellenar un formulario específico de la organización o introducir su información en algún sistema de gestión (de protección de datos).

Para dar una primera idea, el contenido mínimo de los registros de tratamiento para los controladores incluye los siguientes elementos[285]:

- el **nombre** y los datos de **contacto del responsable del tratamiento**, del **representante del** responsable del tratamiento y del **delegado de protección de datos**;
- los **fines** del tratamiento;
- una descripción de las **categorías de interesados** y de las **categorías de datos personales**;
- las **categorías de destinatarios** a los que se han comunicado o se comunicarán los datos personales;
- en su caso, las **transferencias de datos personales a un tercer país (**véase la sección "Transferencia de datos a terceros países" de la Parte II, en los "Principales instrumentos y acciones" de estas Directrices), junto con la documentación de las garantías adecuadas;

---

280 Véase el art. 30(1) RGPD.
281 Véase el art. 30(2) del RGPD.
282 Véase el art. 58(1)(a), 30(4) y 5(2) del RGPD.
283 Véase el art. 30 RGPD.
284 Véase el art. 30(3) del RGPD.
285 Véase el art. 30(1) del RGPD para más detalles.

- en la medida de lo posible, los **plazos** previstos **para la supresión de las diferentes categorías de datos (**véase la "Limitación del almacenamiento" en la sección "Principios" de la Parte II de estas Directrices);
- cuando sea posible, una descripción general de las **medidas de *seguridad* técnicas y organizativas (**véase "Integridad y confidencialidad" en la sección "Principios" de la Parte II de estas Directrices)

Es posible que su organización utilice un conjunto diferente de elementos, ya que, por un lado, ya está en posesión de parte de esta información (como el primer punto), y por otro lado, puede requerir información adicional (como el contacto de la persona responsable de la actividad de procesamiento única en cuestión). Es posible que el mantenimiento de registros exigido por la ley se combine con las necesidades de gestión de la organización, como un inventario interno de recursos informáticos y de computación.

Su organización también puede utilizar múltiples sistemas, por ejemplo, dependiendo de si actúa como controlador o como procesador; o distinguiendo entre las actividades de procesamiento de datos permanentes (como los sistemas de comunicación y la contabilidad) y las temporales (como las vinculadas a proyectos o asignaciones temporales). La creación y mantenimiento de registros en múltiples sistemas no está prohibida por el RGPD.

Si tiene dificultades para proporcionar la información solicitada, su delegado de protección de datos (si su organización tiene uno) puede ayudarle.

Lista de comprobación (registros de procesamiento)

- Póngase en contacto con la oficina/persona que lleva los registros de tramitación de su organización.
    - Si es necesario, el responsable de la protección de datos puede ayudar a establecer el contacto.
- Infórmeles desde el principio de que tiene intención de procesar datos personales.
    - Su actividad de tramitación tiene que estar inscrita en los registros antes de que se inicie la tramitación.
- Siga sus instrucciones de

- qué información debe proporcionar para los registros de procesamiento,
- cuando necesite enviar actualizaciones de esta información.

5.4.2 Documentación adicional relativa a una única actividad de tratamiento

Además de los registros de tratamiento que se gestionan de forma centralizada en la organización, la persona o personas responsables de una actividad de tratamiento específica tienen que mantener una documentación adicional. Para ello, es una buena práctica establecer una **forma sistemática de recopilar la documentación necesaria** desde el **momento en que se concibe y planifica la actividad de posesión**[286]. Este tipo de información puede ser solicitada por las autoridades de control de la protección de datos tanto a distancia[287] como durante las auditorías[288] in situ. Las medidas necesarias se describen en las siguientes DO:

Lo que hay que hacer

- La protección de datos (como la seguridad) es un proceso, no un estado final. Hay que documentar continuamente ese proceso y no sólo las características finales de la actividad de tratamiento.
- Al aplicar la protección de datos por diseño[289], la actividad de tratamiento puede considerarse el resultado de una serie de consideraciones y decisiones. Son estas consideraciones y decisiones las que deben documentarse.
- Decidir una estructura y un formato para recoger sistemáticamente esta información en el momento de concebir su actividad de tratamiento.
- Cuando la propia documentación contenga información personal (véase más abajo), asegúrese de protegerla suficientemente y de limitar su uso posterior al propósito de demostrar el cumplimiento del RGPD.

Esta documentación comprende al menos lo siguiente, que se enumera primero en una lista de control y se describe después con más detalle.

[286] El art. 25(1) del RGPD lo denomina "el momento de la determinación de los medios para el tratamiento".
[287] Véase el artículo 58(1)(a) del RGPD.
[288] Véase el artículo 58(1)(b) del RGPD.
[289] Véase el art. 25 del RGPD.

5.4.2.1 Evaluación de si la actividad de tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas físicas

Para determinar si es necesaria una evaluación de impacto sobre la protección de datos (EIPD) para una actividad de tratamiento, hay que evaluar si el tratamiento puede suponer un riesgo elevado. Esto se describió en la sección *En qué casos debo realizar una EIPD* en la *Evaluación de Impacto sobre la Protección de Datos* anterior. Se basa en las directrices del Grupo de Trabajo del Artículo 29 y consiste en la evaluación booleana de nueve criterios. Es importante documentar esto, en particular como justificación para el caso en que no sea necesaria una EIPD (véase "EIPD" en la parte II, sección "Principales herramientas y acciones" de estas directrices).

