Directrices 4/2019 relativas al artículo 25

Protección de datos desde el diseño y por defecto

Versión 2.0

Adoptadas el 20 de octubre de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historial de versiones

Versión 1.0	13 de noviembre de 2019	Adopción de las Directrices para consulta pública
Versión 2.0	20 de octubre de 2020	Adopción de las Directrices por el CEPD tras la consulta pública

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, el «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, en su versión modificada por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018,

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES:

Resumen ejecutivo

En un mundo cada vez más digital, el cumplimiento de los requisitos de protección de datos desde el diseño y por defecto desempeña un papel crucial en la promoción de la privacidad y la protección de datos en la sociedad. Por consiguiente, es esencial que los responsables del tratamiento asuman esta responsabilidad con seriedad y apliquen las obligaciones del RGPD en el diseño de las operaciones de tratamiento.

Las presentes Directrices ofrecen orientaciones generales sobre la obligación de protección de datos desde el diseño y por defecto (en lo sucesivo, «PDDD») establecida en el artículo 25 del RGPD. La PDDD es una obligación para todos los responsables del tratamiento de datos personales, con independencia de la dimensión y la complejidad del tratamiento. Para poder aplicar los requisitos de PDDD, es crucial que el responsable del tratamiento entienda los principios de protección de datos y los derechos y libertades de los interesados.

La obligación esencial es la aplicación de medidas *adecuadas* y las garantías necesarias para la *aplicación efectiva* de los *principios de protección de datos* y, en consecuencia*, los derechos y libertades de los interesados desde el diseño y por defecto*. El artículo 25 establece los elementos desde el diseño y por defecto que deben tenerse en cuenta. Dichos elementos se explican con más detalle en las presentes Directrices.

El artículo 25, apartado 1, estipula que los responsables del tratamiento deben tener en cuenta la PDDD desde el momento en que comienzan a planificar una nueva operación de tratamiento. Los responsables del tratamiento aplicarán la PDDD *antes* del tratamiento, y también *de forma continuada* en el momento del tratamiento, revisando regularmente la efectividad de las medidas y garantías elegidas. La PDDD también se aplica a los sistemas ya existentes que tratan datos personales.

Estas Directrices también contienen orientaciones prácticas sobre cómo aplicar de manera efectiva los principios de protección de datos del artículo 5, enumeran los elementos clave desde el diseño y por defecto y presentan casos prácticos a título ilustrativo. El responsable del tratamiento debe considerar si las medidas propuestas son adecuadas en el contexto del tratamiento en cuestión.

El CEPD ofrece recomendaciones sobre formas de cooperación entre los responsables y encargados del tratamiento y los productores para cumplir con sus obligaciones de PDDD. Anima a los responsables

del tratamiento en la industria, a los encargados del tratamiento y a los productores a utilizar la PDDD como medio de conseguir una ventaja competitiva en la comercialización de sus productos para los responsables del tratamiento y los interesados. También anima a todos los responsables del tratamiento a utilizar certificaciones y códigos de conducta.

1 ÁMBITO

1. Las Directrices se centran en la aplicación de la PDDD por parte de los responsables del tratamiento, con base en la obligación establecida en el artículo 25 del RGPD.[1] Otros operadores, como los encargados del tratamiento y los proveedores de productos, servicios y aplicaciones (en lo sucesivo, «productores»), que no se mencionan directamente en el artículo 25, también pueden encontrar estas Directrices útiles para crear productos y servicios conformes con el RGPD que permitan a los responsables del tratamiento cumplir con sus obligaciones en materia de protección de datos.[2] El considerando 78 del RGPD agrega que la PDDD debe tenerse en cuenta en el contexto de las licitaciones públicas. A pesar de que todos los responsables tienen el deber de integrar la PDDD en sus actividades de tratamiento, esta disposición fomenta la adopción de los principios de protección de datos, y en este sentido las administraciones públicas deben predicar con el ejemplo. El responsable del tratamiento es el responsable del cumplimiento de las obligaciones en materia de PDDD que afectan a las operaciones de tratamiento realizadas por sus encargados y subencargados y, por tanto, debe tener esto en cuenta a la hora de formalizar contratos con ellos.

2. El requisito descrito en el artículo 25 es que los responsables del tratamiento deben integrar la protección de datos en el diseño del tratamiento de datos personales y como opción por defecto, y esto es aplicable durante todo el ciclo de tratamiento. La PDDD también es obligatoria para los sistemas de tratamiento que ya existían antes de que el RGPD entrase en vigor. Los responsables deben velar por que el tratamiento se actualice sistemáticamente con arreglo al RPGD. Para más información sobre cómo mantener el cumplimiento de la PDDD en un sistema ya existente, véase el apartado 2.1.4 de estas Directrices. Lo fundamental de esta disposición es velar por una protección *adecuada* y *efectiva* de los datos *desde el diseño* y *por defecto*, lo que significa que los responsables del tratamiento deben poder acreditar que han incorporado las medidas oportunas y las garantías necesarias en el tratamiento para que los principios de protección de datos y los derechos y libertades de los interesados sean efectivos.

3. El capítulo 2 de las Directrices pone el foco en la interpretación de los requisitos establecidos en el artículo 25 y explora las obligaciones jurídicas introducidas por esta disposición. En el capítulo 3 se ofrecen ejemplos de cómo aplicar la PDDD en el contexto de los principios específicos de protección de datos.

[1] Las interpretaciones expresadas en el presente documento son igualmente aplicables tanto al artículo 20 de la Directiva (UE) 2016/680 como al artículo 27 del Reglamento (CE) n.º 2018/1725.

[2] El considerando 78 del RGPD establece claramente esta necesidad: «Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos».

4. El capítulo 4 de las Directrices aborda la posibilidad de establecer un mecanismo de certificación para acreditar el cumplimiento del artículo 25, mientras el capítulo 5 explica de qué forma pueden aplicar el artículo las autoridades de control. Por último, las Directrices ofrecen a las partes interesadas recomendaciones adicionales sobre cómo aplicar la PDDD correctamente. El CEPD reconoce las dificultades que tienen las pequeñas y medianas empresas (en lo sucesivo, «pymes») para cumplir las obligaciones de PDDD en todos sus extremos, y ofrece recomendaciones adicionales específicas para las pymes en el capítulo 6.

2 ANÁLISIS DEL ARTÍCULO 25, APARTADOS 1 Y 2, PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

5. El objetivo de este capítulo es explorar y ofrecer orientaciones sobre los requisitos para la protección de datos desde el diseño establecidos en el artículo 25, apartado 1, y para la protección de datos por defecto establecidos en el artículo 25, apartado 2, respectivamente. La protección de datos desde el diseño y la protección de datos por defecto son conceptos complementarios, que se refuerzan mutuamente. Los interesados se beneficiarán más de la protección de datos por defecto si se aplica conjuntamente con la protección de datos desde el diseño, y viceversa.

6. La PDDD es un requisito para todos los responsables del tratamiento, ya sean pequeñas empresas o multinacionales. Partiendo de esta base, la complejidad de la aplicación de la PDDD puede variar en función de la operación de tratamiento concreta. No obstante, con independencia del tamaño, la aplicación de la PDDD tiene ventajas para el responsable del tratamiento y para el interesado en todos los casos.

2.1 Artículo 25, apartado 1: Protección de datos desde el diseño

2.1.1 Obligación del responsable del tratamiento de aplicar en el tratamiento las medidas técnicas y organizativas adecuadas y las garantías necesarias

7. Con arreglo al artículo 25, apartado 1, el responsable del tratamiento aplicará las *medidas* técnicas y organizativas *adecuadas* concebidas para aplicar los principios de protección de datos e integrar las *garantías necesarias* en el tratamiento, a fin de cumplir los requisitos y proteger los derechos y libertades de los interesados. Tanto las medidas adecuadas como las garantías necesarias tienen la finalidad de proteger los derechos de los interesados y garantizar que la protección de sus datos personales se integre en el tratamiento.

8. En un sentido amplio, cabe entender que las *medidas técnicas y organizativas* y las *garantías* son cualquier método o medio que el responsable pueda emplear en el tratamiento. Para que sean *adecuadas*, las medidas y las garantías necesarias deben ser adecuadas para conseguir el fin previsto, es decir, deben aplicar los principios de protección de datos *de forma efectiva*[3]. Por lo tanto, el requisito de que sean adecuadas está estrechamente ligado al requisito de la efectividad.

9. Una medida técnica u organizativa o una garantía puede ser cualquier cosa desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal. Ejemplos que pueden ser adecuados, en función del contexto y de los riesgos asociados al tratamiento en cuestión, son la seudonimización de los datos personales[4]; conservar los datos personales disponibles en un formato

[3] La «efectividad» se analiza en el apartado 2.1.2.
[4] Definida en el artículo 4, apartado 5, del RGPD.

estructurado, de uso común y lectura mecánica; permitir que los interesados intervengan en el tratamiento; facilitar información acerca de la conservación de datos personales; disponer de sistemas de detección de programas maliciosos; formar a los empleados en prácticas básicas de «ciberhigiene»; establecer sistemas de gestión de la privacidad y la seguridad de la información; obligar contractualmente a los encargados del tratamiento a adoptar prácticas específicas de minimización de datos, etcétera.

10. Las normas, las buenas prácticas y los códigos de conducta que sean reconocidos por asociaciones y otros organismos que representen a categorías de responsables pueden ser útiles para determinar las medidas adecuadas. Sin embargo, el responsable debe verificar que las medidas sean adecuadas para el tratamiento en cuestión.

2.1.2 Concebidas para aplicar de forma efectiva los principios de protección de datos y proteger los derechos y libertades de los interesados

11. Los *principios de protección de datos* están en el artículo 5 (en lo sucesivo, «los principios»), mientras que los *derechos y libertades de los interesados* son los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la protección de sus datos personales, cuya protección se menciona en el artículo 1, apartado 2, como el objeto del RPGD (en lo sucesivo, «los derechos»[5]. Su formulación precisa se encuentra en la Carta de los Derechos Fundamentales de la Unión Europea. Es esencial que el responsable del tratamiento conozca el significado de *los principios* y *los derechos* como base de la protección que confiere el RGPD, específicamente por la obligación de PDDD.

12. Al aplicar las medidas técnicas y organizativas adecuadas, es con respecto a la aplicación efectiva de cada uno de los principios mencionados y la consiguiente protección de derechos que deberán *concebirse* las medidas y garantías.

Cómo conseguir la efectividad

13. La efectividad es la base del concepto de protección de datos desde el diseño. El requisito de aplicar los principios de manera efectiva implica que los responsables del tratamiento deben aplicar las medidas y garantías necesarias para proteger dichos principios, a fin de garantizar los derechos de los interesados. Cada medida aplicada debe producir los resultados deseados para el tratamiento previsto por el responsable. Esta observación tiene dos consecuencias.

14. Primero, significa que el artículo 25 no requiere la aplicación de ninguna medida técnica u organizativa específica, salvo en el sentido de que las medidas y garantías elegidas deben ser específicas para la aplicación de los principios de protección de datos en el tratamiento en cuestión. Para ello, las medidas y garantías deben concebirse para que sean sólidas y el responsable debe poder aplicar medidas adicionales a fin de adaptarlas a cualquier incremento del riesgo[6] El hecho de que las medidas sean o no efectivas dependerá, por tanto, del contexto del tratamiento en cuestión y de la evaluación de

[5] Véase el considerando 4 del RGPD.