5.4.2.2 Una evaluación de impacto de la protección de datos cuando la evaluación anterior arroje un resultado afirmativo

Cuando es necesaria una EIPD, la propia EIPD forma parte de la documentación del tratamiento. Véase el art. 35 del RGPD y Evaluación de *Impacto de la Protección de Datos* para más detalles.

5.4.2.3 Posible consulta a la autoridad de control competente antes del tratamiento

Cuando la EIPD indique que el tratamiento podría dar lugar a un riesgo elevado incluso después de la mitigación con medidas técnicas y organizativas adecuadas, el responsable del tratamiento consultará a la autoridad de control antes del tratamiento (véase el art. 36(1) DEL RGPD). Dicha consulta debe estar documentada.

5.4.2.4 Requisitos y pruebas de aceptación para la compra y/o el desarrollo del software, el hardware y la infraestructura empleados

De acuerdo con el Art. 25 del RGPD, al determinar los medios de tratamiento, el responsable del tratamiento debe tener en cuenta lo siguiente:

- El estado de la técnica,
- el coste de la aplicación,
- la naturaleza, el alcance, el contexto y los fines del tratamiento, y
- los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas que plantea el tratamiento.

Sobre la base de esta evaluación, el responsable del tratamiento aplica las medidas técnicas y organizativas apropiadas que están diseñadas para aplicar los principios de protección de datos, para cumplir con los requisitos del RGPD y para proteger los derechos de los interesados.

Esta evaluación y las decisiones tomadas tienen que estar documentadas para cumplir con el requisito de **protección de datos por diseño** (del art. 25 del RGPD). En la práctica, esto puede adoptar la forma de:

- **Requisitos de** protección de datos especificados para la compra (por ejemplo, una licitación) o el desarrollo de software, hardware e infraestructura,
- **Pruebas de aceptación** que verifiquen que el software, los sistemas y la infraestructura elegidos son aptos para el propósito y proporcionan la protección y las salvaguardias adecuadas.

Esta documentación puede formar parte de la EIPD.

5.4.2.5 Aplicación de medidas técnicas y organizativas

La documentación también incluirá las medidas técnicas y organizativas que se aplican para mitigar los riesgos de protección de datos y salvaguardar los derechos y libertades de los interesados.

Las medidas de seguridad también forman parte de los *registros de tratamiento* (véase el art. 30(1)(g) RGPD); todas las medidas aplicadas forman parte de la EIPD (véase el Art. 35(7)(d) RGPD).

5.4.2.6 Comprobación periódica, valoración y evaluación de la eficacia de las medidas técnicas y organizativas

El RGPD hace hincapié en la protección de datos como un proceso. Esto es evidente en el Art. 32(1)(d), que exige la comprobación, valoración y evaluación periódicas de la eficacia de las medidas técnicas y organizativas, y en el art. 35(11), que exige que el responsable del tratamiento lleve a cabo una revisión para evaluar si el tratamiento se realiza de conformidad con la evaluación de impacto de la protección de datos, al menos cuando se produzca un cambio en el riesgo que representan las operaciones de tratamiento. Estas pruebas, valoraciones y evaluaciones recurrentes deberán estar documentadas.

5.4.2.7 Requisitos y pruebas de aceptación para la selección de procesadores

De acuerdo con el Art. 28 (1) del RGPD, el responsable del tratamiento utilizará únicamente encargados del tratamiento que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas adecuadas. Esto requiere un proceso de selección que deberá estar documentado.

5.4.2.8 Contratos estipulados con los transformadores

De acuerdo con el art. 28(3) del RGPD, el tratamiento por parte de un encargado se regirá por un contrato que exija, entre otras cosas, la aplicación de medidas y garantías adecuadas (véanse los puntos d y e) y el derecho de inspección y auditoría por parte del responsable del tratamiento (véase el punto h). Estos contactos forman parte de la documentación.

5.4.2.9 Posibles inspecciones y auditorías del procesador

Cuando un responsable del tratamiento inspeccione o audite a un encargado según el art. 28(3)(h), se documentarán las medidas adoptadas y el resultado.

5.4.2.10 Método para recoger el consentimiento

El consentimiento válido requiere el cumplimiento de requisitos estrictos (véase el art. 4(11) y 7 del RGPD). Cuando un responsable del tratamiento elige el consentimiento como base jurídica para (parte del) tratamiento, la forma (por ejemplo, el diálogo) en que se recogió el consentimiento debe documentarse para demostrar que se cumplieron los requisitos. Cuando los diálogos cambian con el tiempo, es necesario un control de versiones que registre el momento del cambio.

5.4.2.11 Demostraciones de expresiones individuales de consentimiento

De acuerdo con el art. 7, apartado 1, el responsable del tratamiento deberá poder demostrar que el interesado ha consentido el tratamiento de sus datos personales. Este requisito es analizado con más detalle por el *Comité Europeo de Protección de Datos (CEPD),* en sus *Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679*[290]. Una posible forma de demostrar el consentimiento que describen es "conservar información sobre la sesión en la que se expresó el consentimiento, junto con la documentación del flujo de trabajo del consentimiento en el momento de la sesión, y una copia de la información que se presentó al sujeto de los datos en ese momento."[291]

Esto ilustra que la documentación para poder demostrar el consentimiento en sí misma debe considerarse como datos personales. Por lo tanto, debe protegerse adecuadamente y su uso debe limitarse a la finalidad de dicha demostración.

5.4.2.12 Información facilitada a los interesados

Los arts. 13 y 14 del RGPD exigen que el responsable del tratamiento proporcione a los interesados información adecuada sobre el tratamiento. Para demostrar el cumplimiento, se documentará la información realmente proporcionada. De nuevo, es necesario un control de versiones si la información proporcionada cambia con el tiempo.

5.4.2.13 Aplicación de los derechos del interesado

Los artículos 15 a 22 obligan al responsable del tratamiento a conceder a los interesados derechos específicos (como, por ejemplo, el derecho de rectificación de los datos

---

[290] Sección 5.1, páginas 21 y 22 en Comité Europeo de Protección de Datos (CEPD), *Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0,* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Última visita 11/05/2020).

[291] Véase al final del apartado 108.

inexactos o el derecho a ser olvidado) (véase "Derechos del interesado" en la Parte II de estas Directrices). Además, cuando el tratamiento se basa en el consentimiento, los interesados tienen derecho a retirarlo en cualquier momento (véase el art. 7(3) del RGPD). Para demostrar el cumplimiento, es necesario documentar cómo se aplican estos derechos[292]. Una vez más, puede ser necesario el control de versiones.

5.4.2.14 Tratamiento real de los derechos de los interesados

Cuando los interesados invoquen sus derechos, el responsable del tratamiento los tramitará sin demora. Los apartados 3 y 4 del art. 12(3) y (4) especifica los tiempos máximos de respuesta aceptables. Para demostrar la exactitud y la puntualidad de las acciones emprendidas y la respuesta enviada, es necesaria una documentación. Una vez más, esta documentación constituye datos personales y tiene que estar adecuadamente protegida.

5.4.2.15 Posibles notificaciones de infracciones a la autoridad de supervisión competente

El art. 33 del RGPD exige la notificación de una violación de los datos personales a la autoridad de control. Estas notificaciones pasarán a formar parte de la documentación.

5.4.2.16 Posible comunicación de las violaciones de datos al interesado

El artículo 34 del RGPD exige la comunicación de una violación de los datos personales al interesado en determinadas condiciones. Estas comunicaciones deberán estar documentadas. Es probable que contengan datos personales que necesiten protección.

5.4.2.17 Cualquier otra comunicación con la autoridad de control competente

Toda comunicación con una autoridad de control debe estar documentada. Dicha comunicación puede ser iniciada, por ejemplo, por la autoridad de control de acuerdo con el art. 31 del RGPD. La comunicación iniciada por el responsable del tratamiento según el art. 36 ya se ha enumerado anteriormente. Además, los responsables de la protección de datos también pueden consultar a las autoridades de control con arreglo al artículo 39, apartado 1, letra e). 39(1)(e).

Lista de comprobación (documentación adicional relativa a una única actividad de procesamiento)

Deben documentarse los siguientes elementos:

- Evaluación de si la actividad de tratamiento puede suponer un alto riesgo para

[292] El término "implementado" no pretende implicar la automatización; el procesamiento manual, por ejemplo, por el responsable de la protección de datos u otra persona designada, puede ser perfectamente aceptable.

los derechos y libertades de las personas físicas.

- Una evaluación del impacto de la protección de datos cuando la evaluación anterior arroje un resultado afirmativo.
- Posible consulta a la autoridad de control competente antes del tratamiento.
- Requisitos y pruebas de aceptación para la compra y/o el desarrollo del software, el hardware y la infraestructura empleados.
- Implementación de medidas técnicas y organizativas.
- Comprobación, valoración y evaluación periódicas de la eficacia de las medidas técnicas y organizativas
- Requisitos y pruebas de aceptación para la selección de procesadores.
- Contratos estipulados con los transformadores.
- Posibles inspecciones y auditorías del procesador.
- Método para recoger el consentimiento.
- Demostraciones de expresiones individuales de consentimiento.
- Información proporcionada a los interesados.
- Aplicación de los derechos de los interesados.
- Tratamiento real de los derechos de los interesados.
- Posibles notificaciones de infracciones a la autoridad de supervisión competente.
- Posible comunicación de las violaciones de datos al interesado.
- Cualquier otra comunicación con la autoridad de control competente.

5.5 Interés legítimo y prueba de equilibrio

Iñigo de Miguel Beriain (UPV/EHU)

Agradecimientos: El autor agradece los consejos, las aportaciones y los comentarios sobre los borradores de Bud P. Bruegger y Harald Zwingelberg.