[6] «Los principios fundamentales aplicables a los responsables del tratamiento (es decir, la legitimidad, la minimización de datos, la limitación de la finalidad, la transparencia, la integridad de los datos y la exactitud de los datos) deben seguir siendo los mismos, cualquiera que sea el tratamiento y los riesgos para los interesados. No obstante, la naturaleza y el alcance de dicho tratamiento siempre han sido parte integrante de la aplicación de estos principios, de modo que son intrínsecamente modulables». Grupo de Trabajo del Artículo 29, *Statement on the role of a risk-based approach in data protection legal frameworks* (Declaración sobre el papel de un enfoque basado en el riesgo en los marcos jurídicos de protección de datos), WP 218, 30 de mayo de 2014, p. 3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

determinados elementos que deben tenerse en cuenta a la hora de determinar los medios del tratamiento. Los elementos antes mencionados se tratan a continuación en el apartado 2.1.3.

15. Segundo, los responsables del tratamiento deben ser capaces de acreditar que estos principios se han mantenido.

16. Las medidas y garantías aplicadas deben conseguir el efecto deseado en términos de protección de datos, y el responsable del tratamiento debe disponer de documentación sobre las medidas técnicas y organizativas aplicadas[7]. Para ello, el responsable del tratamiento podrá determinar indicadores clave de rendimiento (KPI, por sus siglas en inglés) adecuados para acreditar la efectividad. Un KPI es un valor medible elegido por el responsable del tratamiento que demuestra el grado de efectividad de dicho responsable en el cumplimiento de su objetivo de protección de datos. Los KPI pueden ser *cuantitativos*, como el porcentaje de falsos positivos o falsos negativos, la reducción de las reclamaciones o la reducción del tiempo de respuesta cuando los interesados ejercen sus derechos, o bien pueden ser *cualitativos*, como las evaluaciones del rendimiento, el uso de escalas de calificación o las evaluaciones de expertos. Como alternativa al uso de los KPI, los responsables pueden acreditar que los principios se aplican de forma efectiva explicando el razonamiento de su evaluación del grado de efectividad de las medidas y garantías seleccionadas.

2.1.3 Elementos que deben tenerse en cuenta

17. El artículo 25, apartado 1, enumera los elementos que el responsable del tratamiento debe tener en cuenta a la hora de determinar las medidas de una operación específica de tratamiento. A continuación presentamos orientaciones sobre cómo aplicar estos elementos en el proceso de diseño, que incluye el diseño de las opciones por defecto. Todos estos elementos contribuyen a determinar si una medida es adecuada para la aplicación efectiva de los principios. Es decir, ninguno de estos elementos es un objetivo por sí solo, sino que son factores que han de considerarse en conjunto para alcanzar el objetivo.

2.1.3.1 «estado de la técnica»

18. El concepto de «estado de la técnica» está presente en varios aspectos del acervo de la UE, como la protección del medio ambiente y la seguridad de los productos. En el RGPD, no solo se menciona el «estado de la técnica»[8] en el artículo 32, en relación con las medidas de seguridad[9][10], sino también en el artículo 25, ampliando así esta referencia a todas las medidas técnicas y organizativas integradas en el tratamiento.

19. En el contexto del artículo 25, la referencia al «estado de la técnica» impone a los responsables del tratamiento la obligación de **tener en cuenta el progreso actual de la tecnología** disponible en el mercado a la hora de determinar las medidas técnicas y organizativas adecuadas. Lo que se exige es

[7] Véanse los considerandos 74 y 78.
[8] Véase la decisión «Kalkar» del Tribunal Constitucional Federal alemán de 1978 (https://germanlawarchive.iuscomp.org/?p=67), que puede sentar las bases de una metodología para una definición objetiva del concepto. Sobre esta base, se determinaría el nivel tecnológico del «estado de la técnica» entre «la investigación y los conocimientos científicos existentes» y el concepto más consolidado de «reglas tecnológicas generalmente aceptadas». Así pues, cabe definir el «estado de la técnica» como el nivel tecnológico de un servicio o una tecnología o un producto que existe en el mercado y que es más eficaz para alcanzar los objetivos marcados.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/.

que los responsables del tratamiento conozcan y se mantengan al día de los avances tecnológicos, de cómo la tecnología puede presentar riesgos u oportunidades para la protección de datos, y de cómo aplicar las medidas y garantías que aseguran la aplicación efectiva de los principios y derechos de los interesados teniendo en cuenta la evolución del panorama tecnológico.

20. El «estado de la técnica» es un concepto dinámico que no puede definirse de manera estática en un momento determinado, sino que debe evaluarse *de manera continua* en el contexto del progreso tecnológico. Frente a los avances tecnológicos, un responsable del tratamiento podría considerar que una medida que proporcionaba un nivel adecuado de protección ya no lo hace. Por consiguiente, desatender la obligación de mantenerse al día de los cambios tecnológicos podría dar lugar al incumplimiento del artículo 25.

21. El criterio del «estado de la técnica» no solo se aplica a las medidas tecnológicas, sino también a las de carácter organizativo. La falta de medidas organizativas adecuadas puede reducir o incluso restar toda efectividad a la tecnología elegida. Ejemplos de medidas organizativas pueden ser la adopción de políticas internas, la formación de reciclaje tecnológico, la seguridad y protección de datos, y las políticas de gobernanza y gestión de la seguridad de TI.

22. Los marcos, normas, certificados, códigos de conducta, etcétera, existentes y reconocidos en distintos ámbitos, pueden servir para indicar el «estado de la técnica» actual en un ámbito de uso concreto. Cuando tales normas ya existan y confieran un elevado nivel de protección al interesado de modo que se cumplan —o se excedan— los requisitos legales, los responsables del tratamiento deberán tenerlas en cuenta en la concepción y aplicación de las medidas de protección de datos.

2.1.3.2 «coste de la aplicación»

23. El responsable del tratamiento puede tener en cuenta el coste de aplicación a la hora de elegir y aplicar medidas técnicas y organizativas adecuadas y las garantías necesarias que aseguren la aplicación efectiva de los principios a fin de proteger los derechos de los interesados. El coste hace referencia a los recursos en general, incluidos el tiempo y los recursos humanos.

24. El elemento de coste no obliga al responsable del tratamiento a destinar una cantidad desproporcionada de recursos cuando ya existan medidas alternativas, que exijan menos recursos pero que aun así sean efectivas. Sin embargo, el coste de aplicación es un factor que ha de considerarse para aplicar la protección de datos desde el diseño y no un motivo para no aplicarla.

25. Por tanto, las medidas elegidas garantizarán que la actividad de tratamiento de datos personales prevista por el responsable no incumpla los principios, con independencia del coste. Los responsables deben ser capaces de gestionar los costes totales para poder aplicar todos los principios de forma efectiva y, en consecuencia, proteger los derechos.

2.1.3.3 «naturaleza, ámbito, contexto y fines del tratamiento»

26. Los responsables deben tomar en consideración la naturaleza, ámbito, contexto y fines del tratamiento para determinar las medidas necesarias.

27. Estos factores deben interpretarse de forma coherente con el papel que desempeñan en otras disposiciones del RGPD, como los artículos 24, 32 y 35, con el fin de integrar los principios de protección de datos en el diseño del tratamiento.

28. En pocas palabras, cabe interpretar el concepto de **naturaleza** como las características intrínsecas[11] del tratamiento. El **ámbito** hace referencia al tamaño y a la variedad de actividades del tratamiento. El **contexto** se refiere a las circunstancias del tratamiento, que pueden influir en las expectativas del interesado, mientras que los **fines** son los objetivos del tratamiento.

2.1.3.4 «riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas»

29. El RGPD adopta un enfoque coherente basado en el riesgo en muchas de sus disposiciones, en los artículos 24, 25, 32 y 35, con el fin de determinar las medidas técnicas y organizativas adecuadas para proteger a las personas y sus datos personales y cumplir los requisitos del RGPD. Los bienes protegidos son siempre los mismos (las personas, a través de la protección de sus datos personales), frente a los mismos riesgos (para los derechos de las personas), y teniendo en cuenta las mismas circunstancias (la naturaleza, el ámbito, el contexto y los fines del tratamiento).

30. Al realizar el análisis de riesgos para el cumplimiento del artículo 25, el responsable del tratamiento ha de determinar los riesgos que entraña una violación de los principios para los derechos de los interesados, así como su probabilidad y gravedad a fin de aplicar medidas que mitiguen de forma efectiva los riesgos detectados. En las evaluaciones de riesgos es crucial realizar una evaluación sistemática y minuciosa del tratamiento. Por ejemplo, un responsable evalúa los riesgos concretos asociados a la ausencia de un consentimiento libremente otorgado, que constituye una violación del principio de licitud, en el curso del tratamiento de los datos personales de niños y jóvenes menores de 18 años como grupo vulnerable, en un caso en que no existe ningún otro fundamento jurídico, y aplica medidas adecuadas para abordar y mitigar de forma efectiva los riesgos detectados asociados a este grupo de interesados.

31. Las «Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD)»[12] del CEPD, que tratan de determinar si una operación de tratamiento de datos entraña probablemente un alto riesgo para el interesado o no, también proporcionan orientaciones sobre cómo evaluar los riesgos para la protección de datos y cómo llevar a cabo una evaluación del riesgo en materia de protección de datos. Las presentes Directrices también pueden ser útiles durante la evaluación del riesgo contemplada en todos los artículos antes mencionados, incluido el artículo 25.

32. El enfoque basado en el riesgo no excluye la utilización de valores de referencia, buenas prácticas y normas, que podrían ser herramientas útiles para que los responsables del tratamiento aborden riesgos similares en situaciones similares (naturaleza, ámbito, contexto y fines del tratamiento). No obstante, se mantiene la obligación establecida en el artículo 25 —así como en los artículos 24, 32 y 35, apartado 7, letra c) del RGPD— de tener en cuenta los «riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas». Por lo tanto, los responsables del tratamiento, aunque ayudándose de tales herramientas, deben realizar en cada caso una evaluación de los riesgos para la protección de datos que se deriven de la actividad de tratamiento

[11] Algunos ejemplos son las categorías especiales de datos personales, las decisiones automatizadas, el sesgo en la relación de fuerzas, una actividad de tratamiento impredecible, dificultades para que el interesado ejerza sus derechos, etcétera.

[12] Grupo de Trabajo del Artículo 29, «Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679», WP 248 rev.01, 4 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, refrendadas por el CEPD.

concreta, y verificar la efectividad de las medidas y garantías adecuadas que se hayan propuesto. Posteriormente puede que se requiera además una EIPD, o una actualización de una EIPD ya existente.

2.1.4 Aspecto temporal

2.1.4.1 En el momento de determinar los medios de tratamiento

33. La protección de datos desde el diseño debe llevarse a cabo «en el momento de determinar los medios de tratamiento».

34. Los «medios de tratamiento» van de lo general a los elementos concretos de diseño del tratamiento, como la arquitectura, los procedimientos, los protocolos, la disposición y la apariencia.