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

El interés legítimo es una de las seis bases jurídicas para el tratamiento de datos personales establecidas en el artículo 6, apartado 1, del RGPD (véase la subsección

"Legalidad, equidad y transparencia" en los "Principios" de la Parte II de estas Directrices). Esta base jurídica requiere que los intereses legítimos del responsable del tratamiento o de los terceros a los que se comunican los datos prevalezcan sobre los intereses, los derechos fundamentales y las libertades de los interesados (artículo 6, apartado 1, letra f). Para comprobar que esto es así, los responsables del tratamiento pueden hacer uso de una herramienta denominada ***prueba de equilibrio***, recomendada, por ejemplo, por el Grupo de Trabajo del Artículo 29[293]. Esta herramienta tiene por objeto garantizar que los intereses legítimos del responsable del tratamiento o de los terceros a los que se comunican los datos prevalecen sobre los intereses y los derechos y libertades fundamentales de los interesados.

5.5.1 ¿Cuándo no prevalecen los derechos y libertades fundamentales de la persona afectada por la protección de datos?

Llevar a cabo una prueba de equilibrio implica considerar varios factores clave que son decisivos para determinar qué intereses, libertades o derechos prevalecen, a saber: [294]

- La naturaleza y el origen del interés legítimo: si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, si es de interés público o si goza de reconocimiento en la comunidad en cuestión. Es obligatorio evaluar el posible perjuicio sufrido por el responsable del tratamiento, por terceros o por la comunidad en general si el tratamiento de datos no se lleva a cabo.
- El **poder y el estatus de las dos partes** (responsable del tratamiento o tercero y sujeto de los datos). Por ejemplo, un empresario que pretende tratar los datos de un empleado está en una posición más fuerte que el empleado. Si el interesado es un menor de edad, sus intereses, derechos o libertades deben ser ponderados.
- **La naturaleza de los datos.** Aunque el tratamiento de cualquier dato personal debe ponderarse adecuadamente, el tratamiento de categorías especiales de datos personales, como el origen racial, las creencias religiosas, los datos genéricos o los datos relativos a la salud, debe tener mayor peso.
- **El impacto del tratamiento en los interesados.** Para ello, los responsables del tratamiento deben considerar si el tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas. Si este es el caso, deben realizar una EIPD.

---

[293] A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p. 24. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consultado el 05 de enero de 2020

[294] A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p. 24. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consultado el 5 de enero de 2020.

- Las **expectativas razonables de los interesados** sobre lo que ocurrirá con sus datos. Los responsables del tratamiento deben ser capaces de demostrar que un interesado esperaría el tratamiento a la luz de las circunstancias particulares aplicables. Si la finalidad y el método de tratamiento no son inmediatamente obvios y existe la posibilidad de que haya una serie de opiniones razonables sobre si la gente lo esperaría, los responsables del tratamiento podrían llevar a cabo algún tipo de consulta, grupo de discusión o estudio de mercado con las personas para demostrar las expectativas y apoyar su posición. Si existen estudios previos sobre las expectativas razonables en un contexto concreto, los responsables del tratamiento pueden basarse en ellos para determinar lo que los individuos pueden o no esperar.[295]
- La **forma en que se procesan los datos** (a gran escala, extracción de datos, elaboración de perfiles, divulgación a un gran número de personas o publicación);
- **Las salvaguardias adicionales** que podrían limitar el impacto indebido sobre el interesado, como la minimización de los datos (por ejemplo medidas técnicas y organizativas que garanticen que los datos no puedan utilizarse para tomar decisiones u otras acciones con respecto a las personas ("separación funcional") - amplio uso de técnicas de anonimización, agregación de datos, tecnologías que mejoren la privacidad, privacidad por diseño, evaluaciones de impacto sobre la privacidad y la protección de datos; - mayor transparencia, derecho general e incondicional a oponerse (opt-out), portabilidad de datos y medidas relacionadas para capacitar a los interesados, etc.

5.5.2 La cuestión de la salvaguardia adicional

El Grupo de Trabajo del Artículo 29 considera que las medidas de mitigación y las salvaguardias, como las medidas organizativas o técnicas adoptadas por el responsable del tratamiento para la protección de los datos del interesado, deben incluirse en la prueba de equilibrio. Sin embargo, existe un enfoque alternativo, que considera que el artículo 6.1.f) pide una prueba de equilibrio entre dos valores, los intereses legítimos del responsable del tratamiento (o de un tercero) y los intereses, derechos y libertades del interesado. Las medidas paliativas y las salvaguardias no se ajustan a ninguno de estos valores. Por lo tanto, no deben considerarse. De lo contrario, tendrían un peso excesivo para los responsables del tratamiento, ya que restarían importancia al posible daño que

[295] ICO, ¿Cómo aplicamos los intereses legítimos en la práctica? En: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Consultado: 15 de enero de 2020

se causaría a los intereses, derechos y libertades del interesado. Kamara y De Hert han hecho algunas declaraciones convincentes sobre esta cuestión concreta, al afirmar que[296]

> "la *inclusión de medidas de mitigación en la evaluación llevaría a una representación del impacto real previsto del tratamiento para los derechos de los interesados, y seguiría permitiendo que prevalecieran los intereses legítimos. Este enfoque no "castiga" al responsable del tratamiento que adopta medidas de mitigación y salvaguardias, al no incluirlas en la prueba de sopesamiento. Por el contrario, anima al responsable del tratamiento a hacerlo. Por otra parte, hay que tener en cuenta que el peso de las futuras salvaguardias y medidas de mitigación es siempre relevante para su realización y eficacia. Por lo tanto, dichas medidas deben tenerse en cuenta, pero no deben desempeñar un papel significativo a la hora de determinar hacia qué lado se inclina la balanza."*