35. El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del *software* y *hardware* y los servicios de tratamiento de datos.

36. Tomar en consideración la PDDD desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas.

2.1.4.2 En el momento del propio tratamiento (mantenimiento y revisión de los requisitos de protección de datos)

37. Una vez iniciado el tratamiento, el responsable tiene la obligación permanente de mantener la PDDD, es decir, aplicar los principios de forma efectiva y continuada a fin de proteger los derechos, mantenerse al día del estado de la técnica, reevaluar el nivel de riesgo, etcétera. La naturaleza, el ámbito y el contexto de las operaciones de tratamiento, así como el riesgo, pueden cambiar durante el curso del tratamiento, lo que significa que el responsable deberá reevaluar sus operaciones de tratamiento revisando y valorando periódicamente la efectividad de las medidas y garantías que haya decidido adoptar.

38. La obligación de mantener, revisar y actualizar la operación de tratamiento, según sea necesario, también se aplica a los sistemas ya existentes. Esto significa que los sistemas heredados que se hayan diseñado antes de la entrada en vigor del RGPD deben someterse a revisión y mantenimiento para asegurar que se aplican medidas y garantías que apliquen los principios y derechos de los interesados de forma efectiva, como se explica en estas Directrices.

39. Esta obligación también se extiende a todo tratamiento realizado a través de encargados. Los responsables del tratamiento deben revisar y evaluar periódicamente las operaciones de los encargados del tratamiento para asegurarse de que hacen posible el cumplimiento continuo de los principios y permiten al responsable cumplir con sus obligaciones a este respecto.

2.2 Artículo 25, apartado 2: Protección de datos por defecto

2.2.1 Por defecto, solo son objeto de tratamiento los datos personales que son necesarios para cada uno de los fines específicos del tratamiento.

40. El término «por defecto», tal como se utiliza normalmente en informática, hace referencia al valor preexistente o preseleccionado de un parámetro configurable que se asigna a una aplicación informática, a un programa informático o a un dispositivo periférico. Estos parámetros se denominan «preajustes» o «ajustes de fábrica», especialmente en dispositivos electrónicos.

41. Por tanto, el término «por defecto» aplicado al tratamiento de datos personales se refiere a la toma de decisiones relativas a valores de configuración u opciones de tratamiento establecidos o prescritos en un sistema de tratamiento, como una aplicación informática, un servicio o un dispositivo periférico, o bien un procedimiento de tratamiento manual que afecte a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

42. El responsable debe elegir y responsabilizarse de aplicar parámetros y opciones de tratamiento por defecto de manera que, por defecto, solo se lleve a cabo el tratamiento que sea estrictamente necesario para cumplir el fin lícito establecido. En este caso, los responsables deberán basarse en su evaluación de la necesidad del tratamiento por lo que respecta a los fundamentos jurídicos del artículo 6, apartado 1. Esto significa que, por defecto, el responsable del tratamiento no debe recoger más datos de los que sean necesarios, ni realizar un tratamiento de los datos recogidos más amplio de lo necesario para sus fines, ni conservar los datos durante más tiempo del necesario. El requisito básico es que la protección de datos esté integrada en el tratamiento por defecto.

43. El responsable del tratamiento debe determinar previamente con qué fines especificados, explícitos y legítimos se recogen y se tratan los datos personales[13]. Las medidas deben ser adecuadas para garantizar, por defecto, que solo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Las Directrices del SEPD para evaluar la necesidad y la proporcionalidad de las medidas que limiten el derecho a la protección de datos personales también pueden ser útiles para decidir qué datos es necesario tratar para cumplir un fin determinado[14] [15] [16].

44. Si el responsable utiliza *software* de terceros o *software* comercial estándar, deberá realizar una evaluación de riesgos del producto y asegurarse de que las funciones que no tengan base jurídica o que no sean compatibles con los fines previstos del tratamiento estén desactivadas.

45. Las mismas consideraciones son aplicables a las medidas organizativas de apoyo a las operaciones de tratamiento. Deben estar concebidas para tratar, desde el principio, únicamente la cantidad de datos personales mínima necesaria para las operaciones específicas. Esto debe tenerse especialmente en

[13] Artículo 5, apartado 1, letras b), c), d) y e), del RGPD.
[14] SEPD, *Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection* (Directrices para evaluar la necesidad y la proporcionalidad de las medidas que limiten el derecho a la protección de datos), 25 de febrero de 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[15] Véase también SEPD, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* (Determinación de la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales: kit de herramientas), https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.
[16] Para más información sobre la necesidad, véase Grupo de Trabajo del Artículo 29, «Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE», WP 217, 9 de abril de 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf.

cuenta a la hora de asignar el acceso a los datos a personas con diferentes funciones y diferentes necesidades de acceso.

46. Las «medidas técnicas y organizativas» adecuadas en el contexto de la protección de datos por defecto se entienden pues de la manera ya explicada en el apartado 2.1.1, pero específicamente con respecto a la aplicación del principio de minimización de datos.

47. La citada obligación de tratar únicamente los datos personales que sean necesarios para cada fin específico se aplica a los siguientes elementos.

2.2.2 Dimensiones de la obligación de minimización de datos

48. El artículo 25, apartado 2, enumera las dimensiones de la obligación de minimización de datos para el tratamiento por defecto, cuando establece que la obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

2.2.2.1 «cantidad de datos personales recogidos»

49. Los responsables del tratamiento deben tener en cuenta tanto el volumen de datos personales como los tipos, categorías y nivel de detalle de los datos personales necesarios para los fines del tratamiento. Sus opciones de diseño deben tener en cuenta el aumento de los riesgos para los principios de integridad y confidencialidad, minimización de datos y limitación del plazo de conservación cuando se recogen grandes cantidades de datos personales detallados, y compararlos con la reducción de los riesgos cuando se recogen datos acerca de los interesados en menor cantidad o menos detallados. En cualquier caso, la configuración por defecto no debe incluir la recogida de datos personales que no sean necesarios para el fin concreto del tratamiento. En otras palabras, si algunas categorías de datos personales son innecesarias o si no hacen falta datos detallados porque es suficiente utilizar datos menos pormenorizados, no se recogerán datos personales excesivos.

50. Los mismos requisitos por defecto se aplican a los servicios con independencia de qué plataforma o dispositivo se utilice: solo se podrán recoger los datos personales necesarios para la finalidad concreta.

2.2.2.2 «la extensión de su tratamiento»

51. Las operaciones de tratamiento[17] aplicadas a datos personales se limitarán a lo estrictamente necesario. Muchas operaciones de tratamiento pueden contribuir a una finalidad de tratamiento. Sin embargo, el hecho de que determinados datos personales sean necesarios para una determinada finalidad no implica que se puedan aplicar todo tipo de operaciones de tratamiento a dichos datos ni con cualquier frecuencia. Asimismo, los responsables del tratamiento deben tener cuidado de no ampliar los límites de los «fines compatibles» del artículo 6, apartado 4, y tener presente qué tratamiento se corresponderá con las expectativas razonables de los interesados.

2.2.2.3 «su plazo de conservación»

52. Los datos personales recogidos no se conservarán si no es necesario para la finalidad del tratamiento y no hay otro fin compatible ni fundamento jurídico en virtud del artículo 6, apartado 4. La

[17] De conformidad con el artículo 4, apartado 2, del RGPD, esto incluye la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

conservación de los datos debe ser objetivamente justificable como necesaria por parte del responsable del tratamiento de los datos de conformidad con el principio de responsabilidad proactiva.

53. El responsable del tratamiento limitará el período de conservación a lo estrictamente necesario para el fin previsto. Si los datos personales dejan de ser necesarios para la finalidad del tratamiento, por defecto serán suprimidos o anonimizados. La duración del período de conservación dependerá, por tanto, de la finalidad del tratamiento en cuestión. Esta obligación está directamente relacionada con el principio de limitación del plazo de conservación establecido en el artículo 5, apartado 1, letra e), y se aplicará por defecto, es decir, el responsable del tratamiento debe contar con procedimientos sistemáticos para suprimir o anonimizar los datos que estén incorporados en el tratamiento.

54. La anonimización[18] de los datos personales es una alternativa a la supresión, siempre que se tengan en cuenta todos los elementos contextuales pertinentes y se evalúe periódicamente la probabilidad y la gravedad del riesgo, incluido el riesgo de reidentificación[19].

2.2.2.4 «su accesibilidad»

55. El responsable del tratamiento debe limitar quién tiene acceso y qué tipo de acceso a los datos personales en función de una evaluación de necesidades y asegurarse además de que los datos personales sean efectivamente accesibles para quienes los necesiten cuando los necesiten, por ejemplo en situaciones críticas. Deben observarse controles de acceso para todo el flujo de datos durante el tratamiento.

56. El artículo 25, apartado 2, establece además que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. Por defecto, el responsable del tratamiento debe limitar la accesibilidad y ofrecer al interesado la posibilidad de intervenir antes de publicar o poner de otro modo datos personales acerca del interesado a disposición de un número indeterminado de personas físicas.

57. Poner datos personales a disposición de un número indeterminado de personas puede hacer que los datos se difundan todavía más de lo inicialmente previsto. Esto es especialmente pertinente en el contexto de internet y los motores de búsqueda. Significa que, por defecto, los responsables deben ofrecer a los interesados la oportunidad de intervenir antes de que sus datos personales sean accesibles a través de la internet pública. Esto es especialmente importante en el caso de los niños y grupos vulnerables.

58. En función de los fundamentos jurídicos del tratamiento, la oportunidad de intervenir podría variar en el contexto del tratamiento. Por ejemplo, pedir consentimiento para que los datos personales sean accesibles públicamente, o establecer una configuración de privacidad que permita a los propios interesados controlar el acceso público.

[18] Grupo de Trabajo del Artículo 29, «Dictamen 05/2014 sobre técnicas de anonimización». WP 216, 10 de abril de 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf.

[19] Véase el artículo 4, apartado 1, del RGPD, el considerando 26 del RGPD y el Dictamen 05/2014 del Grupo de Trabajo del Artículo 29 sobre técnicas de anonimización. Véase también el apartado sobre «limitación del plazo de conservación» del capítulo 3 del presente documento, en el que se hace referencia a la necesidad de que el responsable del tratamiento garantice la eficacia de las técnicas de anonimización aplicadas.

59. Aun en el caso de que los datos personales se pongan a disposición del público con el permiso y entendimiento del interesado, ello no significa que cualquier otro responsable del tratamiento que tenga acceso a los datos personales pueda tratarlos libremente por su cuenta y para sus propios fines: estos siempre deben tener su propia base jurídica[20].

3 APLICACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS EN EL TRATAMIENTO DE DATOS PERSONALES UTILIZANDO LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

60. En todas las fases de diseño de las actividades de tratamiento, como contratación, licitación, externalización, desarrollo, asistencia, mantenimiento, ensayo, conservación, supresión, etcétera, el responsable del tratamiento debe tener en cuenta y considerar los distintos elementos de la PDDD que se ilustran con ejemplos en este capítulo en el contexto de la aplicación de los principios[21] [22] [23].

61. Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD. Para entender cómo aplicar la PDDD a la perfección, es esencial entender lo que significa cada uno de los principios.

62. Al presentar los ejemplos de cómo poner la PDDD en práctica hemos elaborado listas de **elementos esenciales de la PDDD** para cada uno de los principios. Los ejemplos, si bien ponen de relieve el principio específico de protección de datos en cuestión, también pueden solaparse con otros principios estrechamente relacionados. El CEPD quiere destacar que los elementos esenciales y los ejemplos aquí presentados no son ni exhaustivos ni vinculantes, sino que pretenden ser elementos orientativos de cada uno de los principios. Los responsables del tratamiento tendrán que valorar cómo garantizar el cumplimiento de los principios en el contexto de la operación de tratamiento concreta.

63. Aunque este capítulo trata de la aplicación de los principios, el responsable también deberá aplicar medidas *adecuadas* y *efectivas* para proteger los derechos de los interesados, también de acuerdo con el capítulo III del RGPD cuando esto no venga ya mandatado por los propios principios.

64. La responsabilidad proactiva es un principio general: obliga al responsable del tratamiento a actuar con responsabilidad en la elección de las medidas técnicas y organizativas necesarias.

3.1 Transparencia[24]

[20] Véase la sentencia Satakunnan Markkinapörssi Oy y Satamedia Oy contra Finlandia n.º 931/13.
[21] Pueden encontrarse más ejemplos en la web de la autoridad noruega de protección de datos, *Software Development with Data Protection by Design and by Default* (Desarrollo de *software* con protección de datos desde el diseño y por defecto), 28 de noviembre de 2017, www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers.
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.
[24] Se puede encontrar información sobre cómo entender el concepto de transparencia en el documento del Grupo de Trabajo del Artículo 29, «Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679», WP 260 rev.01, 11 de abril de 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, refrendadas por el CEPD.

65. El responsable del tratamiento debe hablar clara y abiertamente con el interesado acerca de cómo se recogerán, usarán y compartirán los datos personales. La transparencia consiste en facilitar que los interesados entiendan y, en su caso, ejerzan los derechos que tienen reconocidos en los artículos 15 a 22. Este principio está integrado en los artículos 12, 13, 14 y 34. Las medidas y garantías establecidas para favorecer el cumplimiento del principio de transparencia también deben favorecer la aplicación de estos artículos.

66. Elementos clave desde el diseño y por defecto para el principio de transparencia pueden ser los siguientes:

- Claridad: La información deberá estar redactada en un lenguaje claro y sencillo, ser concisa y comprensible.
- Semántica: La comunicación tendrá un significado claro para el público de que se trate.
- Accesibilidad: La información será fácilmente accesible para el interesado.
- Contexto: La información se facilitará en el momento pertinente y en la forma adecuada.
- Pertinencia: La información será pertinente y aplicable al interesado concreto.
- Diseño universal: La información será accesible para todos, incluido el uso de lenguajes de lectura mecánica para facilitar y automatizar la legibilidad y la claridad.
- Comprensible: Los interesados deberán tener una comprensión razonable de lo que pueden esperar en relación con el tratamiento de sus datos personales, especialmente cuando sean niños u otros grupos vulnerables.
- Multicanal: La información debe facilitarse por diferentes canales y medios, no solo el texto, para aumentar la probabilidad de que la información llegue efectivamente al interesado.
- Multinivel: La información debe presentarse por niveles de manera que se resuelva la tensión entre completitud y entendimiento, teniendo al mismo tiempo en cuenta las expectativas razonables de los interesados.

Ejemplo[25]

El responsable del tratamiento está preparando una política de privacidad en su sitio web para cumplir los requisitos de transparencia. Dicha política de privacidad no debe contener un gran volumen de información que sea difícil de entender para el interesado medio. Debe redactarse utilizando un lenguaje claro y conciso que permita al usuario de la web entender fácilmente cómo se procesarán sus datos personales. Por tanto, el responsable del tratamiento facilita la información en varios niveles, destacando los puntos más importantes. La información más detallada está fácilmente accesible. Se incluyen menús desplegables y enlaces a otras páginas para explicar con más detalle los distintos elementos y los conceptos utilizados en la política. El responsable del tratamiento también se asegura de que la información se facilite en un formato multicanal, con vídeos para explicar los puntos más importantes de la información escrita. La sinergia entre las distintas páginas es vital para garantizar que el enfoque multinivel no contribuya a aumentar la confusión, sino a reducirla.

Los interesados no deben tener dificultades para acceder a la política de privacidad. De este modo, la política de privacidad está disponible y visible en todas las páginas internas del sitio web en cuestión, y el interesado siempre puede acceder a la información con tan solo un clic. La información facilitada también se elabora de acuerdo con las mejores prácticas y normas de diseño universal con el fin de que sea accesible para todos.

[25] La autoridad francesa de protección de datos ha publicado varios ejemplos que ilustran las mejores prácticas de información a los usuarios, así como otros principios de transparencia: https://design.cnil.fr/en.

Por otra parte, también debe proporcionarse la información necesaria en el contexto adecuado y en el momento oportuno. Dado que el responsable realiza muchas operaciones de tratamiento utilizando los datos recogidos en el sitio web, la presencia de una política de privacidad por sí sola no es suficiente para que el responsable cumpla los requisitos de transparencia. Por tanto, este diseña un flujo de información para presentar al interesado información pertinente en los contextos adecuados, utilizando, por ejemplo, pequeños resúmenes informativos (*snippets*) o ventanas emergentes (*pop-ups*). Por ejemplo, al solicitar al interesado que introduzca datos personales, el responsable le informa de cómo se tratarán dichos datos personales y de por qué son necesarios para el tratamiento.

3.2 Licitud

67. El responsable del tratamiento debe establecer una base jurídica válida para el tratamiento de datos personales. Las medidas y garantías deben favorecer que se cumpla el requisito de que todo el ciclo del tratamiento esté en consonancia con los fundamentos jurídicos pertinentes del tratamiento.

68. Elementos esenciales desde el diseño y por defecto con respecto a la licitud pueden ser los siguientes:
- Pertinencia: Se aplicará el fundamento jurídico correcto al tratamiento.
- Diferenciación[26]: Se diferenciará el fundamento jurídico utilizado para cada actividad de tratamiento.
- Fin especificado: El fundamento jurídico apropiado debe estar claramente relacionado con el fin específico del tratamiento[27].
- Necesidad: El tratamiento debe ser necesario e incondicional para ser lícito.
- Autonomía: El interesado debe tener la máxima autonomía posible en lo que respecta al control de sus datos personales en el marco de la base jurídica.
- Obtención del consentimiento: El consentimiento debe ser una manifestación de voluntad libre, específica, informada e inequívoca[28]. Debe tenerse especialmente en cuenta la capacidad de niños y jóvenes para otorgar el consentimiento informado.
- Retirada del consentimiento: Cuando la base jurídica sea el consentimiento, el tratamiento deberá facilitar que se retire. Deberá ser tan fácil retirar el consentimiento como otorgarlo. De lo contrario, el mecanismo de consentimiento establecido por el responsable del tratamiento no cumplirá el RGPD[29].
- Equilibrio de intereses: Cuando la base jurídica sean los intereses legítimos, el responsable del tratamiento deberá equilibrar los intereses de forma ponderada, teniendo especialmente en cuenta el desequilibrio en la relación de fuerzas, en particular con menores de 18 años y otros grupos vulnerables. Se adoptarán medidas y garantías para mitigar los efectos negativos para los interesados.
- Determinación previa: El fundamento jurídico se establecerá antes del inicio del tratamiento.
- Cese: Si el fundamento jurídico deja de ser aplicable, el tratamiento cesará en consecuencia.

[26] CEPD, «Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados», versión 2.0, 8 de octubre de 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf.

[27] Véase más adelante el apartado relativo a la limitación de la finalidad.

[28] Véase *Guidelines 05/2020 on consent under Regulation 2016/679* (Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[29] Véase *Guidelines 05/2020 on consent under Regulation 2016/ 679, 679* (Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

- Ajuste: Si se produce un cambio válido de fundamento jurídico para el tratamiento, el tratamiento propiamente dicho deberá ajustarse al nuevo fundamento jurídico[30].
- Reparto de responsabilidades: Cuando exista corresponsabilidad del tratamiento, las partes deberán repartirse de manera clara y transparente las responsabilidades que les correspondan con respecto al interesado, y diseñar las medidas del tratamiento de acuerdo con dicho reparto.

Ejemplo

Un banco proyecta ofrecer un servicio para mejorar la eficiencia en la gestión de las solicitudes de préstamo. El concepto de servicio es que el banco, al solicitar permiso al cliente, pueda obtener datos acerca del cliente directamente de las autoridades tributarias públicas. En este ejemplo no se considera el tratamiento de datos personales de otras fuentes.

Es necesario obtener datos personales acerca de la situación financiera del interesado para realizar trámites previos a la formalización de un contrato de préstamo a petición del interesado[31]. Sin embargo, no se considera necesario recabar datos personales directamente de la administración tributaria porque el cliente puede formalizar el contrato aportando él mismo la información facilitada por la administración. Aunque el banco puede tener un interés legítimo en recabar la documentación directamente de las autoridades tributarias, por ejemplo para garantizar la eficiencia en la tramitación del préstamo, otorgar a los bancos acceso directo a los datos personales de los solicitantes entraña riesgos relacionados con el uso o posible uso indebido de derechos de acceso.

Al aplicar el principio de licitud, el responsable del tratamiento es consciente de que no puede utilizar el fundamento de «necesario para contratar» para la parte del tratamiento que consiste en recabar datos personales directamente de las autoridades tributarias. El hecho de que este tratamiento específico entrañe el riesgo de que el interesado se involucre menos en el tratamiento de sus datos es también un factor pertinente para evaluar la licitud del tratamiento propiamente dicho. El banco concluye que esta parte del tratamiento ha de basarse en otro fundamento jurídico. En el Estado miembro concreto donde está radicado el responsable del tratamiento, hay leyes nacionales que permiten que el banco recabe información directamente de las autoridades tributarias, siempre que el interesado lo autorice previamente.

Por tanto, el banco presenta información acerca del tratamiento en la plataforma de solicitud en línea de manera que los interesados puedan entender fácilmente qué tratamiento es obligatorio y cuál es optativo. Las opciones de tratamiento, por defecto, no permiten obtener datos directamente de otras fuentes que no sean el propio interesado, y la opción de recabar información directa se presenta de forma que no actúe como factor disuasorio para que el interesado no deniegue su consentimiento. El consentimiento otorgado para recoger datos directamente de otros responsables del tratamiento es un derecho temporal de acceso a un conjunto específico de información.

Cualquier consentimiento otorgado se tramita electrónicamente de una manera documentable, y los interesados disponen de una forma sencilla de controlar para qué han dado su consentimiento y de retirarlo.

[30] Si el fundamento jurídico original era el consentimiento, véase *Guidelines 05/2020 on consent under Regulation 2016/ 679, 679* (Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[31] Véase el artículo 6, apartado 1, letra b), del RGPD.