Lo que hay que hacer

- Compruebe la naturaleza de los datos tratados y preste especial atención a las categorías especiales de datos personales (sobre todo si los interesados son niños).
- Considerar las expectativas razonables de los interesados
- Realizar una EIPD si las circunstancias lo recomiendan

Lo que no hay que hacer

- No trate categorías especiales de datos personales si no es absolutamente necesario para alcanzar el interés perseguido
- No procesar los datos si la prueba de equilibrio no es concluyente
- No dude en introducir salvaguardias adecuadas para minimizar el perjuicio a los intereses, derechos y libertades de los interesados

Lista de comprobación

- Los responsables del tratamiento se han asegurado de que los intereses de la persona no prevalecen sobre los intereses legítimos del responsable del tratamiento o de terceros.

[296] Kamara, Irene y De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. En: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Consultado: 17 de enero de 2020

- Los responsables del tratamiento utilizan los datos de los interesados de la forma que razonablemente cabría esperar.
- Los responsables del tratamiento no utilizan los datos de los interesados de forma muy intrusiva o que pueda causarles un perjuicio, a menos que tengan una razón especialmente buena.
- Los responsables del tratamiento no tratan categorías especiales de datos personales o, si lo hacen, se han asegurado de que se apliquen las garantías técnicas y organizativas adecuadas en el tratamiento.
- Los controladores han estudiado las salvaguardias para reducir el impacto en la medida de lo posible.
- Los controladores han considerado si necesitan realizar una EIPD.

5.5.3 Más información

- El Grupo de Trabajo del Artículo 29 proporcionó ejemplos adicionales de pruebas de equilibrio, que pueden encontrarse en su Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE
- A29WP, Dictamen 06/2014 sobre el concepto de intereses legítimos del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE. Abril de 2014, p. 24. En: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
- SEPD, Evaluación de la necesidad de medidas que limiten el derecho fundamental a la protección de datos personales: A Toolkit, 11 de abril de 2017, en: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Consultado el 5 de mayo de 2020
- ICO, ¿Cómo aplicamos los intereses legítimos en la práctica? En: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/
- ICO, ¿Qué es la base de los "intereses legítimos"? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Consultado el 5 de mayo de 2020.
- Kamara, Irene y De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. En: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

5.6 Transferencia de datos a terceros países

Mikel Recuero Linares (UPV/EHU)

Esta parte de las Directrices ha sido revisada y validada por Marko Sijan, Asesor Superior Especialista, (HR DPA)

El RGPD no define expresamente qué se entiende por transferencia de datos a terceros países u organizaciones internacionales (en adelante, "transferencia internacional"). Sin embargo, el régimen de las transferencias internacionales se establece explícitamente en los artículos 44 a 50 del Reglamento. Por lo tanto, la definición de transferencia internacional debe deducirse evaluando cada concepto por separado, lo que dará lugar a la siguiente definición:

La operación de tratamiento por la que un responsable o un encargado del tratamiento dentro del EEE ("exportador de datos") transfiere (o da acceso a) datos personales a un responsable o encargado del tratamiento fuera del EEE ("importador de datos") o a una organización internacional.

Cualquier transferencia de dato personal a país tercero u organización internacional

Tercer país:	**Organización internacional**:
Un país situado fuera del Espacio Económico Europeo (EEE), que incluye todos los países de la UE e Islandia, Liechtenstein y Noruega.	una organización de derecho internacional público o cualquier otro organismo creado por un acuerdo entre dos o más países o sobre la base de dicho acuerdo

Requisitos generales:

Cumplimiento total del RGPD + al menos uno de los mecanismos del Capítulo V

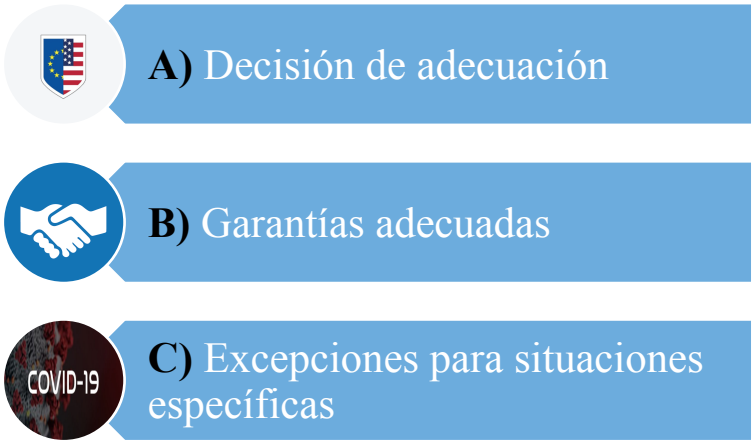
Estas transferencias son perfectamente aceptables y, a menudo, necesarias, pero no deben socavar el nivel de protección de las personas afectadas dado en la UE o concedido por el RGPD. Por lo tanto, las transferencias a terceros países u organizaciones internacionales deben realizarse en pleno cumplimiento del capítulo V del RGPD.