El responsable del tratamiento ha evaluado previamente estos requisitos de PDDD e incluye todos estos criterios en la especificación de sus requisitos para la licitación de contratación de la plataforma. El responsable del tratamiento es consciente de que, si no incluye los requisitos de PDDD en la licitación, puede que después sea demasiado tarde para aplicar la protección de datos o que el proceso sea muy costoso.

3.3 Lealtad

69. La lealtad es un principio general que exige que los datos personales no se traten de manera injustificadamente perjudicial, ilícitamente discriminatoria, inesperada o engañosa para el interesado. Las medidas y garantías que aplican el principio de lealtad también respaldan los derechos y libertades de los interesados, en concreto el derecho a la información (transparencia), el derecho de intervención (acceso, supresión, portabilidad y rectificación de los datos) y el derecho a limitar el tratamiento (derecho a no estar sujeto a decisiones individuales automatizadas y a la no discriminación de los interesados en dichos procesos).

70. Elementos esenciales desde el diseño y por defecto con respecto a la lealtad pueden ser los siguientes:
    - Autonomía: Los interesados deben tener el máximo grado de autonomía posible para determinar el uso que se haga de sus datos personales, así como el ámbito y las condiciones de dicho uso o tratamiento.
    - Interacción: Los interesados deben poder comunicar y ejercer sus derechos en relación con los datos personales tratados por el responsable.
    - Expectativas: El tratamiento debe corresponderse con las expectativas razonables de los interesados.
    - Sin discriminación: El responsable del tratamiento no discriminará a los interesados de forma desleal.
    - Sin abusos: El responsable del tratamiento no abusará de las necesidades o vulnerabilidades de los interesados.
    - Libre elección del consumidor: El responsable no debe «forzar» la elección de sus usuarios de manera desleal. Cuando un servicio que trate datos personales esté patentado, puede ocurrir que el interesado se vea «forzado» a usarlo, lo cual puede ser desleal si dificulta la posibilidad de que el interesado ejerza su derecho a la portabilidad de los datos con arreglo al artículo 20.
    - Equilibrio de fuerzas: El equilibrio de fuerzas debe ser un objetivo esencial de la relación entre el responsable del tratamiento y el interesado. Los desequilibrios en la relación de fuerzas deben evitarse. Cuando esto no sea posible, deberán reconocerse y corregirse adoptando las medidas adecuadas.
    - Sin transferencia de riesgos: Los responsables del tratamiento no deben transferir los riesgos de la empresa a los interesados.
    - Sin engaños: La información y las opciones del tratamiento de datos personales deben proporcionarse de manera objetiva y neutral, evitando todo tipo de lenguaje o diseño engañoso o manipulador.
    - Respeto a los derechos: El responsable del tratamiento debe respetar los derechos fundamentales de los interesados y aplicar medidas y garantías adecuadas, sin que tales derechos se vean afectados salvo en la medida en que la ley lo justifique expresamente.
    - Ética: El responsable debe apreciar los efectos generales que tenga el tratamiento sobre los derechos y la dignidad de las personas.

- Verdad: El responsable debe poner a disposición del interesado la información relativa a la forma en que se tratan los datos personales, debe actuar tal como haya declarado que lo va a hacer, y no inducir al interesado a engaño.
- Intervención humana: El responsable del tratamiento debe incorporar una intervención humana *cualificada*, capaz de detectar los sesgos que las máquinas puedan generar de conformidad con el derecho a no ser objeto de una decisión individual automatizada en virtud del artículo 22[32].
- Lealtad en el funcionamiento de los algoritmos: Se evaluará periódicamente si los algoritmos están funcionando en consonancia con los fines y se ajustarán para mitigar sesgos ocultos y garantizar la lealtad del tratamiento. Los interesados deben recibir información sobre el funcionamiento del tratamiento de los datos personales con algoritmos que analizan dichos datos o se basan en ellos para efectuar predicciones, como el rendimiento en el trabajo, la situación económica, la salud, las preferencias personales, la fiabilidad o el comportamiento, la ubicación o los movimientos[33].

Ejemplo 1

Un responsable del tratamiento gestiona un motor de búsqueda que en su mayor parte trata datos personales generados por los usuarios. El responsable se beneficia de tener a su disposición grandes cantidades de datos personales y poder utilizar dichos datos para realizar publicidad dirigida. Por lo tanto, el responsable desea influir en los interesados para poder obtener y utilizar datos personales más amplios. El consentimiento se va a obtener presentando opciones de tratamiento al interesado.

A la hora de aplicar el principio de lealtad, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, el responsable se da cuenta de que no puede presentar las opciones de manera que induzca al interesado a permitir que el responsable recoja más datos personales que si las opciones se presentaran de forma leal y neutral. Esto significa que no se pueden presentar las opciones de tratamiento de manera que a los interesados les resulte difícil negarse a compartir sus datos o que les resulte difícil ajustar su configuración de privacidad para limitar el tratamiento. Estos son ejemplos de patrones opacos, que son contrarios al espíritu del artículo 25. Las opciones por defecto para el tratamiento no deben ser invasivas, y la decisión de permitir un tratamiento ulterior debe presentarse de manera que no se presione al interesado para que otorgue su consentimiento. Por consiguiente, el responsable presenta las opciones de otorgar o denegar el consentimiento como dos opciones de igual visibilidad, que representan con exactitud las ramificaciones que tiene cada opción para el interesado.

Ejemplo 2

Otro responsable trata datos personales para la prestación de un servicio de *streaming* que permite a los usuarios elegir entre una suscripción normal de calidad estándar y una suscripción superior de mayor calidad. En el marco de la suscripción superior, los abonados reciben un servicio de atención al cliente prioritario.

[32] Véase «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
[33] Véase el considerando 71 del RGPD.

Con respecto al principio de lealtad, el servicio prioritario que reciben los abonados de nivel superior no puede discriminar el acceso del resto de abonados al ejercicio de sus derechos con arreglo al artículo 12 del RGPD. Esto significa que, si bien los abonados de nivel superior reciben un servicio prioritario, dicha prioridad no puede implicar que no se adopten medidas adecuadas para responder a las solicitudes del resto de abonados sin dilaciones indebidas y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud.

Puede que los clientes prioritarios paguen para recibir un mejor servicio, pero todos los interesados deben tener acceso por igual y sin discriminación para hacer valer sus derechos y libertades de conformidad con el artículo 12.

3.4 Limitación de la finalidad[34]

71. El responsable del tratamiento debe recoger los datos con fines determinados, explícitos y legítimos, y no tratarlos ulteriormente de manera incompatible con los fines para los que fueron recogidos[35]. El diseño del tratamiento debe, por tanto, configurarse en función de lo que sea necesario para alcanzar dichos fines. En caso de que vaya a realizarse un tratamiento ulterior, el responsable deberá asegurarse primero de que dicho tratamiento sea compatible con los fines originales y diseñarlo en consecuencia. La compatibilidad o incompatibilidad de un nuevo fin se evaluará con arreglo a los criterios establecidos en el artículo 6, apartado 4.

72. Elementos esenciales desde el diseño y por defecto con respecto a la limitación de la finalidad pueden ser los siguientes:
    - Determinación previa: Los fines legítimos deben determinarse antes de diseñar el tratamiento.
    - Especificidad: Los fines deben ser especificados y explícitos en cuanto a los motivos por los que se tratan los datos personales.
    - Orientación a los fines: La finalidad del tratamiento debe guiar el diseño del tratamiento y el establecimiento de límites al tratamiento.
    - Necesidad: La finalidad determina qué datos personales son necesarios para el tratamiento.
    - Compatibilidad: Cualquier nuevo fin debe ser compatible con el fin original para el que se recogieron los datos y orientar los cambios pertinentes en el diseño.
    - Limitar el tratamiento ulterior: El responsable del tratamiento no debe conectar conjuntos de datos ni realizar ningún tratamiento ulterior para fines nuevos que sean incompatibles.
    - Limitaciones de reutilización: El responsable del tratamiento debe utilizar medidas técnicas, como el cifrado y la función resumen o función *hash*, a fin de limitar la posibilidad de que se cambien los fines de los datos personales. El responsable también debe aplicar medidas organizativas, como políticas y obligaciones contractuales, que limiten la reutilización de datos personales.
    - Revisión: El responsable del tratamiento debe revisar periódicamente si el tratamiento es necesario para los fines para los que se recogieron los datos y comprobar el diseño en función de la limitación de la finalidad.

[34] El Grupo de Trabajo del Artículo 29 elaboró unas orientaciones sobre el principio de limitación de la finalidad con arreglo a la Directiva 95/46/CE. Aunque no fue adoptado por el CPED, este dictamen puede ser pertinente porque la formulación del principio es la misma que en el RGPD. Grupo de Trabajo del Artículo 29, *Opinion 03/2013 on purpose limitation* (Dictamen 03/2013 sobre la limitación de la finalidad), WP 203, 2 de abril de 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[35] Artículo 5, apartado 1, letra b), del RGPD.

Ejemplo

El responsable trata datos personales acerca de sus clientes. La finalidad del tratamiento es cumplir un contrato, es decir, poder entregar mercancías a la dirección correcta y obtener el pago. Los datos personales conservados son el historial de compra, el nombre, la dirección postal, la dirección de correo electrónico y el número de teléfono.

El responsable del tratamiento estudia la posibilidad de comprar un producto de gestión de las relaciones con los clientes (CRM) que reúna todos los datos de clientes acerca de ventas, marketing y atención al cliente en un solo lugar. El producto ofrece la oportunidad de conservar todas las llamadas telefónicas, actividades, documentos, correos electrónicos y campañas de marketing para obtener una perspectiva del cliente de 360 grados. Además, el CRM es capaz de analizar automáticamente el poder adquisitivo de los clientes mediante el uso de información pública. La finalidad del análisis es mejorar la determinación de quiénes deben ser los destinatarios de las actividades publicitarias. Estas actividades no forman parte del fin lícito original del tratamiento.

Para ajustarse al principio de limitación de la finalidad, el responsable obliga al proveedor del producto a asignar las diferentes actividades de tratamiento que utilizan datos personales a los fines pertinentes para el responsable.

Una vez recibidos los resultados de la asignación, el responsable valora si el nuevo fin de marketing y el fin de publicidad dirigida son compatibles con los fines originales que se definieron cuando se recogieron los datos, y si existe suficiente base jurídica para el tratamiento respectivo. Si la evaluación no arroja una respuesta positiva, el responsable no utilizará las funcionalidades en cuestión. Una alternativa es que el responsable decida abstenerse de realizar la evaluación y simplemente no utilice las funcionalidades del producto descritas.

3.5 Minimización de datos

73. Solo se tratarán datos personales que sean adecuados, pertinentes y limitados a lo que sea **necesario** para los fines previstos[36]. En consecuencia, el responsable del tratamiento debe determinar previamente qué características y parámetros de los sistemas de tratamiento y sus funciones complementarias son admisibles. La minimización de los datos justifica y pone en práctica el principio de necesidad. En el tratamiento ulterior, el responsable del tratamiento debe considerar periódicamente si los datos personales tratados siguen siendo adecuados, pertinentes y necesarios, o si los datos se suprimirán o se anonimizarán.