5.6.1 Requisitos

Las transferencias de datos personales a terceros países y organizaciones internacionales sólo podrán realizarse:

i. **Cuando el responsable o el encargado del tratamiento hayan cumplido las demás disposiciones del RGPD[297].** Antes de llevar a cabo la transferencia internacional, también deben cumplirse las disposiciones y requisitos del RGPD. Además de las normas específicas del capítulo V aplicables a las transferencias de datos, el importador y el exportador de datos tendrán que cumplir "las demás disposiciones del presente Reglamento" (por ejemplo, los principios generales, la base jurídica, las excepciones para el tratamiento de datos sensibles, etc.).

ii. **Cuando el responsable o el encargado del tratamiento cumplan las condiciones específicas establecidas en relación con las transferencias de datos personales**. Esto puede llevarse a cabo, principalmente, a través de tres instrumentos, en este orden exacto:



iii. **Estos principios y requisitos no sólo se aplicarán a la primera transferencia de datos, sino también a las transferencias posteriores a otros responsables o encargados del tratamiento en el mismo país o en otro tercer país u organización[298] internacional.**

A) Traslados sobre la base de una decisión de adecuación

En primer lugar, sólo se puede realizar una transferencia si está amparada por una decisión de adecuación. Esta decisión es una resolución de la Comisión Europea que establece que el marco jurídico vigente en ese país, territorio, sector u organización

297 Véase el artículo 44 del RGPD "Toda transferencia de datos personales (...) sólo tendrá lugar si, sin perjuicio de las demás disposiciones del presente Reglamento (...)".

298 Véase el artículo 44 *in fine* del RGPD.

internacional ofrece una protección "adecuada" de los derechos y libertades de las personas para sus datos[299] personales. Una "decisión de adecuación" es un acto de ejecución de la Comisión [300]adoptado con arreglo a un procedimiento de examen [301]y sujeto a una revisión periódica.

La adopción de una decisión de adecuación implica:

- una propuesta de la Comisión Europea;
- un dictamen del Comité Europeo de Protección de Datos (CEPD);
- una aprobación de los representantes de los países de la UE; y
- La adopción de la decisión por parte de los Comisarios Europeos.

El objetivo de esta decisión es, por tanto, evaluar si un país, territorio, sector u organización internacional ofrece un nivel "adecuado" de protección de los derechos y libertades de las personas (véase Derechos del interesado en la parte II de estas Directrices). Además, el artículo 45, apartado 2, del RGPD enumera los elementos que la Comisión tendrá en cuenta, en particular, al evaluar la adecuación del nivel de protección en un tercer país u organización internacional.

Las ventajas de basarse en las decisiones de adecuación para realizar transferencias internacionales son evidentes. La decisión tendrá efectos en toda la UE [302]y no se necesitará una autorización específica[303]. Sin embargo, este mecanismo también presenta varias deficiencias:

- **Hay muy pocos países con decisiones de adecuación válidas en vigor[304].**
- **Las decisiones de adecuación en vigor no se aplican necesariamente a y/o cubren todas las operaciones y sectores de transformación.**
- **La jurisprudencia del Tribunal de Justicia de la Unión Europea ha disminuido significativamente la solidez y la confianza en estas herramientas.** Cabe referirse específicamente a sus [305]sentencias Schrems I[306] y II, que, entre otras cuestiones, anularon las decisiones "Safe Harbour" y "Privacy Shield", respectivamente:
    - El término "adecuado" debe entenderse como la exigencia de que el tercer país garantice de hecho, en virtud de su Derecho interno o de sus compromisos internacionales, un nivel de protección de los derechos y libertades fundamentales esencialmente equivalente al garantizado en la

299 Artículo 45(1) del RGPD.
300 Artículo 45(3) del RGPD.
301 Artículo 93(2) del RGPD.
302 Considerando 103 del RGPD.
303 Artículo 45(1) *in fine* del RGPD.
304 Tras la nueva anulación del Escudo de la privacidad por parte del TJUE, actualmente solo hay decisiones en vigor con: Andorra, Argentina, Canadá (organizaciones comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay.
305 Tribunal de Justicia de la Unión Europea. Sentencia de 6 de octubre de 2015, Maximillian Schrems/Comisario de Protección de Datos (C-362/14, Schrems I).
306 Tribunal de Justicia de la Unión Europea. Sentencia de 16 de julio de 2020, Comisario de Protección de Datos contra Facebook Ireland Ltd, Maximillian Schrems, (C-311/18, Schrems II)

UE[307], aunque los medios a los que recurra ese tercer país puedan ser diferentes de los empleados en la UE[308].