74. En primer lugar, los responsables del tratamiento deben determinar si tienen siquiera necesidad de tratar datos personales para sus fines pertinentes. El responsable debe verificar si se pueden alcanzar los fines pertinentes tratando menos datos personales, o utilizando datos personales menos detallados o agregados, o sin tener que tratar datos personales en modo alguno[37]. Dicha verificación debe tener lugar antes de cualquier tratamiento, pero también puede llevarse a cabo en cualquier momento durante el ciclo de tratamiento. Esto también es coherente con el artículo 11.

[36] Artículo 5, apartado 1, letra c), del RGPD.
[37] el considerando 39 del RGPD establece: «Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios».

75. La minimización también puede referirse al grado de identificación. Si la finalidad del tratamiento no requiere que el conjunto final de datos se refiera a una persona física identificada o identificable (como en las estadísticas), pero el tratamiento inicial sí (por ejemplo, antes de la agregación de datos), el responsable del tratamiento suprimirá o anonimizará los datos personales tan pronto como la identificación deje de ser necesaria. O bien, si se requiere una identificación continua para otras actividades de tratamiento, los datos personales deberán ser seudonimizados a fin de mitigar los riesgos para los derechos de los interesados.

76. Elementos esenciales desde el diseño y por defecto con respecto a la minimización de datos pueden ser los siguientes:
    - Evitación de datos: Se evitará todo tratamiento de datos personales cuando ello sea posible para cumplir la finalidad pertinente.
    - Limitación: Se limitará la cantidad de datos personales recogidos a lo estrictamente necesario para el fin previsto.
    - Limitación de acceso: Se configurará el tratamiento de datos de manera que se minimice el número de personas que necesiten acceder a datos personales para desempeñar sus funciones, y se limitará el acceso en consecuencia.
    - Pertinencia: Los datos personales deben ser pertinentes para el tratamiento en cuestión, y el responsable del tratamiento deberá poder acreditar dicha pertinencia.
    - Necesidad: Cada categoría de datos personales será necesaria para los fines especificados y solo deberá ser objeto de tratamiento si no es posible cumplir la finalidad por otros medios.
    - Agregación: Deberán utilizarse datos agregados cuando sea posible.
    - Seudonimización: Se deberán seudonimizar los datos personales en cuanto ya no sea necesario tener datos personales identificables directamente, y se conservarán las claves de identificación por separado.
    - Anonimización y supresión: Cuando los datos personales no sean o hayan dejado de ser necesarios para el fin previsto, serán anonimizados o suprimidos.
    - Flujo de datos: El flujo de datos deberá ser lo suficientemente eficiente como para no crear más copias de las necesarias.
    - «Estado de la técnica»: El responsable del tratamiento debe aplicar tecnologías actualizadas y adecuadas para evitar y minimizar el uso de datos.

Ejemplo 1

Una librería quiere aumentar sus ingresos vendiendo libros en línea. El propietario de la librería quiere establecer un formulario normalizado para el proceso de realización de pedidos. Para asegurarse de que los clientes cumplimenten toda la información deseada, el propietario de la librería hace que todos los campos del formulario sean obligatorios (si no se cumplimentan todos los campos, el cliente no puede realizar el pedido). El propietario de la tienda en línea utiliza inicialmente un formulario de contacto estándar, que solicita información como la fecha de nacimiento del cliente, su número de teléfono y su dirección postal. Sin embargo, no todos los campos del formulario son estrictamente necesarios para los fines de la compra y entrega de libros. En este caso concreto, si el interesado paga el producto por adelantado, ni la fecha de nacimiento ni el número de teléfono del interesado son datos necesarios para la compra del producto. Esto significa que estos campos del formulario web no pueden ser obligatorios para realizar el pedido, a menos que el responsable del tratamiento pueda acreditar claramente que son necesarios y por qué. Además, hay situaciones en las que no se necesita

la dirección postal. Por ejemplo, si lo que se pide es un libro electrónico, el cliente puede descargar el producto directamente en su dispositivo.

Por tanto, el propietario de la tienda en línea decide crear dos formularios web: uno para pedir libros que incorpora el campo para la dirección postal del cliente y otro para pedir libros electrónicos, que no incluye este campo.

Ejemplo 2

Una empresa de transporte público desea recoger información estadística basada en los itinerarios de los viajeros. Esto es útil para tomar decisiones adecuadas a la hora de realizar cambios en los horarios de transporte público y establecer itinerarios adecuados para los trenes. Los viajeros deben pasar el billete por un lector cada vez que entran o salen de un medio de transporte. Después de realizar una evaluación de riesgos al respecto de los derechos y libertades de los viajeros en relación con la recopilación de sus itinerarios, el responsable del tratamiento determina que el identificador del billete permite identificar a los viajeros que viven o trabajan en zonas poco pobladas sobre la base de un solo itinerario identificado. Por lo tanto, puesto que no es necesario para optimizar los horarios y los itinerarios de los trenes, el responsable del tratamiento no almacena el identificador del billete. Una vez finalizado el viaje, el responsable del tratamiento solo almacena los itinerarios individuales de manera que no pueda identificar los viajes relacionados con un único billete, sino que solo conserve información sobre itinerarios distintos.

En los casos en que aún pueda existir el riesgo de que se identifique a una persona únicamente por su itinerario en el transporte público, el responsable del tratamiento aplica medidas estadísticas para reducir dicho riesgo, como cortar el principio y el final del itinerario.

Ejemplo 3

Un servicio de mensajería pretende evaluar la eficacia de sus entregas en lo que respecta a los plazos de entrega, la programación de la carga de trabajo y el consumo de combustible. Para alcanzar este objetivo, el mensajero debe tratar una serie de datos personales de los empleados (conductores) y de los clientes (direcciones postales, artículos que deben entregarse, etcétera). Esta operación de tratamiento conlleva riesgos, tanto de control de los empleados, que requiere garantías jurídicas específicas, como de seguimiento de los hábitos de los clientes mediante el conocimiento de los artículos entregados a lo largo del tiempo. Estos riesgos pueden reducirse significativamente con una seudonimización adecuada de los empleados y los clientes. En particular, si las claves de seudonimización se rotan con frecuencia y se utilizan macrozonas en lugar de direcciones postales detalladas, se consigue minimizar los datos de manera efectiva, y el responsable del tratamiento puede centrarse únicamente en el proceso de entrega y en la finalidad de optimización de los recursos, sin cruzar el umbral de controlar el comportamiento de las personas (clientes o empleados).

Ejemplo 4

Un hospital recoge datos de sus pacientes en un sistema de información hospitalaria (historia clínica electrónica). El personal del hospital necesita acceder a las historias de los pacientes para tomar

decisiones informadas de tratamiento médico, y para documentar todas las actuaciones de diagnóstico y tratamiento. Por defecto, solo se da acceso a los miembros del personal médico asignados al tratamiento del paciente respectivo en el departamento de la especialidad a la que corresponde. El número de personas que tienen acceso a la historia del paciente aumenta si hay otros departamentos o unidades de diagnóstico que participan en su tratamiento. Una vez que el paciente es dado de alta y se completa la facturación, se reduce el acceso a un pequeño grupo de empleados por departamento de especialidad que responde a las solicitudes de información médica o consultas planteadas por otros proveedores de servicios médicos con autorización del paciente respectivo.

3.6 Exactitud

77. Los datos personales deberán ser exactos y mantenerse actualizados, y se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan[38].

78. Los requisitos deben considerarse en relación con los riesgos y las consecuencias del uso concreto de los datos. Los datos personales inexactos podrían suponer un riesgo para los derechos y libertades de los interesados, por ejemplo, cuando den lugar a un diagnóstico erróneo o a un tratamiento injustificado de un protocolo de salud, o puede que una imagen incorrecta de una persona ocasione que se tomen decisiones por motivos incorrectos, bien sea manualmente, bien mediante un proceso de toma de decisiones automatizado o bien mediante inteligencia artificial.

79. Elementos esenciales desde el diseño y por defecto con respecto a la exactitud pueden ser los siguientes:
    - Fuente de los datos: Las fuentes de datos personales deben ser fiables en cuanto a la exactitud de los datos.
    - Grado de exactitud: Cada elemento de datos personales deberá ser tan exacto como sea necesario para los fines especificados.
    - Exactitud medible: Se reducirá el número de falsos positivos o negativos, por ejemplo, sesgos en las decisiones automatizadas y la inteligencia artificial.
    - Verificación: En función de la naturaleza de los datos, en relación con la frecuencia con la que puedan cambiar, el responsable deberá contactar con el interesado para verificar si los datos personales son correctos antes del tratamiento y en sus diferentes fases (por ejemplo, cuando existan requisitos de edad).
    - Supresión y rectificación: El responsable del tratamiento debe suprimir o rectificar los datos inexactos sin dilación. El responsable deberá facilitar esto, en particular, cuando los interesados sean o hayan sido menores y posteriormente quieran eliminar dichos datos personales[39].
    - Evitación de la propagación de errores: Los responsables deben mitigar el efecto de un error acumulado en la cadena de tratamiento.
    - Acceso: Se debe facilitar a los interesados información acerca de sus datos personales y acceso efectivo a los mismos, de conformidad con los artículos 12 a 15 del RGPD, a fin de controlar su exactitud y rectificarlos si es necesario.
    - Exactitud continuada: Los datos personales deben ser exactos en todas las fases del tratamiento, debiendo llevarse a cabo pruebas de exactitud en puntos críticos.
    - Actualizados: Los datos personales se actualizarán si es necesario para el fin previsto.

[38] Artículo 5, apartado 1, letra d), del RGPD.
[39] Véase el considerando 65.

- Diseño de los datos: Se utilizarán elementos de diseño tecnológico y organizativo para reducir la inexactitud, como la presentación de opciones predeterminadas concisas en lugar de campos de texto libre.

Ejemplo 1

Una compañía de seguros desea utilizar inteligencia artificial (IA) para elaborar perfiles de los clientes que compran sus seguros como base para tomar sus decisiones al calcular el riesgo del seguro. Cuando determina cómo deben desarrollarse sus soluciones de IA, está determinando los medios de tratamiento y debe tener en cuenta la protección de datos desde el diseño para elegir una aplicación IA de un proveedor y para decidir la manera de entrenar a la IA.

Cuando determina cómo entrenar a la IA, el responsable del tratamiento debe disponer de datos exactos para obtener resultados precisos. Por tanto, el responsable del tratamiento debe garantizar que los datos utilizados para el entrenamiento de la IA son exactos.

Con la premisa de que tiene un fundamento jurídico válido para entrenar a la IA utilizando datos personales de un gran número de sus clientes ya existentes, el responsable del tratamiento elige un grupo de clientes representativo de la población para evitar también el sesgo.

A continuación obtiene los datos de los clientes del sistema respectivo de tratamiento de la información, que incluye datos sobre el tipo de seguro —por ejemplo seguro de salud, seguro de hogar, seguro de viaje, etcétera—, así como datos de los registros públicos a los que tenga acceso lícito. Todos los datos son seudonimizados antes de transferirse al sistema de entrenamiento del modelo IA.

Para asegurarse de que los datos utilizados para entrenar a la AI sean lo más exactos posible, el responsable del tratamiento solo recoge datos de fuentes de información correcta y actualizada.

La compañía de seguros realiza pruebas para determinar si la IA es fiable y proporciona resultados no discriminatorios durante su desarrollo y antes de comercializar el producto. Cuando la IA está totalmente entrenada y operativa, la compañía utiliza los resultados como apoyo de las evaluaciones de riesgos de los seguros, pero sin basarse exclusivamente en la IA para decidir si concede el seguro, a menos que la decisión se tome con arreglo a las excepciones recogidas en el artículo 22, apartado 2, del RGPD.

La compañía de seguros también revisará periódicamente los resultados de la IA, para mantener su fiabilidad y, en su caso, ajustar el algoritmo.

Ejemplo 2

El responsable del tratamiento es una institución sanitaria que busca métodos para garantizar la integridad y la exactitud de los datos personales en sus registros de clientes.

En los casos en que dos personas llegan a la institución al mismo tiempo y reciben el mismo tratamiento médico, existe el riesgo de confundirlas si el único parámetro para distinguirlas es su nombre. Para garantizar la exactitud, el responsable del tratamiento necesita un identificador único para cada persona y, por tanto, más información que el mero nombre del cliente.

La institución utiliza varios sistemas que contienen información personal de los clientes y tiene que garantizar que la información relativa al cliente sea correcta, exacta y coherente en todos los sistemas

en todo momento. La institución ha identificado varios riesgos que pueden surgir si se modifica la información en un sistema, pero no en otro.

El responsable del tratamiento decide mitigar el riesgo por medio de una función *hash* que puede utilizarse para garantizar la integridad de los datos en el diario de tratamiento médico. Se crean sellos de tiempo criptográficos inalterables para los registros de tratamiento médico y el cliente asociado a ellos, de manera que se pueda reconocer, correlacionar y rastrear cualquier cambio si es necesario.

3.7 Limitación del plazo de conservación

80. El responsable del tratamiento debe velar por que los datos personales se conserven en un formato que permita la identificación de los interesados durante un período de tiempo no superior al necesario para el cumplimiento de los fines para los que se tratan[40].
Es fundamental que el responsable del tratamiento sepa exactamente qué datos personales se tratan en la compañía y por qué. La finalidad del tratamiento será el criterio principal para decidir durante cuánto tiempo se conservarán los datos personales.

81. Las medidas y garantías que apliquen el principio de limitación del plazo de conservación complementarán los derechos y libertades de los interesados, en particular el derecho de supresión y el derecho de oposición.

82. Elementos esenciales desde el diseño y por defecto con respecto a la limitación del plazo de conservación pueden ser los siguientes:
    - Supresión y anonimización: El responsable del tratamiento debe tener procedimientos y funcionalidades claros de supresión y anonimización.
    - Eficacia de la anonimización o supresión: El responsable del tratamiento se asegurará de que no sea posible volver a identificar los datos anonimizados o recuperar datos suprimidos, y deberá comprobar si esto es posible.
    - Automatización: La supresión de determinados datos personales debe ser automatizada.
    - Criterios de conservación: El responsable del tratamiento debe determinar qué datos y qué plazos de conservación son necesarios para los fines previstos.
    - Justificación: El responsable del tratamiento deberá poder justificar por qué el plazo de conservación es necesario para los fines y los datos personales en cuestión, así como explicar el razonamiento y los fundamentos jurídicos del plazo de conservación.
    - Ejecución de las políticas de conservación: El responsable del tratamiento debe aplicar políticas internas de conservación y realizar pruebas para determinar si la organización pone en práctica sus políticas.
    - Copias de seguridad y registros: Los responsables del tratamiento deben determinar qué datos personales y plazos de conservación son necesarios para las copias de seguridad y los registros.
    - Flujo de datos: Los responsables del tratamiento deben ser cuidadosos con el flujo de datos personales y la conservación de sus copias, y procurar limitar su conservación «temporal».

Ejemplo

[40] Artículo 5, apartado 1, letra c), del RGPD.

El responsable del tratamiento recoge datos personales cuyo tratamiento tiene la finalidad de administrar una afiliación del interesado. Los datos personales se suprimirán cuando finalice la afiliación y no exista base jurídica para la conservación ulterior de los datos.

El responsable del tratamiento establece primero un procedimiento interno de conservación y supresión de datos. De acuerdo con esto, los empleados deben suprimir los datos personales manualmente cuando finaliza el período de conservación. El empleado sigue el procedimiento para suprimir y corregir periódicamente los datos de cualquier dispositivo, de copias de seguridad, registros, correos electrónicos y otros medios de conservación pertinentes.

Para que la supresión sea más eficaz, y menos propensa a errores, el responsable del tratamiento aplica entonces un sistema automático para suprimir los datos automáticamente, de forma fiable y con mayor regularidad. El sistema se configura para seguir el procedimiento establecido para la supresión de datos, que se realiza en función de un intervalo de tiempo predefinido para eliminar los datos personales de todos los medios de conservación de la empresa. El responsable del tratamiento revisa y ensaya el procedimiento de conservación periódicamente y se asegura de que se ajuste a la política de conservación actualizada.

3.8 Integridad y confidencialidad

83. El principio de integridad y confidencialidad incluye protección contra el tratamiento no autorizado o ilícito y contra pérdidas, destrucción o daños accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas. La seguridad de los datos personales requiere medidas adecuadas concebidas para prevenir y gestionar incidentes de vulneración de datos, para garantizar la debida ejecución de las tareas de tratamiento de datos y el cumplimiento de otros principios, y para facilitar el ejercicio efectivo de los derechos de las personas.

84. En el considerando 78 se afirma que una de las medidas de PDDD podría consistir en permitir al responsable del tratamiento «crear y mejorar elementos de seguridad». Junto con otras medidas de PDDD, el considerando 78 apunta que los responsables del tratamiento tienen la responsabilidad de evaluar de forma continua si están utilizando medios apropiados de tratamiento en todo momento y si las medidas elegidas neutralizan verdaderamente las vulnerabilidades existentes. Además, los responsables del tratamiento deben llevar a cabo revisiones periódicas de las medidas de seguridad de la información que rodean y protegen los datos personales, así como el procedimiento para gestionar vulneraciones.

85. Elementos esenciales desde el diseño y por defecto con respecto a la integridad y la confidencialidad pueden ser los siguientes:
    - Sistema de gestión de la seguridad de la información (SGSI): Un medio operativo para gestionar las políticas y los procedimientos de seguridad de la información.
    - Análisis de riesgos: Se evaluarán los riesgos contra la seguridad de los datos personales teniendo en cuenta cómo afectan a los derechos de las personas y se neutralizarán los riesgos identificados. Para su uso en la evaluación de riesgos, se desarrollará y mantendrá un «modelo de amenazas» exhaustivo, sistemático y realista y un análisis de la superficie de ataque del *software* diseñado para reducir los vectores de ataque y las oportunidades de aprovechar puntos débiles y vulnerabilidades.
    - Seguridad desde el diseño: Se considerarán los requisitos de seguridad lo antes que sea posible en el diseño y desarrollo del sistema y se integrarán y realizarán los ensayos pertinentes de forma continuada.

- Mantenimiento: Se realizarán revisiones y ensayos periódicos del *software*, *hardware*, sistemas y servicios, etcétera, para detectar vulnerabilidades de los sistemas de apoyo al tratamiento.
- Gestión del control de acceso: Solo el personal autorizado que lo necesite deberá tener acceso a los datos personales necesarios para sus tareas de tratamiento, y el responsable deberá diferenciar los privilegios de acceso del personal autorizado.
    - Limitación de acceso (agentes): Se configurará el tratamiento de datos de manera que se minimice el número de personas que necesiten acceder a datos personales para desempeñar sus funciones, y se limitará el acceso en consecuencia.
    - Limitación de acceso (contenido): En el contexto de cada operación de tratamiento, se limitará el acceso exclusivamente a aquellos atributos de cada conjunto de datos que sean necesarios para realizar esa operación. Además, se limitará el acceso a los datos que pertenezcan a aquellos interesados que estén incluidos en el ámbito de competencia del empleado respectivo.
    - Segregación de acceso: Se configurará el tratamiento de datos de manera que ninguna persona necesite acceder a todos los datos de un interesado, y mucho menos a todos los datos personales de una determinada categoría de interesados.
- Transferencias seguras: Las transferencias se protegerán contra accesos y cambios no autorizados y accidentales.
- Conservación segura: La conservación de los datos se protegerá contra accesos y cambios no autorizados. Deberá haber procedimientos para evaluar el riesgo de la conservación centralizada o descentralizada, y a qué categorías de datos personales se aplica. Puede que algunos datos necesiten más medidas de seguridad que otros o estar aislados de otros.
- Seudonimización: Los datos personales y las copias de seguridad o los registros deben seudonimizarse como medida de seguridad para minimizar los riesgos de vulneración de los datos, por ejemplo mediante cifrado o función *hash*.
- Copias de seguridad y registros: Se mantendrán copias de seguridad y registros en la medida en que sea necesario para la seguridad de la información, utilizándose registros de auditoría y monitorización de eventos como control de seguridad rutinario. Estos se protegerán contra accesos y cambios no autorizados y accidentales y se revisarán periódicamente, y cualquier incidente deberá resolverse de forma inmediata.
- Recuperación de desastres/continuidad de la actividad: Se abordarán los requisitos del sistema de información en materia de recuperación de desastres y continuidad de la actividad para restaurar la disponibilidad de los datos personales cuando ocurran incidentes graves.
- Protección en función del riesgo: Todas las categorías de datos personales deberán protegerse con medidas adecuadas con respecto al riesgo de una vulneración de la seguridad. Los datos que presenten riesgos especiales deberán mantenerse separados del resto de datos personales en la medida de lo posible.
- Gestión de la respuesta a incidentes de seguridad: Se establecerán rutinas, procedimientos y recursos para detectar, contener, gestionar, notificar y aprender de las vulneraciones de los datos.
- Gestión de incidentes: El responsable del tratamiento deberá establecer procesos de gestión de vulneraciones e incidentes, a fin de aumentar la solidez del sistema de tratamiento. Esto incluye procedimientos de notificación, como la gestión de notificaciones (a la autoridad de control) y de la información (a los interesados).

Ejemplo

El responsable del tratamiento desea extraer grandes cantidades de datos personales de una base de datos médicos que contiene las historias clínicas electrónicas (de los pacientes) para incorporarlos a un servidor de base de datos específico de la empresa a fin de tratar dichos datos con fines de aseguramiento de la calidad. La empresa ha valorado que la transferencia de los datos extraídos a un servidor que es accesible para todos los empleados de la empresa probablemente entraña un riesgo elevado para los derechos y libertades de los interesados. Dado que solo hay un departamento en la empresa que necesita tratar los datos extraídos, el responsable decide que el acceso al servidor específico se limite a los empleados de dicho departamento. Por otra parte, a fin de reducir todavía más el riesgo, los datos serán seudonimizados antes de transferirse.