- Las autoridades nacionales de control están facultadas para comprobar si una transferencia de datos personales desde su propio Estado miembro a un tercer país se ajusta a las normas[309] europeas de protección de datos. Sin embargo, por regla general, mientras la decisión de la Comisión no sea declarada inválida por el TJUE, los Estados miembros y las autoridades de control no pueden adoptar medidas contrarias a dicha decisión[310]. Esto no puede impedir que las personas cuyos datos personales han sido o podrían ser transferidos a un tercer país presenten una reclamación[311].
- La legislación que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas debe considerarse que compromete la esencia de los derechos fundamentales de los interesados[312] europeos. Del mismo modo, una legislación que no prevea ninguna posibilidad de que una persona pueda interponer recursos judiciales para tener acceso a los datos personales que le conciernen, o para obtener su rectificación o supresión, no respeta la esencia del derecho fundamental a la tutela[313] judicial efectiva.

B) Transferencias sujetas a las garantías adecuadas

En ausencia de una "decisión de adecuación", un responsable o un encargado del tratamiento puede transferir datos personales a un tercer país o a una organización internacional sólo si el responsable o el encargado del tratamiento ha proporcionado las garantías adecuadas, y a condición de que se disponga de derechos exigibles de los interesados y de recursos jurídicos efectivos para los mismos[314]. Es decir, si no existe una "decisión de adecuación" sobre el país, el territorio o el sector al que se va a realizar la transferencia, el responsable o el encargado del tratamiento puede elegir entre los mecanismos establecidos en el artículo 46 del RGPD para ofrecer "garantías adecuadas".

En la aplicación de los mecanismos del artículo 45 no es necesario observar un orden específico. Es posible elegir los mecanismos en función de las necesidades particulares o de la finalidad del tratamiento. Sin embargo, el RGPD clasifica estos mecanismos en función de si requieren o no una autorización específica de una autoridad de control:

---

307 Tribunal de Justicia de la Unión Europea. Sentencia de 6 de octubre de 2015, Maximillian Schrems contra el Comisario de Protección de Datos (C-362/14, Schrems I). Parag. 73.
308 Ibid. parag. 74.
309 Ibid. parag. 47.
310 Ibid. parag. 52.
311 Ibid. parag. 53 y 66.
312 Sentencia del TJUE de 16 de julio de 2020, Comisario de Protección de Datos contra Facebook Ireland Ltd, Maximillian Schrems, (C-311/18, Schrems II) Parag. 185.
313 Ibid. parag. 197 y 198.
314 Art. 46 del RGPD.

i. **Mecanismos que no requieren ninguna autorización específica de una autoridad[315] de supervisión:**

a) Instrumentos jurídicamente vinculantes y ejecutables entre autoridades u organismos públicos. Por ejemplo, acuerdos administrativos que incluyan derechos individuales exigibles y efectivos

b) Normas corporativas vinculantes (*Binding Corporate Rules* o *BCR*). Éstas se utilizan habitualmente para las transferencias de datos dentro de las empresas multinacionales. Las *BCR* son un código de conducta interno que funciona dentro de un grupo multinacional y que se aplica a las transferencias restringidas de datos personales de las entidades del grupo en el EEE a entidades del grupo fuera del EEE. Hay muchos documentos sobre las *BCR* adoptados por el Comité Europeo de Protección de Datos y el antiguo Grupo de Trabajo del Artículo 29[316]

c) Cláusulas contractuales tipo adoptadas por la Comisión. También se conocen como cláusulas modelo. Contienen las obligaciones contractuales del exportador de datos y del importador de datos, así como los derechos de las personas. Por lo tanto, deben firmarse entre el exportador de datos (país de las CEA) y el importador de datos (país de las CEA u organización internacional). La Comisión Europea adoptó modelos de CCE para los responsables del tratamiento y para los encargados del mismo[317].

d) Un código de conducta aprobado. La transferencia puede llevarse a cabo si el receptor ha suscrito un código de conducta previamente aprobado por una autoridad de control. El código de conducta debe incluir un contenido y unos requisitos mínimos de conformidad con el artículo 40 del RGPD (es decir, garantías adecuadas para proteger los derechos de las personas). El Comité Europeo de Protección de Datos ha adoptado un conjunto de directrices sobre códigos de conducta.[318] Todavía no se utiliza ningún código aprobado. Sin embargo, muchas instituciones y organizaciones están desarrollando códigos (por ejemplo, el BBMRI-ERIC está desarrollando un Código de Conducta para la Investigación en Salud).[319]

e) Una certificación aprobada. La transferencia puede llevarse a cabo si el receptor dispone de una certificación, en virtud de un régimen aprobado

---

315 En virtud del art. 46.2 del RGPD.

316 CE. Normas corporativas vinculantes. En: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en Consultado el 12 de mayo de 2020.

317 Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. C/2021/3972. DO L 199 de 7.6.2021, p. 31-61. Disponible en: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

318 Comité Europeo de Protección de Datos (CEPD). Directrices 1/2019 sobre los códigos de conducta y los organismos de supervisión en virtud del Reglamento 2016/679 Versión 2.0 4 de junio de 2019. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf Consultado el 12 de mayo de 2020

319 *BBMRI-ERIC, Code of conduct for health research: taking up speed & calling for your input*, En: https://www.bbmri-eric.eu/news-events/code-of-conduct-for-health-research/ Consultado el 12 de mayo de 2020

por una autoridad de control. El mecanismo de certificación debe incluir un contenido y unos requisitos mínimos de conformidad con el artículo 40 del RGPD (es decir, garantías adecuadas para proteger los derechos de las personas). El Comité Europeo de Protección de Datos, ha adoptado un conjunto de directrices sobre mecanismos de certificación[320]. Todavía no se utiliza ningún mecanismo de certificación aprobado.

ii. **Mecanismos que requieren autorización de la autoridad de supervisión competente:**

a) Cláusulas contractuales autorizadas por una autoridad de supervisión. Aunque no se utilicen los modelos de cláusulas adoptados por la Comisión Europea, pueden adoptarse otros modelos de CSC si son aprobados previa e individualmente por la autoridad de supervisión competente.

b) Disposiciones que deben incluirse en los acuerdos administrativos entre autoridades u organismos públicos que incluyan derechos exigibles y efectivos de los interesados, por ejemplo, un documento como un memorando de entendimiento.