Para regular el acceso y mitigar posibles daños causados por programas maliciosos, la empresa decide segregar la red y establecer controles de acceso al servidor. Además, pone en marcha un sistema de control de la seguridad y un sistema de detección y prevención de intrusiones, y lo aísla del uso rutinario. Se establece un sistema de auditoría automatizado de control de accesos y cambios. Desde ahí se generan notificaciones y alertas automatizadas cuando se configuran determinados eventos en función del uso. El responsable del tratamiento garantizará que los usuarios solo tengan acceso en función de lo que necesiten y con el nivel adecuado de acceso. Los usos indebidos se podrán detectar rápida y fácilmente.

Algunos datos extraídos deberán compararse con datos que se extraigan posteriormente, por lo que deberán conservarse durante tres meses. El responsable decide ponerlos en bases de datos separadas en el mismo servidor, y utilizar el cifrado transparente y a nivel de columna para almacenarlos. Las claves para descifrar los datos de las columnas se conservan en módulos de seguridad específicos de modo que solo puedan utilizarse por personal autorizado, pero sin que se puedan extraer.

La gestión de posibles incidentes hace que el sistema sea más sólido y fiable. El responsable del tratamiento entiende que es preciso integrar medidas y garantías preventivas y efectivas en todas las operaciones de tratamiento de datos personales que lleve a cabo ahora y en el futuro, y que ello puede contribuir a evitar futuros incidentes de vulneración de datos.

El responsable del tratamiento establece estas medidas de seguridad para garantizar la exactitud, la integridad y la confidencialidad, pero también para evitar la propagación de programas maliciosos por medio de ciberataques y para dotar de solidez a la solución. Establecer medidas de seguridad sólidas contribuye a generar confianza en los interesados.

3.9 Responsabilidad proactiva[41]

86. El principio de responsabilidad proactiva establece que el responsable del tratamiento debe responsabilizarse del cumplimiento de todos los principios antes mencionados y ser capaz de acreditarlo.

87. El responsable del tratamiento debe ser capaz de acreditar el cumplimiento de los principios. Para ello, el responsable puede acreditar los efectos de las medidas adoptadas para proteger los derechos de los interesados, y por qué se considera que las medidas son adecuadas y efectivas. Por ejemplo, acreditando por qué una medida es adecuada para garantizar el principio de limitación del plazo de conservación de manera efectiva.

88. El responsable del tratamiento, para poder tratar datos personales de manera responsable, debe tener conocimientos y capacidades para implementar la protección de los datos. Esto implica que el

[41] Véase el considerando 74, en el que se exige que los responsables del tratamiento demuestren la eficacia de sus medidas.

responsable debe comprender sus obligaciones de protección de datos en virtud del RGPD y ser capaz de cumplir con dichas obligaciones.

4 CERTIFICACIÓN, ARTÍCULO 25, APARTADO 3

89. En virtud del artículo 25, apartado 3, la certificación conforme al artículo 42 puede utilizarse como elemento que acredite el cumplimiento de la PDDD. A la inversa, los documentos que acrediten el cumplimiento de la PDDD también pueden ser útiles en un proceso de certificación. Esto significa que cuando una operación de tratamiento de un responsable o encargado haya sido certificada en virtud del artículo 42, las autoridades de control la tendrán en cuenta en su evaluación del cumplimiento del RGPD, específicamente en relación con la PDDD.

90. Cuando una operación de tratamiento de un responsable o encargado se certifica en virtud del artículo 42, los elementos que contribuyen a acreditar el cumplimiento del artículo 25, apartados 1 y 2 son los procesos de diseño, es decir, el proceso de determinación de los medios de tratamiento, la gobernanza y las medidas técnicas y organizativas para aplicar los principios de protección de datos. Los criterios de certificación de la protección de datos son determinados por los organismos de certificación o por los propietarios del sistema de certificación y aprobados después por la autoridad de control competente o por el CEPD. Para más información acerca de los mecanismos de certificación, véanse las Directrices del CEPD sobre certificación[42] y otras orientaciones pertinentes publicadas en el sitio web del CEPD.

91. Aun cuando se certifique una operación de tratamiento conforme al artículo 42, el responsable del tratamiento seguirá teniendo la responsabilidad de controlar y mejorar continuamente el cumplimiento de los criterios de PDDD del artículo 25.

5 APLICACIÓN DEL ARTÍCULO 25 Y CONSECUENCIAS

92. Las autoridades de control podrán evaluar el cumplimiento del artículo 25 de acuerdo con los procedimientos enumerados en el artículo 58. Los poderes correctivos se especifican en el artículo 58, apartado 2, e incluyen advertencias, apercibimientos, órdenes de atender los derechos de los interesados, limitaciones o prohibiciones del tratamiento, multas administrativas, etcétera.

93. Además, la PDDD se tiene en cuenta para determinar la cuantía de las sanciones pecuniarias por infracciones del RGPD; véase el artículo 83, apartado 4[43] [44].

[42] CEPD, «Directrices 1/2018 sobre la certificación y la determinación de los criterios de identificación de conformidad con los artículos 42 y 43 del Reglamento», versión 3.0, 4 de junio de 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf.

[43] El artículo 83, apartado 2, letra d), del RGPD establece que, para determinar la imposición de multas por infracciones del RGPD, «se tendrá debidamente en cuenta [...] el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32».

[44] Para más información sobre multas, véase el documento del Grupo de Trabajo del Artículo 29, «Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679», WP 253, 3 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237, refrendadas por el CEPD.

6 RECOMENDACIONES

94. Aunque el artículo 25 no se dirige a ellos directamente, los encargados del tratamiento y los productores también están reconocidos como esenciales para la aplicación de la PDDD, y deben saber que los responsables del tratamiento tienen la obligación de tratar los datos personales únicamente con sistemas y tecnologías que incorporen la protección de datos.

95. Cuando realicen el tratamiento en nombre de los responsables, o proporcionen soluciones a los responsables, los encargados del tratamiento y los productores deberán utilizar sus conocimientos técnicos para generar confianza y orientar a sus clientes, incluidas las pymes, en el diseño/adquisición de soluciones que integren la protección de datos en el tratamiento. Esto significa a su vez que el diseño de los productos y servicios debe facilitar las necesidades de los responsables del tratamiento.

96. En la aplicación del artículo 25, hay que tener en cuenta que el objetivo principal del diseño es que la *aplicación efectiva* de los principios y la *protección* de los derechos de los interesados se integren en las medidas adecuadas del tratamiento. A fin de facilitar y mejorar la adopción de la PDDD, recomendamos lo siguiente a los responsables del tratamiento, así como a los encargados del tratamiento y a los productores:
    - Los responsables del tratamiento deben pensar en la protección de datos desde las *fases iniciales* de la planificación de una operación de tratamiento, incluso antes de la determinación de los medios de tratamiento.
    - Cuando el responsable del tratamiento tenga un delegado de protección de datos (DPD), el CEPD promueve la participación activa del DPD en la integración de la PDDD en los procedimientos de contratación y desarrollo, así como en todo el ciclo de tratamiento.
    - La operación de tratamiento podrá ser *certificada*. La capacidad de conseguir que se certifique una operación de tratamiento proporciona un valor añadido al responsable a la hora de elegir entre diferente *software* y *hardware*, servicios o sistemas de tratamiento de los productores o encargados. Por tanto, los productores deben esforzarse por acreditar la PDDD durante todo el ciclo de desarrollo de una solución de tratamiento. Un sello de certificación también puede orientar a los interesados a la hora de elegir entre distintos bienes y servicios. La capacidad de conseguir que se certifique un tratamiento puede ser una ventaja competitiva para los productores, encargados y responsables, e incluso aumenta la confianza de los interesados en el tratamiento de sus datos personales. Si no se ofrece certificación, los responsables del tratamiento deben procurar obtener otras *garantías* de que los productores o encargados del tratamiento cumplen los requisitos de PDDD.
    - Los responsables, encargados y productores deben tener en cuenta sus obligaciones de proporcionar a los menores de 18 años y otros grupos vulnerables protección específica en cumplimiento de la PDDD.
    - Los productores y los encargados del tratamiento deben facilitar la aplicación de la PDDD a fin de ayudar al responsable del tratamiento a cumplir con las obligaciones del artículo 25. Por otra parte, los responsables no deben elegir a productores o encargados que no ofrezcan sistemas que permitan o faciliten que el responsable del tratamiento cumpla con lo dispuesto en el artículo 25, ya que los responsables del tratamiento deberán rendir cuentas de su inaplicación.
    - Los productores y los encargados deben desempeñar un papel activo para garantizar que se cumplen los criterios del «estado de la técnica», y notificar a los responsables cualquier cambio en el «estado de la técnica» que pueda afectar a la efectividad de las medidas que hayan

establecido. Los responsables del tratamiento deben incluir este requisito como cláusula contractual para asegurarse de que se mantienen al día.

- El CEPD recomienda a los responsables que exijan a productores y encargados que acrediten cómo su *hardware* o *software* o sus servicios o sistemas permiten que el responsable cumpla con los requisitos de responsabilidad proactiva de conformidad con la PDDD, por ejemplo utilizando indicadores clave de rendimiento para acreditar la efectividad de las medidas y garantías en la aplicación de los principios y derechos.
- El CEPD destaca la necesidad de un enfoque armonizado para aplicar los principios y derechos de manera efectiva e insta a las asociaciones y organismos a preparar códigos de conducta de conformidad con el artículo 40 que incorporen también orientaciones sectoriales sobre la PDDD.
- Los responsables del tratamiento deben ser leales con los interesados y transparentes en su forma de evaluar y acreditar la aplicación efectiva de la PDDD, del mismo modo que los responsables del tratamiento acreditan el cumplimiento del RGPD en virtud del principio de responsabilidad proactiva.
- Las tecnologías de protección de la intimidad (PET, por sus siglas en inglés) que hayan alcanzado la madurez del estado de la técnica podrán emplearse como medida de conformidad con los requisitos de PDDD si es apropiado en el marco de un enfoque basado en riesgos. Las PET por sí solas no satisfacen necesariamente las obligaciones del artículo 25. Los responsables del tratamiento deberán valorar si la medida es adecuada y efectiva para aplicar los principios de protección de datos y los derechos de los interesados.
- Los sistemas heredados existentes deben cumplir las mismas obligaciones de PDDD que los sistemas nuevos. Si un sistema heredado no cumple con la PDDD y no es posible realizar cambios para que cumpla con las obligaciones del RGPD, entonces dicho sistema sencillamente no es conforme al RGPD y no puede utilizarse para el tratamiento de datos personales.
- El articulo 25 no rebaja el umbral de los requisitos para las pymes. Los siguientes puntos pueden facilitar que las pymes cumplan el artículo 25:
    - Realizar evaluaciones de riesgos tempranas
    - Comenzar con un tratamiento de pequeña escala y ampliar posteriormente su ámbito y complejidad
    - Buscar garantías de PDDD en los productores y encargados del tratamiento, como certificaciones y cumplimiento de códigos de conducta
    - Utilizar socios que tengan un buen historial
    - Hablar con autoridades de protección de datos (APD)
    - Consultar orientaciones publicadas por las APD y por el CEPD
    - Regirse por los códigos de conducta disponibles
    - Obtener ayuda y asesoramiento profesionales

En nombre del Comité Europeo de Protección de Datos

La presidenta

(Andrea Jelinek)