No obstante, la jurisprudencia derivada de la sentencia Schrems II del Tribunal de Justicia de la Unión Europea ha tenido importantes consecuencias para las cláusulas contractuales tipo y el resto de mecanismos de transferencia de datos a terceros países sobre la base de garantías adecuadas. En primer lugar, porque los interesados cuyos datos personales se transfieren a un tercer país en virtud de las cláusulas contractuales tipo (u otros mecanismos) deben gozar, como en el contexto de una decisión de adecuación, de un nivel de protección esencialmente equivalente al garantizado en la Unión Europea[321]. En segundo lugar, porque esto puede requerir, en función de la posición imperante en un tercer país concreto, la adopción de medidas complementarias por parte del responsable del tratamiento para garantizar el cumplimiento de ese nivel de protección[322]. En consecuencia, si el exportador de datos establecido en la UE no puede adoptar las medidas complementarias adecuadas, está obligado a suspender o prohibir la transferencia de datos personales "en caso de incumplimiento de dichas cláusulas o de imposibilidad de cumplirlas"[323].

C) Excepciones para situaciones específicas

Por último, cuando la transferencia no esté amparada por una decisión de adecuación, ni por un mecanismo de salvaguardia adecuado, sólo se llevará a cabo si

320 Comité Europeo de Protección de Datos (CEPD). Directrices 1/2018 sobre la certificación y la identificación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento Versión 3.0 4 de junio de 2019. En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf. Consultado: 12 de mayo de 2020.

321 Tribunal de Justicia de la Unión Europea. Sentencia de 16 de julio de 2020, *Comisario de Protección de Datos contra Facebook Ireland Ltd, Maximillian Schrems*, (C-311/18, *Schrems II*). Parag. 96.

322 Ibid. Parag. 132 y 125.

323 Ibid. Parag. 134 y 135.

está amparada por alguna de las excepciones o situaciones excepcionales establecidas en el artículo 49 del RGPD[324]:

i. Cuando el interesado haya dado su consentimiento explícito a la transferencia propuesta.
ii. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o la aplicación de medidas precontractuales adoptadas a petición del interesado.
iii. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado en interés del interesado entre el responsable del tratamiento y otra persona física o jurídica.
iv. Cuando la transferencia sea necesaria por razones importantes de interés público.
v. Cuando la transferencia sea necesaria para el establecimiento, ejercicio o defensa de reclamaciones legales.
vi. Cuando la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o legalmente incapacitado para dar su consentimiento.
vii. Cuando la transferencia se realice desde un registro que, según el Derecho de la Unión o de los Estados miembros, esté destinado a proporcionar información al público y que esté abierto a la consulta del público en general o de cualquier persona que pueda demostrar un interés legítimo.

5.6.2 Más información

Grupo de Trabajo de Protección de Datos del Artículo 29. Recomendación sobre la aprobación del formulario de normas corporativas vinculantes para los procesadores. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51307

Grupo de Trabajo de Protección de Datos del Artículo 29. Recomendación sobre la solicitud estándar de aprobación de normas corporativas vinculantes para el controlador para la transferencia de datos personales. https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf

Tribunal de Justicia de la Unión Europea. Sentencia de 16 de julio de 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, (C-311/18, *Schrems II*).

Tribunal de Justicia de la Unión Europea. Sentencia de 6 de octubre de 2015, Maximillian Schrems/Comisario de Protección de Datos (C-362/14, Schrems I).

324 Más información sobre el art. 49 derogaciones y excepciones se puede encontrar en el Comité Europeo de Protección de Datos (CEPD), Directrices 2/2018 sobre las derogaciones del artículo 49 en virtud del Reglamento 2016/679 Adoptado el 25 de mayo de 2018, En: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf Accedido: 14 de mayo de 2020

Comisión Europea. Normas Corporativas Vinculantes (BCR). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

Comisión Europea. Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. C/2021/3972. DO L 199 de 7.6.2021, p. 31-61. Disponible en: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Comisión Europea. Normas sobre transferencias internacionales de datos. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

Comité Europeo de Protección de Datos (CEPD). Directrices 1/2018 sobre la certificación y la identificación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

Comité Europeo de Protección de Datos (CEPD). Directrices 1/2019 sobre los códigos de conducta y los organismos de control en virtud del Reglamento 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

Comité Europeo de Protección de Datos (CEPD). Directrices 2/2018 sobre las excepciones del artículo 49 del Reglamento 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf